



City Research Online

City St George's, University of London

Citation: Devey, C. S. H. (2019). A triage playbook: privacy harm and data incident response in the UK. (Unpublished Doctoral thesis, City, University of London)

This is the accepted version of the paper.

This version of the publication may differ from the final published version. To cite this item please consult the publisher's version.

Permanent repository link: <https://openaccess.city.ac.uk/id/eprint/23225/>

Copyright and Reuse: Copyright and Moral Rights remain with the author(s) and/or copyright holders. Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge, unless otherwise indicated, provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way. For full details of reuse please refer to [City Research Online policy](#).

A Triage Playbook: Privacy Harm and Data Incident Response in the UK



Cher S H Devey

Submitted in fulfillment of the requirement for the degree of

Doctor of Philosophy

City, University of London

School of Mathematics, Computer Science and Engineering

Department of Computer Science

June 2019

First Supervisor: Professor Stephanie Wilson

Second Supervisor: Dr. Ilir Gashi

Advisor: Dr. David Haynes

Table of Contents

List of Diagrams	7
List of Diagrams in Appendices.....	9
Acknowledgements.....	11
Declaration	12
Abstract	13
Glossary	14
Chapter 1 Introduction	17
1.1 Setting the scene	17
1.1.2 What is data loss?.....	18
1.1.3 What are personal data, data breach and privacy harm?	18
1.1.4 Framework vs playbook	19
1.2 Motivation and rationale	19
1.3 Summary of identified problems and a research gap	20
1.4 Research question (RQ), aim (RA) and objectives (RO)	22
1.5 Research scope	23
1.6 Overview of methodology	24
1.7 Research contribution and knowledge	25
1.8 Thesis structure	27
Chapter 2 Literature Review.....	29
2.1 Systematic Scoping/Mapping technique (SSM), objectives and questions.....	29
2.1.1 SSM steps and execution.....	30
2.1.1.1 Plan review.....	30
2.1.1.2 Conduct review.....	31
2.1.1.3 Document review	31
2.1.1.4 Synthesise data	31
2.2 Background and related work.....	32
2.2.1 A brief history of data breaches	32
2.2.2 GDPR and EU data landscape	33
2.2.3 What constitutes a DBI and breach notification under the GDPR? (RO1-a).....	34
2.2.3.1 GDPR: beyond the data principles.....	35
2.2.3.2 Breach notification and notification fatigue.....	37
2.2.4 How to assess data harm for breach notification? (RO1-b)	39
2.2.4.1 On privacy harm	40
2.2.4.2 On privacy harm assessment.....	42
2.2.5 What are the characteristics of existing incident response frameworks? (RO1-c).....	45
2.2.5.1 On incident management/handling and triage.....	45
2.2.5.2 Digital investigative processes (DIP) and framework standardisation	47
2.2.6 What is triage and how does it work? (RO1-d)	48
2.2.6.1 Incident triage and medical triage	48
2.2.6.2 Triage ethical principles.....	50
2.2.6.3 Triage in digital forensics	51
2.2.7 What visual methods provide meaningful and practical support for triage processes? (RO1-e)	52
2.2.7.1 Timely initial phased response	52
2.2.7.2 Design principles and visual representation	54
2.3 What did the SSM studies reveal? (RO1)	56
2.3.1 Identified issues.....	56
2.3.2 Ethical triage for DBI response	59
2.3.3 Synthesised triage processes (RO1-1).....	60
Chapter 3 Research Methodology	62
3.1 On Research theorising.....	63
3.1.1 Peirce's pragmatism and modes of inquiry	66
3.1.2 Peirce semiotics-ternary.....	67
3.1.2.1 Peirce ternary	68
3.2 Design Science Research (DSR)	70
3.2.1 Philosophical grounding of DSR	71
3.3 DSR Framework.....	73
3.3.1 DSR activity and process	74
3.3.2 Pre-theory knowledge and framework.....	75

3.4 Application of DSR	78
3.5 Rapid Iterative Testing and Evaluation (RITE)	79
Chapter 4 Personal Data Incident (DBI) Interview Study	81
4.1 Interview study aim and rationale	81
4.1.1 Hybrid Thematic Analysis (hybrid TA) and explanatory framework	81
4.1.2 Justification for the interview study	82
4.2 Summary of interview study approach	83
4.3 Hybrid Thematic Analysis (TA) of interview responses	84
4.3.1 Thematic phases and identification of themes	86
4.3.2 Organising framework	87
4.3.3 Execution of hybrid thematic analysis (TA)	87
4.3.3.1 Set up coding approaches	87
4.3.3.2 Pre-coded questions and topic identification	88
4.3.3.3 Create interviewee's map with the topics	89
4.3.3.4 1st pass coding	89
4.3.3.5 2nd pass coding	90
4.3.3.6 Final analysis of extracts and report themes	90
4.4 Background on the interview results	90
4.5 On DBI response frameworks (EQ1)	92
4.5.1 Organisation, personal and referenced cases	93
4.5.2 Frameworks mentioned by interviewees	96
4.5.3 On standards, plans and tools	98
4.5.4 On effectiveness and efficiency	99
4.5.5 Practical response activities: checklists and triage	100
4.6 Concerns or views on DBI response (EQ2)	101
4.7 Concerns or views on privacy harm to individuals (EQ3)	103
4.8 What did the interviews expose? (RO2)	104
4.8.1 Organisations and DBI response	104
4.8.2 Triage for DBI response	106
4.8.3 Information Governance (IG) and human costs	108
4.8.4 Privacy harm	109
Chapter 5 Prototype Dashboard Design and Build (D&B)	110
5.1 Identified problem and suggestion	111
5.1.1 A triage playbook solution	112
5.2 Dashboard requirements	113
5.2.1 High-level requirements and assumptions	113
5.2.2 Formulation of the checklists	114
5.2.3 On checklists: background and justification	114
5.2.4 Checklists as artefact and conceptual model for decision support during DBI response	115
5.2.5 On breach assessment for notification	116
5.2.6 On the breach indicators and data sensitivity	117
5.2.7 Data matrix	118
5.2.7.1 On the data harm entities	119
5.2.7.2 On data privacy harm assessments (PHA)	120
5.3 Dashboard design	121
5.3.1 Why a visual dashboard?	122
5.3.2 Dashboard design aim	123
5.3.2.1 Functional design level	123
5.3.2.2 Operational design features	123
5.3.3 Dashboard design guidelines	123
5.4 Design and Build (D&B) with developers	125
5.4.1 Iteration 1: DashboardV1	125
5.4.2 Iteration 2: DashboardV2	125
Chapter 6 User Evaluation Study (UES)	128
6.1 UES objective and questions	128
6.2 Justification for the multi-method UES approach	129
6.2.1 On multi-method evaluation	129
6.2.2 Dashboard for prototyping and walkthrough with users	129
6.2.3 Questionnaire design and use	130
6.2.4 Walkthrough techniques	131
6.3 UES Walkthrough with Users	132
6.3.1 Preparation and user selection	134
6.3.2 Pre-Dashboard	135

6.3.3 Dashboard.....	135
6.3.4 Post-Dashboard.....	137
6.4 Data preparation and synthesis	138
6.4.1 Dashboard files	138
6.4.2 Transcript files.....	142
6.5 Results from the Questionnaire (RO4)	143
6.5.1 Profile of Group1 & Group2 Users.....	143
6.5.2 Questionnaire results for Group1 & Group2 (Q19-Q30).....	144
6.5.2.1 How useful are the triage sequence of steps? (RO4-a)(RO4-b)	145
6.5.2.2 How useful are the checklists? (RO4-c).....	145
6.5.2.3 How useful is the dashboard? (RO4-d) (RO4-e) (RO4-f).....	145
6.5.2.4 What are users' views on the impact of the dashboard on their initial DBI response? (RO4-g)	145
6.5.3 Summary and discussion on the Questionnaire results (RO4).....	146
6.6 What did the UES reveal? (RO4)(RA)	150
6.6.1 Justification for scenario and storytelling	151
6.6.2 Storytelling approach and the plot.....	152
6.7 What are the stories from the UES datasets?	154
6.7.1 Profiles and experiences (Q1-Q6)	154
6.7.2 Generic incidents stories (Q7-Q10).....	157
6.7.2.1 On minimal breach information during initial DBI response	157
6.7.2.2 On data breaches and a person's risk.....	157
6.7.2.3 On data breaches and adverse effects on individuals	158
6.7.2.4 On notification fatigue and breach notification	159
6.7.3 Specific incidents stories (Q11-Q18).....	160
6.7.3.1 Scenarios of the triage of the incidents	161
6.7.3.2 Stories on the individual and personal data types.....	162
6.7.3.3 Stories on the protection of data.....	164
6.7.3.4 Scenarios on privacy harm and breach notification: Group1 stories	164
6.7.3.5 Scenarios on privacy harm and breach notification: Group2 stories	169
6.8 What are the Users' stories? (RO4-h) (RO4-i).....	171
6.9 Summary of the stories.....	174
6.9.1 Some quotes from the Group1 Users	174
6.9.2 Some quotes from the Group2 Users	174
Chapter 7 Reflection and Conclusion	176
7.1. Reflection.....	177
7.1.1 Why triage for DBI response?.....	177
7.1.2 Why DSR and Peirce semiotics-ternary?.....	178
7.1.3 Why is there a need to address privacy harm to affected individuals?	179
7.1.4 How to tackle a 'tricky to measure' privacy harm?	180
7.1.5 A data matrix to address a breach notification prioritising question: to notify or not?	181
7.1.6 Concluding remarks on research question (RQ)	183
7.2 Contributions	183
7.2.1 Research contribution – (RC-1).....	183
7.2.2 Research contribution – (RC-2).....	184
7.2.3 Research contribution – (RC-3).....	187
7.2.4 Research contribution – (RC-4).....	188
7.3 Limitations and assumptions	188
7.3.1 Limitations	188
7.3.2 Assumptions	189
7.4 Implications for practice	190
7.5 Suggestions for further research and concluding personal remarks	191
7.5.1 Further research.....	191
7.5.2 Concluding personal remarks.....	193
References	194
Appendices	209
Appendix A: DSR knowledge	209
Appendix B: This research referenced by sources	210
Appendix C: SSM search scope and results.....	211
Appendix D: SSM document review outcomes.....	213
Appendix E: Incident Management Process (IMP) (Tøndel et al., (2014)	214
Appendix F: Hierarchical Objective-based Framework (HOBf) and forensic science maxim	215
Appendix G: Personal Data Breach handling procedure (ENISA, 2012)	216
Appendix H: Interview Study: planning, designing and conducting.....	217

<i>H-1: Elicitation and dialogue</i>	217
<i>H-2: Planning the interview</i>	217
<i>H-3: Designing the interview questions</i>	218
<i>H-4: Selecting interviewees</i>	218
<i>H-5: Pseudonymisation of data</i>	219
<i>H-6: Conducting the interview</i>	219
Appendix I: Interview scripts (original)	221
Appendix J: Interview scripts (revised)	223
Appendix K: Organising framework for Hybrid Thematic Analysis	225
Appendix L: Interviews maps and results	226
Appendix M: Dashboard requirements	231
Appendix N: Verify-Assess-Prioritise with Checklists	233
Appendix O: Data Matrix	236
Appendix P: Design concepts and icons.....	237
Appendix Q: Dashboard components and structure (Ines et al., 2017).....	240
Appendix R: Samples of mockup screens	241
Appendix S: Notes and Job Post	242
Appendix T: Iteration 1 DashboardV1 screenshots	245
Appendix U: Iteration 2 DashboardV2 screenshots	254
Appendix V: UES Questionnaire.....	260
Appendix W: UES user note and consent form.....	264
Appendix X: UES user selection criteria and sample invitation email	266
Appendix Y: UES Walkthrough briefing snapshots	267
Appendix Z: UES Group1: a User Walkthrough screenshots.....	269
Appendix AA: UES Group2: a User Walkthrough screenshots	281
Appendix AB: UES Users: MSD Dashboard screenshots	284
Appendix AC: UES Groups: MSD Dashboard screenshots.....	285
Appendix AD: UES Groups: Qualtrics reports transformation	286
Appendix AE: UES Groups: Questionnaire-MSD	287
Appendix AF: UES NVivo Samples.....	289
Appendix AG: Specific incidents descriptions	291
Appendix AH: Data scenarios: data and impact.....	292

List of Diagrams

Figure 1-1 Research aim (RA), question (RQ), objectives (RO), activities and contributions (RC)	22
Figure 1-2 DSR process, research activities and outputs adapted from Vaishnavi et al. (2017)	24
Figure 1-3 Thesis structure mapped to DSR processes adapted from Van der Merwe et al. (2017)	27
Figure 2-1 SSM objectives and questions	30
Figure 2-2 SSM steps and activities adapted from Petersen et al. (2008)	30
Figure 2-3 Timeline of key data privacy breach notification events	32
Figure 2-4 EU data laws (2003-2018)	34
Figure 2-5 GDPR Data Principles (ICO, 2018)	36
Figure 2-6 Data Abuse Pyramid synthesised from Solove (2008)	40
Figure 2-7 Incident Handling and Triage (ENISA, 2010)	46
Figure 2-8 Notification in the Incident Response Phase in the IMP from Tøndel et al. (2014)	46
Figure 2-9 Computer Forensics Field Triage Process Model (CFFTPM) (Rogers et al., 2006)	51
Figure 2-10 Incident stages and phases	61
Figure 2-11 Triage DBI response entities	61
Figure 3-1 Theory Change (UC Berkely, 2010)	65
Figure 3-2 Peirce Ternary	69
Figure 3-3 Peirce-Morris Semiotics simplified from Huang (2006)	70
Figure 3-4 Triage Semiotics	70
Figure 3-5 Philosophical assumption of three research perspectives (Vaishnavi et al., 2017)	72
Figure 3-6 DSR Framework adapted from Vaishnavi et al. (2017)	74
Figure 3-7 DSR Activity	75
Figure 3-8 DSR Process Flow adapted from Offermann et al. (2009)	75
Figure 3-9 Outputs of DSR (Vaishnavi et al., 2017)	76
Figure 3-10 Levels of contribution in DSR (Gregor and Hevner, 2013)	77
Figure 3-11 Pre-theory design framework: the triage playbook	77
Figure 3-12 RITE Process adapted from Shirey et al. (2013)	80
Figure 3-13 Prototyping activity	80
Figure 4-1 Interview Study Aim and Explanatory Questions	81
Figure 4-2 Hierarchical Structure	85
Figure 4-3 Thematic Phases and Steps synthesised from Braun and Clarke (2006)	86
Figure 4-4 Hybrid Thematic Analysis Steps	88
Figure 4-5 1 st Pass Coding	88
Figure 4-6 2 nd Pass Coding	88
Figure 4-7 Interviewee's map for coding	89
Figure 4-8 A view of all indexed and extracted Theme Maps	91
Figure 4-9 DBIs mentioned by interviewees	94
Figure 4-10 Interviewees victim in DBI	94
Figure 4-11 Referenced DBI	95
Figure 4-12 Organisation-Referenced-Personal Incidents and Types	96
Figure 4-13 Frameworks mentioned by Interviewees	97
Figure 4-14 DBI response activities synthesised from Interviews	101
Figure 5-1 Design & Build (D&B) objective/sub-objective	110
Figure 5-2 Triage playbook: entities	112
Figure 5-3 Triage playbook: conceptual model	113
Figure 5-4 Triage playbook: design space	121
Figure 5-5 Triage playbook: solution space	122
Figure 5-6 DSR process mapping for the D&B Iteration 1	126
Figure 5-7 DSR process mapping for the D&B Iteration 2	127
Figure 6-1 UES objective and questions	129
Figure 6-2 Summary view of UES Questionnaire & Dashboard	131
Figure 6-3 UES Activity Flows	133
Figure 6-4 Data Preparation and Synthesis	138
Figure 6-5 UES Integrated Excel files: Group1 lists	140
Figure 6-6 UES Integrated Excel files: Group2 lists	141
Figure 6-7 UES Group1 Triage Results	142
Figure 6-8 UES Group2 Triage Results	142
Figure 6-9 NVivo Coding Structure	143
Figure 6-10 NVivo Coded Nodes	143
Figure 6-11 UES Users' Profiles	144
Figure 6-12 Questionnaire results Q19-Q20 (Sequence of steps)	145
Figure 6-13 Questionnaire results Q22-Q25 (Checklists)	145
Figure 6-14 Questionnaire results Q26-Q29 (Dashboard and alerts)	145
Figure 6-15 Group1 Q30	146
Figure 6-16 Group2 Q30	146

Figure 6-17 Group1 Synthesised Charts Results	148
Figure 6-18 Group2 Synthesised Charts Results	149
Figure 6-19 Abductive-Deductive-Inductive Storytelling	152
Figure 6-20 Group1 profiles and experiences (DBI, PIA & PHA)	155
Figure 6-21 Group2 profiles and experiences (DBI, PIA & PHA)	156
Figure 6-22 Group2 minimal breach information	157
Figure 6-23 Group1 minimal breach information	157
Figure 6-24 Group2 data breach and a person's risk	157
Figure 6-25 Group1 data breach and a person's risk	157
Figure 6-26 Group1 data breach and adverse effects	158
Figure 6-27 Group2 data breach and adverse effects	158
Figure 6-28 Group1 notification fatigue and breach notification	159
Figure 6-29 Group2 notification fatigue and breach notification	159
Figure 6-30 Group1 scenarios of the triage	161
Figure 6-31 Group2 scenarios of the triage	162
Figure 6-32 Personal data types	163
Figure 6-33 Individual types	163
Figure 6-34 Group2 individual checklist (usage)	163
Figure 6-35 Group1 individual checklist (usage)	163
Figure 6-36 Group1 data checklist (usage)	164
Figure 6-37 Group2 data checklist (usage)	164
Figure 6-38 Group1 level of impact – harm and distress	165
Figure 6-39 Data types and impact levels (e.g. c6's data scenarios)	166
Figure 6-40 Data types and impact levels (e.g. f8, g7 and h5)	166
Figure 6-41 Group1 impact and notification	168
Figure 6-42 Group2 level of impact – harm and distress	170
Figure 6-43 Group2 impact and notification	170
Figure 6-44 Data types and impact levels (e.g. b11, b12, b16 and h9)	171
Figure 6-45 Group1 users' remarks	172
Figure 6-46 Group2 users' remarks	173
Figure 7-1 Summary view of research question (RQ), objectives (RO) and contributions (RC)	176

List of Diagrams in Appendices

Figure A- 1 Useful knowledge (Gregor and Hevner, 2013)	209
Figure A- 2 DSR knowledge form (Johannesson and Perjons, 2014, p 21-28)	209
Figure A- 3 DSR knowledge types (Johannesson and Perjons, 2014, p 21-28)	209
Figure B- 1 Triage semiotics steps: referenced in (Conference, April 2017)	210
Figure B- 2 A business interested in research (Email, February 2018).....	210
Figure B- 3 A DPO interested in research (DPO, July 2018)	210
Figure C- 1 Scoping and search keywords.....	211
Figure C- 2 Search result September - October 2016	211
Figure C- 3 Search result from EThOS August and October 2016	212
Figure D- 1 Scope-Assumption-Finding.....	213
Figure E- 1 The incident management lifecycle process (IMP) (Tøndel et al., 2014)	214
Figure F- 1 Overarching investigative objectives (Beebe and Clark, 2005)	215
Figure F- 2 First tier phases of the HOBf framework (Beebe and Clark, 2005).....	215
Figure G- 1 Personal Data Breach handling procedure (ENISA, 2012)	216
Figure H- 1 Interview activities cycle	218
Figure K- 1 Organising framework for Hybrid Thematic Analysis	225
Figure L- 1 Interviewees – industry profile	226
Figure L- 2 Interviewees – shared notes	226
Figure L- 3 Experience and interviews duration	227
Figure L- 4 Incidents reported by interviewees	228
Figure L- 5 Frameworks by interviewees	229
Figure L- 6 Data types mentioned by interviewees	230
Figure N- 1 Verification and Checklists	233
Figure N- 2 Assessment and Checklists.....	234
Figure N- 3 Prioritisation and Checklists	235
Figure O- 1 Data Matrix	236
Figure P- 1 Tentative design concepts	237
Figure P- 2 Tentative design icons	238
Figure P- 3 Design icons.....	239
Figure P- 4 A Good Practice Guide.....	239
Figure Q- 1 Dashboard component (Ines et al., 2017)	240
Figure Q- 2 Dashboard structure (Ines et al., 2017).....	240
Figure S- 1 First email with Developer1	242
Figure S- 2 Job details on upwork.com	243
Figure S- 3 First email with Developer2	244
Figure T- 1 Welcome screen and Menu	245
Figure T- 2 Log a new incident.....	246
Figure T- 3 Calendar for selecting the date and time	246
Figure T- 4 Verification of individuals	247
Figure T- 5 Verification of individuals: location	247
Figure T- 6 Verification of individuals: types.....	248
Figure T- 7 Verification of individuals: number.....	248
Figure T- 8 Verification of data: types.....	249
Figure T- 9 Assessment of data: volume	249
Figure T- 10 Assessment of data: form	250
Figure T- 11 Assessment of data: security	250
Figure T- 12 Assessment of data: security measures (non-digital)	251
Figure T- 13 Prioritisation screen: triage and notification results.....	251
Figure T- 14 Prioritisation screen: impact levels	252
Figure T- 15 Prioritisation screen: why notify individuals?	252
Figure T- 16 Prioritisation screen: why notify the ICO?	252
Figure T- 17 Dashboard Menu: features	253
Figure T- 18 Dashboard Menu: top right-hand menu	253
Figure U- 1 Verification of individuals: new type.....	254
Figure U- 2 Confidence level: individuals suffer distress	254
Figure U- 3 Verification of data: new types	255
Figure U- 4 Confidence level: personal data compromised	255
Figure U- 5 Confidence level: compromised volume of data.....	256
Figure U- 6 Confidence level: security protection.....	257
Figure U- 7 Confidence level: results on prioritisation screen (1).....	258
Figure U- 8 Confidence level: results on prioritisation screen (2).....	259
Figure Z- 1 Pre-Dashboard: Background Q1-3	269
Figure Z- 2 Pre-Dashboard: Views on PHA Q6	269
Figure Z- 3 Pre-Dashboard: Scenario selection Q11	270

Figure Z- 4 Pre-Dashboard: Scenario description Q12	270
Figure Z- 5 Pre-Dashboard: Breach notification Q15	271
Figure Z- 6 Pre-dashboad: Breach Notification Q18	271
Figure Z- 7 Pause Questionnaire	272
Figure Z- 8 Dashboard: Welcome Screen	272
Figure Z- 9 Dashboard: Select date incident logged	273
Figure Z- 10 Dashboard: Select time incident logged	273
Figure Z- 11 Dashboard: Verification Checklists Individuals	274
Figure Z- 12 Dashboard: Verification Checklists Data	274
Figure Z- 13 Dashboard: assessment data volume	275
Figure Z- 14 Dashboard: assessment data form	275
Figure Z- 15 Dashboard: Prioritisation screen	276
Figure Z- 16 Dashboard: Why notify the individuals?	276
Figure Z- 17 Dashboard: Why notify the ICO?	277
Figure Z- 18 Dashboard: Menu	277
Figure Z- 19 Dashboard: Incident List Menus Options	278
Figure Z- 20 Dashboard: Incident still in Verification stage	278
Figure Z- 21 Post-Dashboard: Triage sequence of steps Q1	279
Figure Z- 22 Post-Dashboard: Checklists Q22-Q23	279
Figure Z- 23 Post-Dashboard: Notification & Alerts Q27-Q28	280
Figure Z- 24 Post-Dashboard: Impact & Improvements Q30-Q31	280
Figure AA- 1 DashboardV2: Help Text	281
Figure AA- 2 DashboardV2: Verification-Confidence Level-distress	281
Figure AA- 3 DashboardV2: Verification-Confidence Level-data	282
Figure AA- 4 DashboardV2: Assessment-Confidence Level-volume	282
Figure AA- 5 DashboardV2: Assessment-Confidence Level-security	282
Figure AA- 6 DashboardV2: Prioritisation-Confidence Level-display	283
Figure AA- 7 DashboardV2: Prioritisation-Confidence Level-display2	283
Figure AB- 1 JSON-MSD: A Group1 User	284
Figure AB- 2 JSON-MSD: A Group2 User	284
Figure AC- 1 Group1 Dashboard: Impact levels & notification	285
Figure AC- 2 Group2 Dashboard: Data Impact levels	285
Figure AD- 1 UES Qualtrics Export	286
Figure AD- 2 UES Qualtrics Group1 Report	286
Figure AD- 3 UES Qualtrics Group2 Report	286
Figure AE- 1 UES Questionnaire-MSD: organised topic	287
Figure AE- 2 UES Questionnaire-MSD: Checklist	287
Figure AE- 3 UES Questionnaire-MSD: Other remarks (Q31-Q32)	288
Figure AF- 1 NVivo coded: checklists	289
Figure AF- 2 NVivo coded: dashboard remarks	289
Figure AF- 3 NVivo coded: harm assessments	290
Figure AF- 4 NVivo coded: prioritisation	290
Figure AF- 5 NVivo coded: notification alert	290
Figure AG- 1 Group1 specific incidents description	291
Figure AG- 2 Group2 specific incidents description	291
Figure AH- 1 Group1 data types and impact levels	292
Figure AH- 2 Group2 data types and impact levels	293
Figure AH- 3 Group1 individual types and impact levels	293
Figure AH- 4 Group2 individual types and impact levels	293

Acknowledgements

My PhD journey would not have been possible without the financial bursary from City, University of London (City), and the on-going valuable and dedicated support from my supervisors, Steph and Ilir. Many gracious thanks to my supervisors and also special thanks to David who has provided loyal support and advice throughout my time at City. Many thanks to Ludi Price who came to my rescue when I was pushed for time to get icons for my prototype dashboard. Ludi beautifully drew the individual icons based on my specified examples and specifications.

I am grateful to all the people who kindly took time off from their busy schedules to support and participate in interviews and the user evaluation study. The outcome of this research is for these people and their organisations who recognised their valuable contributions towards privacy and data incident response research.

My time at City has been full of challenges and adventures but it has all been worth it. There are countless friends, and the unsung heroes – City’s library staff – who have made a difference to my PhD journey. I want to extend my heartfelt thanks to them.

To my wonderful girls, Rebecca and twins Sonya and Tanya, who have had to endure my anguish and dramas for the past years while I pursue my personal goals. In loving memory of my beloved parents who gave me unconditional love and who taught me the meaning of being alive.

Lastly, I dedicate this to my dear friend Roger Clough without whom I would never have started and finish this journey.

Declaration

I grant powers of discretion to the University Librarian to allow this thesis to be copied in whole or in part without further reference to me. The permission covers only single copies made for study purposes, subject to normal conditions of acknowledgement.

Abstract

Personal data incidents have become a serious concern in almost every industry. In the UK, the TalkTalk data breach in October 2015 generated headline news and raised public awareness of data breaches. Under the EU General Data Protection Regulation (GDPR), organisations in the UK are held accountable for reporting data breach incidents to the Information Commissioner's Office (ICO) within 72 hours. Furthermore, organisations are required to notify the ICO and to communicate with affected individuals where there is high risk. However, the triggers or criteria for what constitutes a general risk and a high risk are not clear.

Researchers have pointed out that privacy impact assessments (PIA) and breach notifications are new concepts. There is no universal PIA framework which could be used for comparative privacy risk analysis. Security-related literature on PIA primarily addresses the prevention of harm through technical measures or system development and says little about assessing the harm to individuals. The overall aim of this PhD was to explore personal data incident (DBI) response, data privacy harms and breach notifications under the GDPR.

Firstly, in-depth personal interviews were conducted to gauge the extent and nature of DBI responses by organisations in the UK. Interviewees viewed breach notifications as a '*right thing to do*' but raised concerns about the GDPR breach notification timelines. Although there is no dedicated DBI response framework, interviewees were using triage and checklists during DBI response. Based on these findings, in the second stage of the research, a research question was framed: *How can a triage playbook be used to address data privacy harms for breach notification prioritisation during the initial response to a personal data incident?* A triage playbook was developed; this synthesised the triage steps; operationalised the steps with checklists; and created a data matrix for scoring the likely impact on individuals. Finally, in a third study, two dashboards were iteratively designed and tested with practitioners through a facilitated walkthrough and online questionnaire.

The triage playbook was found to meet practitioners' need to prioritise notification for the ICO and affected individuals when there is a data breach. The overall novel contribution of this research is to extend knowledge of how triage, checklists and a data matrix can be used to support organisations in the UK to address privacy harm to affected individuals for prioritising breach notifications during the initial response to a DBI.

Glossary

Term	Description
3LevelModel	A three-level hierarchical model for analysing existing forensics frameworks by Pollitt (2007).
AI	Artificial Intelligence.
Artefact	An artefact is defined here as an object made by humans with the intention that it be used to address a practical problem. Examples of artefacts in the IT and information systems area are: algorithms, information models, design guidelines to demonstrators, prototypes, and production systems (Johannesson and Perjons, 2014, p 3). The British spelling, <i>artefact</i> was used throughout this research except in direct quotes where <i>artifact</i> was used.
BCS	British Computer Society (The Chartered Institute for IT).
C	C – in the dialogues with users in the User Evaluation Study (UES) – refers to this researcher i.e. Cher Devey.
CERT	Computer Emergency Response Team.
CFFTPM	Computer Forensics Field Triage Process Model by Rogers et al. (2006).
Checklist	<i>A checklist is typically a list of action items or criteria arranged in a systematic manner, allowing the user to record the presence/absence of the individual items listed to ensure that all are considered or completed</i> (Hales and Pronovost, 2006).
CIA	Confidentiality, Integrity, Availability.
CSIRTs	Computer Security Incident Response Teams.
CSREC	Computer Science Research Ethics Committee at City, University of London.
Cyber Essentials	Cyber Essentials is a UK government-backed cyber security certification scheme that sets out a good baseline of cyber security suitable for all organisations in all sectors.
Cyberspace	Refers to the virtual environment of information and interactions between people.
Data	Data and information are used interchangeably.
Data harm	Refers to privacy harm.
Data incident	Refers to personal data incident where personal data is the primary focus and not the security practices/measures to protect the architecture covering network, device, software or systems.
Datix	A software toolkit: https://www.datix.co.uk/en/about [Accessed 30-December-2018].
DB	Refers to personal data breach or data breach.
DBI	Refers to personal data incident.
DCMS	Refers to the UK Department of Digital, Culture, Media & Sport
DFRWS	Refers to the Digital Forensic Research Workshop (DFRWS) in 2001: https://www.dfrws.org/about-us [Accessed 28-December-2018].
DIP	Digital Investigative Processes.
DPA	Data Protection Act 1998, UK; Repealed on 25 th May 2018 by DPA UK 2018 [Not examined in this research which started before 2018].
DPIA	Data protection impact assessment as in the GDPR Article 35. However, the term privacy impact assessment (PIA) is commonly used as privacy has wider implications than data protection. PIA is used in this research instead of DPIA.
DPM	Data Protection Manager.
DPO	Data Protection Officer.
DSR	Design Science Research.
ENISA	The European Union Agency for Network and Information Security (ENISA) is a centre of expertise for cyber security in Europe.
ePrivacy	Refers to the EU Electronic Privacy Directive.
ePR	Refers to the EU Electronic Privacy Regulation which will repeal ePrivacy [Not examined in this research].
EQ	Refers to the explanatory questions (EQ), framed around the interview study aim, for reporting the themes that were extracted (using hybrid TA) from the interview study data.
EU	European Union.
EU data laws	Refers to the EU data protection and privacy related Regulations and Directives.
Forensics	Digital forensics.
Framework	Frameworks as a label to include procedures, processes, policies, principles, approaches, plans, steps or activities.
FreeMind	Free mindmapping software. FreeMind was used throughout this thesis for presenting information visually: http://freemind.sourceforge.net/wiki/index.php/Main_P [Accessed 28-December-2018].
GDPR	EU General Data Protection Regulation implemented on 25 th May 2018. GDPR Articles and Recitals are from GDPR (2018).
Hybrid TA	A deductive and inductive (hybrid) thematic approach (TA).
ICO	UK Information Commissioner's Office.
IG	Information Governance.

IMP	Refers to <i>The incident management lifecycle process</i> , synthesised from ISO/IEC27035 and NIST SP 800-61 by Tøndel et al. (2014).
Incident	Refers to security incident, computer security incident, information security incident, ICT security incident or cybersecurity incident.
Individual	Refers to customer/subscriber/consumer or data subject.
INT	Interviewer (this researcher, Cher Devey) in the interview study.
Interviewee ID	Refers to the code (industry code + number) for marking the interviewee who took part in the interview study. Participant in interview study is referred to as interviewee.
IS	Information System.
ISO/IEC	International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
ISPs	Internet Service Providers.
IT	Information Technology.
JSON	JavaScript Object Notation a lightweight data-interchange format.
KWIC	<i>Key word in context</i> : In a KWIC approach, key words or phrases were identified and the corpus of text was systematically searched to find all instances of each key word or phrase (Ryan and Bernard, 2003).
Labels/titles	The labels/titles in all the figures used the computer modelling style (i.e. not grammar constructs) and/or the labels as used in the extracted figures. Most large <i>tables</i> (i.e. sheets) are presented as <i>images</i> . Editing large <i>tables</i> in MS Office (Mac version) <i>text</i> boxes were avoided. Short labels were used in Figure 4-13 p 97 and Figure L- 5 p 229, i.e. mgt = management; ISI = Information Security Incident; cmd & ctrl=command & control; appl=application; PIA=privacy impact assessment; fw=framework; HSC=health & social care; int=internal; M-UFO-N=Mutual-unidentified flying object-Network; NHS=National Health Service; CI=cyber incident; RCA=root cause analysis; LC assess=lifecycle assessment; DPA=Data Protection Act; BAU=business as usual; CIA=Confidentiality, Integrity, Availability.
MSD	Refers to the MicroStrategy Desktop. MSD is a Business Intelligence platform which provides easy interface to perform data analysis with charting (intelligence) capabilities. MicroStrategy Desktop at: https://www.microstrategy.com/us/platform [Accessed 28-December-2018].
NHS	National Health Service
NIS	Network and Information Security.
NIST SP 800-61	National Institute of Standards and Technology (NIST), U.S. Department of Commerce: A special publication which aims to assist organisations in mitigating risks from computer security incidents by providing guidelines on how to respond to incidents effectively and efficiently.
NVivo	NVivo (for Mac V11.4.3) is Qualitative Data Analysis Software (QDAS).
OECD	Organisation for Economic Co-operation and Development
OODA	OODA loop refers to the decision cycle of observe, orient, decide, and act, developed by US military strategist Colonel John Boyd.
Organisation	An organisation is an entity with one person or more, who provides services/goods, and generally conducts its business in cyberspace. Organisations in the critical infrastructure services industry, i.e. energy and other utility companies, are excluded in this research. Organisations in the context of GDPR discussion are the Data Controllers and Data Processors. They have joint responsibilities for data protection and breach assessment for DBI response. The Processor notifies the Controller instead of the individuals upon <i>first aware</i> . GDPR Article 33(2).
p	Page number.
Paradigm	A way (approach) of looking at the world or problems (viewpoint/perspective).
PECR	Privacy and Electronic Communications (ePrivacy Directive) Regulations 2003, UK.
Peirce	Charles Sanders Peirce (1839-1914) American philosopher, logician, mathematician and scientist.
PHA	Data privacy harm assessments. PHA is similar in concept with PIA, except in PHA the focus is on <i>the likely consequences of the data breach</i> to data subjects.
Philosophy	The study of knowledge.
PIA	Privacy impact assessments. PIA is a methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts.
PII	Personally Identifiable Information
Playbook	A script for action. A set of rules or suggestions (scripts) that are considered to be suitable for a particular activity, industry, or job: http://dictionary.cambridge.org/dictionary/english/playbook [Accessed 28-December-2018].

	The word <i>scripts</i> sounds more in tune with the nature of the usage of a playbook. Playbook also denotes <i>action</i> , unlike a framework. A <i>frame for working</i> rather than a <i>script for action</i> .
PRIAM	A privacy risk analysis methodology (PRIAM) by De and Le Métayer (2016a).
Privacy harm	Data privacy harm or data harm e.g. distress to individuals whose personal data have been compromised due to a DBI. The terms <i>privacy harm</i> and <i>harm</i> are used synonymously. The terms <i>consequence</i> or <i>damage</i> instead of <i>harm</i> are also used. For example, the GDPR uses <i>damage</i> instead of <i>harm</i> .
Prototype	Prototyping was used as a proof-of-concept and proof-of-use to demonstrate feasibility, utility and the significant triage playbook components.
Proof-of-concept	Proof-of-concept prototypes demonstrate understandings of technical feasibility (Nunamaker and Briggs, 2012).
Proof-of-use	Proof-of-use constitutes evidence of holistic understandings of the rich social, political, economic, cognitive, emotional, and physical contexts in which our systems operate (Nunamaker and Briggs, 2012).
Qualtrics	Qualtrics survey tool is a resource provided by City, University of London. URL for Qualtrics (Signed-on via City's account): https://cityunilondon.eu.qualtrics.com/ControlPanel/?ClientAction=ChangeP&Section=MyProjectsSection [Accessed 28-July-2018].
RA	Research aim of this Thesis.
RES	Respondent in the interview study.
RITE	Rapid Iterative Testing and Evaluation.
RO	Research objectives and sub-objectives of this Thesis.
RQ	Research question of this Thesis.
SEI-CMU	Software Engineering Institute - Carnegie Mellon University.
SLR	Systematic Literature Review
SSM	Systematic Scoping or Mapping Studies. Does not cover details of meta-analysis nor does it discuss the implications that different types of systematic review questions have on research procedures.
TA	Thematic Approach
Text in <i>italics</i>	Questions, original texts and quotations are in <i>italics</i> . Quotations e.g. by interviewees and UES users are also enclosed with single quotation marks.
Text in bold	Texts in bold are to emphasise or highlight the texts e.g. 1 st use of a shortening label. Also, data captured in the prototype dashboard is shown in <i>italic and bold</i> and using the field names as displayed on the dashboard screens.
Thematic Phases	Refers to Braun and Clarke's (2006) thematic phases.
Theory	System of ideas or beliefs or models.
Triage playbook	A triage playbook using triage steps, checklists and data matrix for assessing data privacy harm to support breach notifications during initial personal data incident response.
UES	User Evaluation Study.
User ID	Refers to the code (industry code + number) for marking the user (in lower case industry code) who took part in the UES. Participant in UES is referred to as User/user.
Zotero	Zotero was used for document and citation management: https://www.zotero.org/ [Accessed 28-December-2018].

Chapter 1 Introduction

The technology is linked data, and data is relationships – Sir Tim Berners-Lee (TED.com, 2009)

Information has financial value, and data is the new 21st Century currency for doing business. Personal information is an important currency in the digital age. It can be used to control people, steal their identities or be mined to extract value (Gunasekara, 2014).

In today's age of prolific transmission of vital data, organisations can face serious problems relating to data cyber invasion and hacking, resulting in data loss and data breach. If there is one constant, it is the changing cyberspace landscape. And almost daily we hear of theft and/or disclosure of personal information.

In the UK, the TalkTalk data breach in October 2015 generated headline news (Auchard, 2015; Johnston, 2015). Although the amount of compromised personal data (i.e. 156,959 customers (ICO, 2017)) was not on the same scale (40 million credit and debit card) as the US Target case (Shacklett, 2014), the data incident cost TalkTalk £42million (BBC News, 2016). TalkTalk was fined £400k out of a maximum of £500k, the largest fine imposed by the ICO in 2016 (ICO, 2017), and also generated public awareness of data breaches which are normally unreported. Under GDPR, which came into effect on 25th May 2018 (GDPR, 2018), with stringent breach notification requirements and hefty breach fines, TalkTalk could have been fined 79 times more or £59million (Leyden, 2017). Such financial fines do not reveal the damages or harm that affected TalkTalk customers. A *fuming* TalkTalk customer said: *'The late announcement is not really acceptable either but even worse is the communications. By the time people are informed who knows how much could have been stolen'* (Johnston, 2015).

Besides large reported data breaches, there are countless news items about organisations suffering some form of data hack, data loss or data breach almost on a daily basis. For example, BCI (2014) reveals that organisations are concerned with data breach and cyber-attack. As noted in Ring (2013), *security breaches are reaching crisis levels – 93% of large UK organisations were breached in the past 12 months as well as 87% of small businesses.*

Such motivating data breach related themes and the GDPR provided the context for this research and subsequent identification of research questions and objectives. The following sections set the scene by describing the notable and challenging keywords or phrases which will then lead on to the motivation and rationale behind this research.

1.1 Setting the scene

In the context of data protection, Stalla-Bourdillon and Knight's (2016) and Elliot et al's (2016) descriptions of *data* are relevant: *'The idea of data characteristics as fluid concepts which, as a matter of fact, can only be understood in the context of appreciating ongoing processes related to the data environment, and which does not 'simply' focus upon data as having static and immovable qualities.'* Similar contextual and fluid concepts of data are also described by Rowley (2007). In this research, the terms data and information are used interchangeably and shared the same meaning.

The terms data loss and data breach have appeared in the context of data privacy or personal data security related breaches or incidents as reported in the news and also in Hinde and Ophoff (2014)

and Phua (2009). However, these terms are not defined. As these terms have various usage and associated privacy harm issues they are discussed briefly in the following sections.

1.1.2 What is data loss?

Open Security Foundation (2014) uses the term data loss incidents but has no definition for data loss. In *Threatsaurus: Data loss is the result of the accidental misplacement of data, rather than its deliberate theft, and data theft is the deliberate theft of information, rather than its accidental loss. Data loss frequently occurs through the loss of a device containing data, such as a laptop, tablet, CD/DVD, mobile phone or USB stick. Data theft can take place both inside an organisation (e.g. by a disgruntled employee), or by criminals outside the organisation* (Sophos Limited, 2013).

Other terms for this phenomenon include data leak and also data spill which refer to unintentional information disclosure (ACSC, 2018). Howard (1997) however mentioned *loss of computer files* and *breach of computer security* in the context of computer security.

In essence, there is data loss due to computer hardware, software loss (Smith, 2003) or computer files damaged or lost, and there is data loss due to leakage, disclosure or theft of data, where loss is when the data is no longer under the control of the rightful (Layton and Watters, 2014) or legitimate owner(s). Data loss i.e. *loss of control over their personal data* constitutes a personal data breach under GDPR Recital 85.

1.1.3 What are personal data, data breach and privacy harm?

The term data breach has the connotation of breach, as in *the act of breaking or failing to observe a law, agreement, or code of conduct* (Dictionary.com, 2016). Data refers to personal data, hence data breach stands for personal data breach or personal data incident (**DBI**). In this research, incident refers to security incident, computer security incident, information security incident, ICT security incident or cybersecurity incident. The term data incident will refer to personal data incident where personal data is the primary focus and not the security practices/measures to protect the architecture covering network, device, software or systems. In essence the scope is on data incident response during a personal data incident in organisations in the UK.

GDPR Article 4(1) defines *personal data* as: *any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*. This research adopted the GDPR definitions for personal data and GDPR Article 4(12) for *personal data breach*, which means *a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*.

Howard and Gulyas (2014) describe personal records as: *a) data containing privileged information about an individual that cannot be readily obtained through other public means and b) this information only known by an individual or by an organisation under the terms of a confidentiality agreement*. Such business data related agreements are a norm, but they do not offer personal data or privacy protection.

Personal data is no ordinary *asset*. It is tradable (the new oil) – the processing of it is legally restricted by data protection and privacy laws (e.g. GDPR) – and it can be highly sensitive and revealing about a person’s identity (Spiekermann et al., 2015). Privacy or data privacy is difficult to operationalise or grapple with – it is intangible – unlike personal data or PII which is the new tradable oil. The World Economic Forum (2011) states: *personal data will be the new oil - a valuable resource of the 21st century*.

However, personal data in relation to privacy shares similar intrinsic value in the form of a *human matter or human trait* (Al-Fedaghi and Thalheim, 2008). It is this intrinsic human matter value (or *human costs*) that makes personal data a valuable tradable asset to organisations and other stakeholders including hackers and which makes headline news under the broad terms of data breach incidents. Being a tradable asset, there are also the consequences of such data exchanges, namely the privacy harm on the individuals whose personal data are compromised by data incidents. De and Le Métayer (2017) say this: *A privacy harm is a negative impact of the use of the system on a data subject, or a group of data subjects (or society as a whole) as a result of a privacy breach*. In this research, data privacy harm or data harm refers to the distress to individuals whose personal data have been compromised due to a DBI. There are numerous terms used in this thesis, most are listed in the glossary. However, the term *playbook* as used in this thesis title is described next.

1.1.4 Framework vs playbook

Many authors have indirectly or implicitly used the term *framework*, to represent a conceptual model/structure or a set of workflows/activities or processes or models, and/or for organising a collection of contents (under investigations/studies) and the relationships between entities/elements in the contents. One characteristic of these frameworks is that they depict concepts diagrammatically. Framework does not denote interactivity or human-interaction, unlike the term *playbook*. A *playbook* denotes a script for action. It seems that industry practitioners¹ use *playbook* in describing security or cyber events and their associated activities/processes. For example, a book written by members of Cisco's CSIRT includes: *know what actions to take during the incident response phase* (Bollinger et al., 2015).

As the outcome of this research was an actionable triage *playbook*, therefore, the use of the term *playbook* for this research is appropriate. Most importantly, *a triage playbook* – in the title for this research – distinguishes this research outcome from other referenced security incident related frameworks.

1.2 Motivation and rationale

This researcher’s work drove her to study aspects of data law. Obtaining a post graduate diploma in law led to publication of a paper on electronic discovery (Devey, 2008), and two data-law related talks

¹ Examples [Accessed 28-December-2018]: A Playbook for Cyber Events, Second Edition by the American Bar Association: <http://shop.americanbar.org/eBus/Store/ProductDetails.aspx?productId=133210976>
Cyber Exercise Playbook by the Mitre Corporation: https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf

presented at the BCS Office in London. Most recently in 2018, this researcher publicised² her research interests on the EU General Data Protection Regulation (GDPR). GDPR repeals the 1995 Data Protection Directive on 25th May 2018. A stated objective of the GDPR is to strengthen personal data protection and unifying European data protection law. Although this researcher presented a talk on GDPR in 2012³, this research focus on GDPR only started in October 2015. One key driving motivation was the GDPR which underpins the issues affecting organisations when faced with data breaches. For example, Schwartz and Peifer (2017) describe GDPR as *the future DNA of EU privacy law*. However, research on GDPR focusing on themes relating to privacy and incidents appears to represent new fields for IT/computer researchers⁴. Since the TalkTalk incident, there is more public awareness of data breaches which in the GDPR era, means that organisations need to be prepared for timely reporting or notification of the incident to the ICO, and in certain cases also notify their affected customers or individuals. Failure to comply with the GDPR on breach notification will expose organisations to financial fines and other non-financial repercussions related to data privacy harm on the individuals.

Interests in data privacy led to an overarching research aim: To explore personal data incident (**DBI**) response, data privacy harms (**data harm**) and breach notifications under the GDPR. During the exploration a solution also emerged to address the identified problem and a gap in research. The rationale for developing the solution and the nature of the identified problem led to the adoption of design science research (**DSR**) for this research methodology which is described in Section 1.6. The following section describes the identified problems and a research gap.

1.3 Summary of identified problems and a research gap

A problem was identified: organisations will need to conduct data privacy harm assessment (**PHA**) during initial DBI response to meet the GDPR breach notification requirements. Research on PHA and breach notification during DBI response appeared to be new research topics in the field of incident response. In particular, a gap in research seemed to be the data privacy harm to affected individuals as a consequence of DBIs. Although there are numerous available risk assessment methodologies, there is no universal privacy impact assessment (**PIA**) framework which could be used for referencing or comparative privacy risk analysis. Even in the established information security risk domains, there is a lack of agreed reference benchmarking, as well as in the comparative framework for evaluating information security risk methods and information security risk (Shamala et al., 2013). The notion of *privacy harm* or *avoiding harm to people* whose personal data has been compromised or lost in a DBI or a security incident appears not to be an area of research in the computer science and security incident domains. This is in contrast to *damage to systems* which has appeared in computer security incident responses (Brownlee and Guttman, 1998, p 15). However, researchers (Asokan, 2017; Abrams et al., 2019) have started discussions on ethics which will help our understanding of the notion of privacy harm. Also, the DCMS's (2019) white paper on

² <https://www.city.ac.uk/news/2018/april/city-academics-discuss-gdpr-at-press-briefing>
<https://www.infosecurity-magazine.com/next-gen-infosec/gdpr-phd-subject/>
<https://www.infosecurity-magazine.com/webinars/post-gdpr-will-it-be-too-late-to/> [Accessed 28-December-2018].

³ The GDPR talk at BCS Office:
<http://jollyvip.com/edisclosure/2013/09/02/bcs-techlaw-talk/> [Accessed 28-December-2018].

⁴ E.g. search on (((GDPR) AND privacy) AND incident) on IEEE.org retrieved 1 item - an IEEE Course, no articles; on Scopus.com - 3 articles dated 2017-2018; on heinonline.org - 16 articles [Accessed 16-September-2018].

Online harms will raise awareness of the need to address privacy harm which should also generate more interest and research on the notion of harm to people.

The breach notifications in GDPR requires organisations (Data Controllers) to notify the ICO where there *is risk to the rights and freedoms of individuals*, and to communicate to the data subjects (individuals) where there is *high risk*. However, the triggers or criteria for what constitute *risk* and *high risk* are not clear. This means any PIA as a consequence of the compromised data, for breach notification requirements will be fraught with challenges as privacy is contextual. What organisations perceived as harm to the affected individuals may not be viewed as risk or high risk by the individuals and/or by ICO. Assessing privacy harm risks in the context of a DBI response would require a risk model that not only includes the privacy of data subjects but other impacted stakeholders. Privacy harm differs from the adverse impacts of security events as such impacts *may extend beyond the data subjects to relatives, friends or wider society* (Alshammari and Simpson, 2018)⁵.

Moreover, during initial DBI response, there is usually little available reliable breach information, and no formal procedures that address the GDPR breach notification timeframe i.e. report within 72 hours or without undue delay. Organisations may face fines and penalties for failure to comply with the GDPR breach notification requirements. Also, organisations (interviewees in the interview study) have expressed concerns about the notification timeframe of 72 hours to notify the ICO. Furthermore, DBI is nuanced and is a crisis event and existing incident response frameworks/procedures, including standards, are deemed not suitable (interview study). The interview study is described in Chapter 4.

Privacy harm research have primarily examined harm to data on devices or harm to organisations (e.g. Clarke, 2013; De and Le Métayer, 2016a; Williams et al., 2017). The legal concepts attached to privacy have been challenged for lack of theoretical grounding by Fuchs (2011). Although privacy and privacy harm are contextual, when there is a DBI, breach notifications to affected individuals are seen as the *right thing to do* (interview study). However, not all organisations report data breaches due to fear of harm to their reputation and consequently breach notifications are also avoided.

In the GDPR era, the urgency and impetus to notify affected individuals in a timely manner, viewed as important to minimise further likely data harm to the affected individuals, have raised breach notification fatigue concerns (e.g. ENISA (2011), Bolson (2014) and Esayas (2014)). This raised a prioritisation question that organisations need to address during initial DBI response: *to notify or not affected individuals and/or the ICO?* To prioritise whether to notify or not will require answering this: *How to assess data privacy harms for breach notification during initial DBI response?* To answer this question, this research's scope and aim was to explore DBI response, data privacy harms and breach notifications under the GDPR **(RA)**.

During initial exploration (i.e. literature review and interview study), a research gap was identified which led to a proposed solution and the formulation of the research question and objectives and sub-objectives. These are outlined next.

⁵ The authors cited Solove (2006).

1.4 Research question (RQ), aim (RA) and objectives (RO)

Research question (RQ): How can a triage playbook be used to address data privacy harms for breach notification prioritisation during the initial response to a personal data incident? To meet the RQ, a research objective (RO3) was to develop a triage solution. Figure 1-1, p 22 captures the research aim (RA), research question (RQ), research objectives and sub-objectives (RO), research activities and research contributions (RC).

Research Aim (RA)		
To explore personal data incident (DBI) response, data privacy harms and breach notifications under the GDPR.		
Research Question (RQ)		
<i>How can a triage playbook be used to address data privacy harms for breach notification prioritisation during the initial response to a personal data incident?</i>		
Research Objectives/Sub-Objectives (RO)	Research Activities and Contributions (RC)	
(RO1) To examine the underlying concepts/principles/theories/approaches or rationales that are applied in the construction/design of the incident frameworks.	Literature review (Chapter 2)	(RC-1)
(RO1-1) To synthesise existing incident frameworks/models or incident approaches.	Literature review (Chapter 2)	(RC-1)
(RO1-2) To apply Peirce semiotics-ternary for the triage steps.	Application of Peirce ternary (Chapter 3)	(RC-3)
(RO2) To gauge the extent and nature of personal data breach incident (DBI) responses by organisations in the UK.	Interview Study (Chapter 4)	(RC-1)
(RO3) To develop a triage playbook for organisations in the UK to assess data privacy harm (data harm) for breach notification during initial DBI response.	Design & Build Prototype Dashboard (Chapter 5) and 2 nd literature review	(RC-3) and (RC-4)
(RO3-1) To iteratively design and build the prototype dashboard (Dashboard) to address the initial breach notification question: <i>to notify or not affected individuals and/or the ICO?</i>	Design & Build Prototype Dashboard (Chapter 5)	(RC-1), (RC-2), (RC-3) and (RC-4)
(RO4) To validate the triage playbook using a prototype dashboard (Dashboard).	User Evaluation Study (UES) (Chapter 6)	(RC-1), (RC-2) and (RC-3)

Figure 1-1 Research aim (RA), question (RQ), objectives (RO), activities and contributions (RC)

The ROs were also framed as research objective questions (objective questions) to enable findings or the artefacts to be examined and analysed from the different research activities (i.e. literature review, the interview study, the triage solution construction and the user evaluation study). Perhaps rather surprisingly, the literature review using Systematic Scoping/Mapping technique (SSM) revealed that DBI response, data privacy harm and breach notifications were fairly new research fields (RO1). To explore and gauge the nature of DBI responses by organisations in the UK, an interview study was conducted (RO2). As there is little research on DBI responses, the semi-structured interview questions were improved after five interviews to capture the nuances of DBIs for addressing the exploratory nature and broad aim of interview study. This is shown in the interview scripts in Appendix I p 221 questions B 2), 3) and C 1) were merged to B 3) in Appendix J p 223.

As triage is used in digital forensics, but there is little literature for triage in DBI response, a synthesised triage entity in a tree diagram for DBI response (Triage DBI response) was created (Figure 2-11, p 61). Although triage appeared in a computer forensics model (CFFTPM), there are no clear operational triage steps. Hence a triage sequence of steps was formulated during the literature review.

Peirce semiotics and ternary (Peirce semiotics-ternary) was applied for the discovery and explanation of the triage steps in a visual diagram (Figure 3-4, p 70) (RO1-2). Peirce semiotics-ternary (Section 3.1.2) is a ternary system of sign relationship between a *representamen* (*Firstness*), an *object* (or *Secondness*) and an *interpretant* (*Thirdness*). An interview study was conducted (Chapter 4) which exposed that triage is used in industry but there are no formal or written triage procedures. Furthermore, DBI is considered a crisis and checklists are used to gather information to assess the nature of the data breach.

Although breach notification was seen as a *right thing to do*, organisations faced the daunting breach notification timeline of 72 hours under the GDPR (interview study). The GDPR also compels organisations to only report *risk* and/or *high-risk* breaches to the ICO, and to conduct a phased response (GDPR Article 33(4)). As there are no clear description for what constitutes risk or high risk to the rights and freedoms of individuals is, this research proposed a triage playbook solution to assess the impact of the data breach to affected individuals during initial DBI response.

The findings from the interview study and the synthesised Triage DBI response steps (Figure 2-11, p 61) were used to derive a conceptual triage playbook model (Figure 5-3, p 113). This framed the context for the construction or build of the triage playbook (RO3). This research designed a prototype dashboard to implement the triage playbook. Further details of the design and build are described in Chapter 5.

Then to ensure rigor and relevance (Design Science Research in Chapter 3) of the constructed artefact i.e. the prototype dashboard that implemented it, the dashboard was evaluated (RO4) with practitioners (User Evaluation Study). A set of evaluation questions (Figure 6-1, p 129) was used to validate (i.e. proof-of-concept and proof-of-use) the dashboard.

Although the RQ was explicated from motivation and interests that addressed a broad RA, the outcome of the RQ was to solve a practical business problem in the era of the GDPR. Besides, the identified problem also raised a relevant and meaningful RQ that contributed to the research domains as outlined in Section 1.7.

1.5 Research scope

This research falls under two disciplinary areas, extracted from Theoharidou and Gritazalis (2007):

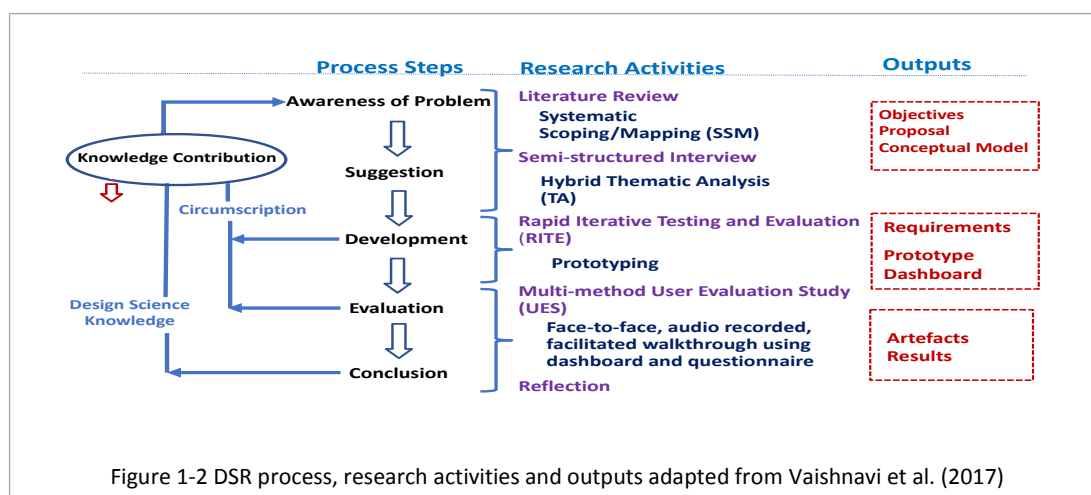
- Incidence Response in Business Management and Information Systems Security.
- Privacy and Ethics in Social, Ethical and Legal aspects of Security in Information Security.

This research examined privacy harm to affected individuals as a consequence of a DBI from the perspective of organisations who are held accountable for breach notifications under the GDPR. Hence the problems and the suggested triage playbook solution addressed in this research were directed to organisations. In this research, organisations are businesses or corporations or institutions in the UK. Organisations in the critical national infrastructure services industry (e.g. energy companies) and in the defence and national security are excluded. In particular, organisations based in/around London across industry sectors (the sample populations or demographics) were targeted. Because of time, resource and other practical constraints, London provided the base for conducting the interviews and the user evaluation study (UES).

In terms of legal compliance with personal data, the GDPR and the ICO guidelines provide the context for assessing personal data breach and breach notification. The UK context is stressed as data privacy laws differ in different territories or jurisdictions⁶.

1.6 Overview of methodology

The problems investigated in this research were directed at solving practical real-world problems i.e. data breach assessment and breach notifications as required under the GDPR. In addition, the research involved the construction of a design artefact. As described by Eze (2013), Design Science Research (**DSR**) provides systematic and rigorous methodology for producing novel research artefacts which can be building blocks towards solving both practical and theoretical Computer Science problems. The DSR framework by Vaishnavi et al. (2017)⁷ provided the lens for guiding, structuring and describing the various research activities (study and methods), processes and their outputs (Figure 1-2, p 24)⁸. As the DSR framework has inherent process and activity cycles to ensure *rigor and relevance* in conducting this research, this enhanced the validity of the research outputs/artefacts. Furthermore, such new artefacts are evaluated – a defining features of DSR – not just for how valid or reliable they are but also how well the artefacts perform (Hevner et al., 2004; McLaren and Buijs, 2011).



This research conducted the research activities (as shown in Figure 1-2, p 24): a systematic scoping/mapping literature review (**SSM**); a semi-structure interview study (**interview study**) with industry practitioners (**interviewees**); two prototype dashboards (**dashboards**) were designed and build (**D&B**) i.e. two iterative D&B with developer using **RITE** (Shirey et al., 2013); Figure 3-13, p 80. The dashboards – implemented the triage playbook – were used in a multi-method user evaluation study (**UES**) with two groups of different industry users (**Users**).

The outputs of the SSM and interview study, driven by the broad RA and the RO, informed and led to the proposal of a triage playbook. A triage conceptual model was constructed (Figure 5-3, p 113),

⁶ Post Brexit (UK voted in June 2016 to leave the EU), the GDPR is still relevant as indicated by the ICO in: <https://iconewsblog.wordpress.com/2016/07/07/gdpr-still-relevant-for-the-uk/> [Accessed 20-September-2016].

⁷ Their 2011 version was used by Wilson (2013). Piirainen et al. (2010) cited their 2004 version. Also, the authors claimed they have a combined 70+ years of DSR experience.

⁸ The DSR framework by Vaishnavi et al. (2017) is shown in Figure 3-6, p 74. The *Research Activities* and *Outputs* are specific to this research.

to show the dashboard solution and the interaction with the users or stakeholders. The requirements for the dashboard solution were elicited from the problems identified, the GDPR and the ICO guidelines for breach notifications (Chapter 5, Section 5.2).

The prototype dashboard provided a proof-of-concept and proof-of-use of the triage playbook (Nunamaker and Briggs, 2012). The UES used a multi-method evaluation approach involving users using the dashboard, a questionnaire in a face-to-face, audio recorded, facilitated walkthrough. Figure 6-2, p 131 shows a summary of the questionnaire and dashboard. The outputs from the UES were prepared, consolidated, analysed and synthesised using NVivo for the transcribed audio text files, Excel and MSD (Figure 6-4 p 138).

The underlying philosophy of this research was centered on Peirce's pragmatism and his semiotics-ternary of *Firstness*, *Secondness* and *Thirdness* (Lazanski and Kljajić, 2006; Everaert-Desmedt, 2011; Mingers and Willcocks, 2014). Peirce's pragmatism is a philosophical tradition that gives *emphasis to the link between action and truth, positing that the definitive test of knowledge is the readiness to act on it* (Nenonen et al., 2017). The DSR focus on practical problems is also centered on pragmatism (Vaishnavi et al., 2017).

Moreover, research artefacts are DSR knowledge that are manifested not only in *abstract design principles* but also *material instantiations* (e.g. prototype). At the same time, instantiation with *no or minimal contribution of abstract artefacts* is also a DSR knowledge contribution (Vaishnavi et al., 2017). Hence instantiation can also be included in an abstract design theory (Vaishnavi et al., 2017) such as in a pre-theory design framework (Baskerville and Vaishnavi, 2016). This then makes the prototype dashboard – an instantiation – of the triage playbook which then makes the playbook a DSR knowledge contribution.

In a widely cited paper by Nunamaker et al. (1990), on engineering and system research, *prototyping is used as a proof-of-concept to demonstrate feasibility in the life cycle: concept - development - impact*. They pointed out that the concept at issue has *wide-range of applicability* and *each stage of the life cycle obviously contributes to 'fuller scientific knowledge of the subject'*. This is because the developed system serves both as a proof-of-concept for the fundamental research and provides an artefact that becomes the focus of expanded and continuing research. Hence the prototype dashboard, developed iteratively, contributed subject domain knowledge.

1.7 Research contribution and knowledge

This research's novel contribution **(RC)** is expanding the knowledge of how triage, checklists and a data matrix can be used to support organisations in the UK to address privacy harm to affected individuals for prioritising breach notifications during the initial response to a personal data breach incident. The RC is broken down into the following facets:

(RC-1) This research advances understanding of data privacy (data) harm to the individual as a consequence of data breaches.

(RC-2) This research demonstrates a novel triage playbook for data harm assessment (PHA) to support quick breach notification (i.e. as required under the GDPR) during initial data incident response through a proof-of-concept and proof-of-use prototype dashboard.

(RC-3) This research illustrates the application of Peirce semiotics-ternary for contextualising the triage principles and the steps.

(RC-4) This research provides a pre-theory design playbook for initial data incident response through the use of checklists, triage principles (i.e. *first do no harm*), and a harm entities approach to data harm assessment.

The above RC are mapped to the RO as shown in Figure 1-1, p 22.

According to Vaishnavi et al. (2017) the *conclusion of a research effort needs to appropriately position the research being reported and make a strong case for its knowledge contribution*. This thesis is a form of reporting of the research effort.

Furthermore, the UES showcased and demonstrated (proof-of-use) the dashboard (artefacts) and validated through practitioners the proof-of-concept of the triage playbook. The findings from the UES indicated the dashboard was useful and also has the potential to be further developed for commercial use. As pointed out by Piirainen et al. (2010), the contribution of DSR research is twofold: *it results in new knowledge through refinement and use of existing theories, as well as in new artifacts that enable possibilities previously unavailable to practitioners*. Such *contributions to business or real-world application environment* are stated by Hevner et al. (2004) and restated by Gregor and Hevner (2013).

Furthermore, the pre-theory design framework by Baskerville and Vaishnavi (2016) was used to show the knowledge contribution in the triage playbook which is composed of artefacts (Figure 3-11, p 77). This was based on the inherent pragmatism that underlies this statement by Vaishnavi et al. (2017): *an interesting partial or even an incomplete design theory is also a possible knowledge contribution with potential for further work*.

As the triage playbook was conceptualised (abstracted) from multiple sources of knowledge, this may be an *abstracting concepts* pattern under the list of *generalisation type patterns*. Such *patterns are useful in making significant research contribution* (Vaishnavi and Kuechler, 2015, p 249).

Also, the *knowledge forms and types* in Johannesson and Perjons (2014, p 21-28) were referenced to describe the types of knowledge for the outcome of this research. The descriptions of the *knowledge forms and types* were interpreted by this researcher and hence form a *good enough* (Vaishnavi et al., 2017) description of *these knowledge forms and types*. The *knowledge forms and types* were analysed and are shown in Appendix A p 209, and also the extracted DSR knowledge base (useful knowledge) provided by Gregor and Hevner (2013).

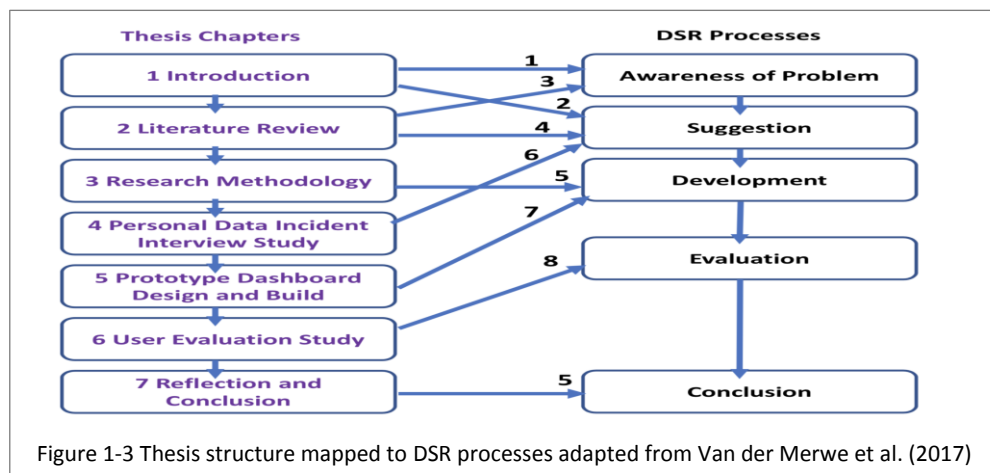
The outcome of this research has commercial and practical use. The collection of sources that been referenced or interest shown in this research's outputs:

- (1) The triage semiotics sequence of steps – i.e. Verify, Assess, Prioritise – was referenced by a practitioner at a conference in London (Conference, April 2017).
- (2) A UES user and another MD of their company have initiated a dialogue with this researcher to expand the dashboard to add to their GDPR products/services (Email, February 2018).
- (3) A Dutch DPO has expressed interests via Twitter with this request: *'You referred to your PhD research as a tool to decide whether or not to notify a data breach? I'm interested. Where can I find that?'* (DPO, July 2018).

The referenced sources are in Appendix B p 210.

1.8 Thesis structure

This thesis is organised in chapters as shown in Figure 1-3 p 27. The list of references and the appendices are presented after Chapter 7. There are two sections for all tables, figures and screenshots (figures) in this thesis. Figures in the chapters are listed under List of Diagrams. Figures in the appendices are in List of Diagrams in Appendices. Figure 1-3 p 27 shows the thesis structure mapped onto the DSR process model outlined in the DSR Framework in Figure 1-2 p 24. This thesis *structure mapping* is recommended by Van der Merwe et al. (2017)⁹ to document the research to support the research contribution.



Chapter 1: Provides description of the basic terminologies and structure of this report; introduces the motivation and the identified problems; outlines the research aim, objectives, question and the methods for achieving the research aim; provides the scope; provides an overview of the research methodology; and describes the research contribution.

Chapter 2: Describes the Systematic Scoping/Mapping technique (**SSM**) for the literature review; reports the reviewed literature on the research issues; outlines the synthesised triage entities for DBI response from the reviewed literature; and proposes an interview study to explore the extent and nature of DBI responses by organisations in the UK.

Chapter 3: Outlines the DSR framework (Vaishnavi et al., 2017) used in this research; shows the iterative nature of the DSR activities and their corresponding high-level processes i.e. the research study methods and their outputs (Figure 3-7 p 75); shows the process flow executed in terms of DSR activities and their artefacts/outputs (Figure 3-8 p 75); describes the application of DSR; describes the RITE process (Figure 3-12 p 80); shows the rigor and relevance of the two iterations of design and build (D&B) and UES of two prototype dashboards; shows the designing and prototyping steps (Figure 3-13 p 80), with the developer; discusses the research theory that underpins this research, i.e. Peirce semiotics-ternary and also pragmatism in DSR; applies Peirce semiotics-ternary for the triage steps (Triage Semiotics, Section 3.1.2.1); justifies the triage playbook as a pre-theory design artefact (Figure 3-11 p 77), based on a DSR

⁹ The authors use the DSR framework and process model from Vaishnavi et al. (2017).

pre-theory design framework. The triage playbook is composed of the formulated and conceptualised triage steps, checklists and the data harm matrix.

Chapter 4: Contains the detailed description of the interview study approach; outlines the interview study aim and the explanatory questions; describes the hybrid TA approach that was used for analysis and synthesis of the results; reports the interview findings; proposes a triage playbook solution for the identified problems and suggests a prototype dashboard to implement the triage playbook for proof-of-concept and proof-of-use.

Chapter 5: Describes and executes the design and build of the prototype dashboard with developers; shows the triage playbook components; shows the initial conceptual model; shows the tentative formulation and describes the dashboard requirements; applies Peirce semiotics-ternary for illustrating the design and solution space; discusses the dashboard design aim and design guidelines; documents the design and build (D&B) with the developers i.e. one developer for the mockups and another developer for D&B of the two dashboards (i.e. DashboardV1 and DashboardV2).

Chapter 6: Contains the detailed description of the two UES with users; outlines the objectives of the UES; describes and justifies the UES multi-method evaluation approach i.e. facilitated, walkthrough face-to-face interactions with two groups of users, the use of questionnaire (Qualtrics), the dashboard and audio recorded walkthrough; explains the questionnaire design; shows a summary view of the dashboard and the questionnaire; describes the facilitated walkthrough techniques; outlines and describes the data preparation and synthesis approach (included NVivo) for the three outputs i.e. dashboard, questionnaire and the transcribed interviews; describes the charts from the questionnaire results; describes using scenario and storytelling for the synthesised dashboard, questionnaire and transcripts results.

Chapter 7: Discusses the reflection and conclusion. Besides the reflection on the research question, findings, contributions, limitations and assumptions, this researcher's personal reflections are also expressed. Implications for practice and suggestions for further research provide the final conclusion.

Chapter 2 Literature Review

Traditional narrative literature reviews typically present research findings relating to a topic of interest; the activities are to digest, sift, classify and synthesise the information (Evans and Kowanko, 2000; Cooper and Hedges, 2009). Mohammad et al. (2012) highlighted that these traditional or ad hoc review activities are not standardised or structured in any coherent or systematic or scientific way. Furthermore, Gough et al. (2012) pointed out that the aim of reviewing systematically is to have explicit, rigorous and accountable methods so that it is possible to interpret the meaning of the review findings.

In software engineering, the Systematic Literature Review (**SLR**) or systematic review (Zhang and Ali Babar, 2013) approach is a systematic, transparent, and rigorous approach that has been used by researchers in the software engineering fields such as Zhang et al. (2011), Fernández-Alemán et al. (2013) and House et al. (2014). Although SLR also has several drawbacks, the main one being the considerable effort (i.e. involving the use of statistical meta-analysis) required, it has several benefits due to its well-defined methodology which reduces bias, a wider range of situations and contexts that can allow more general conclusions (Petersen et al., 2008). Moreover, the Systematic Scoping/Mapping technique (SSM), a *light* version of the SLR is suitable for PhD researchers (Kitchenham and Charters, 2007; Budgen et al., 2008). SSM does not cover details of meta-analysis nor does it discuss the implications that different types of systematic review questions have on research procedures.

2.1 Systematic Scoping/Mapping technique (SSM), objectives and questions

SSM offers features of SLR such as the visual systematic mapping for summarising and presenting the results (Petersen et al., 2008; Barbosa and Alves, 2011; Kitchenham et al., 2011). Kitchenham and Charters (2007) on SSM: *designed to provide a wide overview of a research area, to establish if research evidence exists on a topic and provide an indication of the quantity of the evidence*. Budgen et al. (2008) pointed out that SSM forms a useful preliminary step for PhD study as it *provides a systematic and objective procedure for identifying the nature and extent of the empirical study data, and gaps to be identified and highlighted*. In essence SSM is done without the synthesis step in SLR and often addressing a broad area or phenomenon rather than a more specific research question (Wohlin et al., 2013) and to identify gaps in the set of primary studies (Barreiros et al., 2011). As the aim and themes of this research are broad, SSM is a useful and systematic approach (Kitchenham et al., 2011). In particular, the SSM techniques described by Petersen et al. (2008) were used for the initial literature review driven by the research objective (RO1). Although Kitchenham and Charters (2007) is widely cited in software engineering SLR and SSM studies, the SSM techniques described by Petersen et al. (2008) are most commonly followed.

As pointed out by Petersen et al. (2015), the review process is iterative and may require revisions. This iterative approach aligns with the DSR (Figure 3-8 p 75), whereby a second literature review/search was done following the interview study. The second search¹⁰ was taken to identify any new studies or literature on the proposed triage solution. This was similar to the SLR approach taken by Tøndel et al. (2014). The SSM literature review was to address RO1. To answer RO1, the following SSM objectives were

¹⁰ E.g. focused search on GDPR breach notification, checklists, prototype dashboard and DSR. These references were reported in the relevant sections and chapters.

driven by the SSM questions as shown in Figure 2-1 p 30. The following sections describe the executed SSM steps.

SSM objectives	SSM questions
(RO1) To examine the underlying concepts/principles/theories/approaches or rationales that are applied in the construction/design of the incident frameworks	(RO1-a) What constitutes a personal data breach incident (DBI) and breach notification under the GDPR? (RO1-b) How to assess data privacy harm (data harm) for breach notification? (RO1-c) What are the characteristics of existing incident response frameworks? (RO1-d) What is triage and how does it work? (RO1-e) What visual methodologies or approaches or theories (methods) provide meaningful and practical support for triage processes? What did the SSM studies reveal?
(RO1-1) To synthesise existing incident frameworks/models or incident approaches.	

Figure 2-1 SSM objectives and questions

2.1.1 SSM steps and execution

Petersen et al. (2008) state that SSM steps are: *Defining research questions; Conducting the search for primary studies; Screening papers based on inclusion/exclusion criteria; Classifying the papers; Data extraction and aggregation*. The SSM steps were organised into three review processes i.e. Plan Review, Conduct Review and Document Review and their activities, as shown in Figure 2-2 p 30.

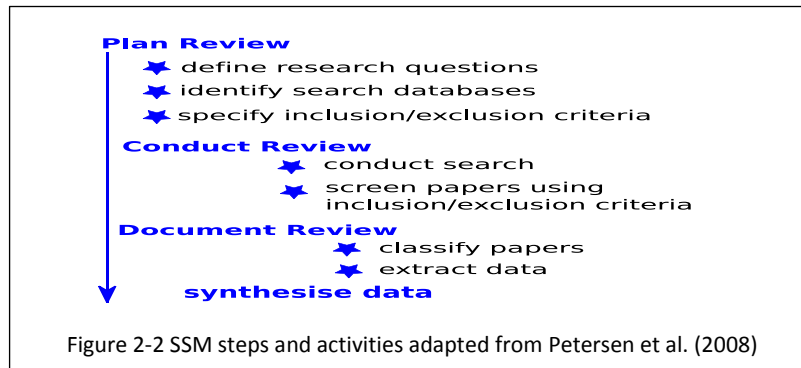


Figure 2-2 SSM steps and activities adapted from Petersen et al. (2008)

The final step that is normally omitted under SSM, namely, *synthesis of the extracted data (synthesise data)* was conducted to identify a potential incident response framework from the SSM studies (RO1-1).

2.1.1.1 Plan review

The SSM objectives and questions as outlined in Figure 2-1 p 30 drove this literature review study. Although the search requirements are less stringent in SSM (Petersen et al., 2015), the recommendation by Kitchenham et al. (2010) is to select databases of interest when searching the databases. For example, Appendix C p 211 shows a snapshot of the first search results and the document reviews are in Appendix D p 213. Initial searching for peer-reviewed literature was done using multi-contextual title, abstract and

keyword searches. The three well-known databases: IEEE Xplore, ACM, and Scopus¹¹, and also ScienceDirect, were used alongside LexisNexis and HeinOnline. Other sources¹² were also referenced to obtain the latest developments. The scoping and keywords (i.e. the inclusion/exclusion criteria) are shown in Appendix C, Figure C- 1 p 211.

2.1.1.2 Conduct review

Literature where the keywords do not appear in the abstract and/or title were excluded for reviewing and for conducting the data extraction. Besides the relevance of the topic of the article, the time period (i.e. from year available up to 2016¹³), venue (i.e. UK, EU and US) and also language (i.e. English language) of the publication were also included together with the criteria for inclusion/exclusion (Petersen et al., 2015). To organise and keep track of the literature searches, Freemind maps were used to record the paths of various entries retrieved for the keywords. Each path leading from the node/keyword shows the combined number of search entries for those keywords. In fact, *bubble and tree-like* diagrams shown in Appendix C p 211 are Freemind maps, showing the collection of articles retrieved using the specified keywords.

As a concept or theme, *personal data incident response* has yet to surface in (UK) PhD theses (Figure C- 3 p 212) and in key databases (Figure C- 2 p 211), unlike the concept of *computer security incident response*, which has become widely accepted and implemented (Cichonski et al., 2012). Hence computer security incidents, including digital forensics, were searched for incident lifecycle and/or incident frameworks.

During the **Conduct Review** activities (searching and screening), text or phrases or contents or stories covering or touching on the research aim were captured into Zotero. The search results were organised using Freemind maps as shown in Appendix C p 211.

2.1.1.3 Document review

A snapshot of a result from the **Document Review** activities is shown in Appendix D, Figure D- 1 p 213.

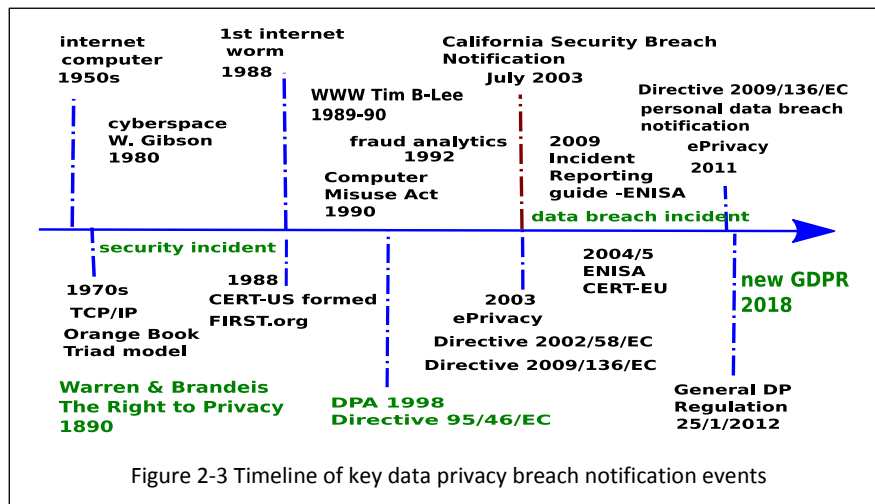
2.1.1.4 Synthesise data

A timeline of key events (key privacy related events are shown in **green**) was synthesised as shown in Figure 2-3 p 32, which further enhanced the search include/exclude criteria as well as article extraction and analysis. For instance, in extracting data for synthesis of articles on data privacy and breach notification, significant years are from 2003 (i.e. ePrivacy regulation) and 2011 (i.e. breach notification regulation).

¹¹ Dyba et al. (2007) and Kitchenham and Brereton (2013) recommended the use of IEEE and ACM as well as indexing databases e.g. Inspec/Compendex and/or Scopus as sufficient.

¹² Sources: ENISA.europa.eu, ICO.org.uk, SEI-CMU, CERT.org, FIRST.org, Google Scholar, Academia.net, Researchgate.net, events and conferences.

¹³ Initial literature search was up to 2016. Further literature search was done in 2018 and up to 18th January 2019.



2.2 Background and related work

The remaining sections in this chapter describe the findings driven by the questions as listed in Figure 2-1 p 30. A brief history of data breaches and a sketch of the GDPR and the EU data laws are outlined for research background context.

2.2.1 A brief history of data breaches

There is a history of data security breaches. According to the computerhistory.org site the *Morris Worm*¹⁴ was the first worm to have a major effect on real-world computer systems. This computer or internet worm incident was first analysed by Spafford (1989). An aftermath of this internet incident (Martins et al., 2019) was the establishment of a CERT¹⁵ Coordination Center (**CERT/CC**) by the US Defense Advanced Research Projects Agency (DARPA) at the Software Engineering Institute (SEI) of Carnegie Mellon University (CMU), Pittsburgh (**SEI-CMU**). The aim of CERT/CC was to provide the Internet community with a single organisation that can coordinate responses to security incidents on the Internet (Howard, 1997). At organisation levels, the acronym CSIRT¹⁶ for Computer Security Incident Response Team is commonly used in discussions on CERT and incident management.

Not long after the creation of CERT/CC, an international confederation of trusted computer incident response teams was set-up, known as FIRST¹⁷. Although these two organisations and ENISA provided the primary coverage in terms of industry practitioners' research activities/publications in the broad incident management fields, other industry solutions and service providers were also referenced. As shown by the historical data incident events¹⁸ that triggered government and industry led initiatives,

¹⁴ The Morris Worm listed in <http://www.computerhistory.org/timeline/1988/> [Accessed 29-December-2018].

¹⁵ As the CERT® is registered in the US Patent and Trademark Office by Carnegie Mellon University, all references to CERT include the ® symbol: <http://www.sei.cmu.edu/legal/marks/index.cfm> [Accessed 29-December-2018].

¹⁶ CERT and CSIRT are now used interchangeably.

¹⁷ Forum of Incident Response and Security Teams (FIRST): <https://www.first.org/about/history> [Accessed 29-December-2018].

¹⁸ Similar to the establishment of CERT/CC, in October 1989, a major incident called the 'Wank worm' highlighted the need for better communication and coordination between teams. FIRST was formed in 1990 in response to this problem: <https://www.first.org/about/history> [Accessed 29-December-2018].

practitioners in the fields have also chronicled and discussed the ever changing data breach incidents landscape¹⁹.

In the UK the ICO has a website²⁰ to show trends for data breaches. In examining the data breach incidents landscape, one has to note that the majority of data breaches go undetected for 160-240 days as cited by Densham (2015). It is worth pointing out that not all DBIs are reported. This may be because in genuine cases organisations do not know they have a DBI, and if they do know, disclosure is withheld to avoid the unintended legal and non-legal consequences of DBI disclosure. Campbell et al. (2003) investigated the economic cost of information security breaches which revealed that the majority of organisations are reluctant to report breaches for fear of market reprisal. Also, although CERT and FIRST address security-related incidents there appears to be little literature and few conferences on DBIs at the time of writing this thesis. However, Dsouza (2018) highlighted that cybersecurity incidents can have severe consequences for individuals e.g. the devastating psychological effects associated with the leak of Ashley Madison customer details.

2.2.2 GDPR and EU data landscape

Data breach notification is not new in the EU. Since 2013, Internet Service Providers (ISPs) or telecommunication providers (telco) are required to notify affected subscribers/individuals when personal data is breached under the EU Electronic Privacy Directive (**ePrivacy**) Directive²¹. The ePrivacy Directive was amended by the Directive 2009/136/EC which introduces breach notification obligations under Article 4(2) and Article 4(3). However, this Directive will be replaced/repealed by the ePrivacy Regulation (**ePR**)²². There are also the Network and Information Security (**NIS**)²³ Directive, and the Regulation on electronic identification and trust services (**eIDAS**)²⁴, all imposing data breach notification on organisations. The NIS Directive (aka cybersecurity Directive) imposes data breach notification on *market operators* or *critical infrastructure operators*²⁵, whereas the eIDAS Regulation imposes data breach notification on *trust service providers*²⁶.

Essentially any organisations processing personal data of data subjects who are in the EU will need to notify the individuals whose personal data have been compromised or breached as required under the ePR or NIS or eIDAS or GDPR. For example, PayPal may be required under the GDPR, the NIS, and the eIDAS to serve a notice of breach. The relevant data supervisory authority, for example in the UK, it is the

¹⁹ Some links are listed on this researcher's blog at: <http://jollyvip.com/research/> [Accessed 29-December-2018].

²⁰ <https://ico.org.uk/action-weve-taken/data-security-incident-trends/> [Accessed 29-December-2018].

²¹ ePrivacy Directive - Directive 2002/58, of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37 (EC).

²² On 10 July 2018, the Council of the European Union has published a draft revision to the proposed ePrivacy Regulation (ePR). The ePR is likely to come into force in 2019 and is not examined.

²³ NIS - Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union 2, COM (2013) 48 final (Feb. 7, 2013).

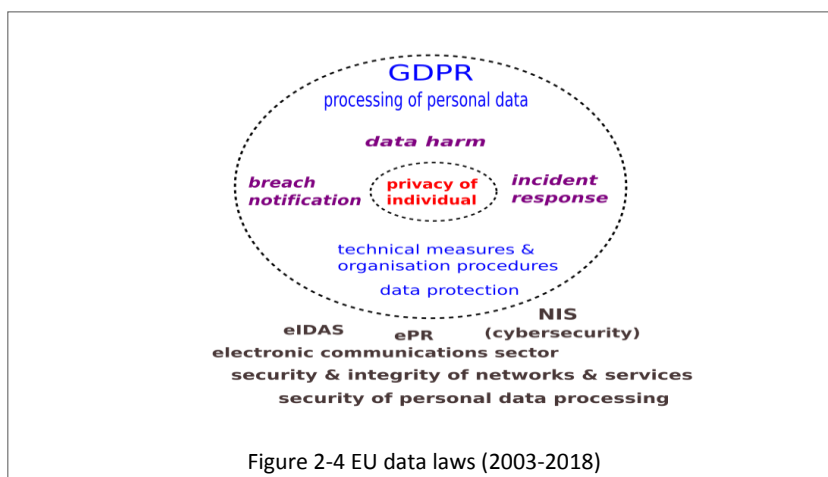
²⁴ eIDAS - Regulation 910/2014, of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC, 2014 O.J. (L.257) 73 (EU).

²⁵ In the NIS, the critical infrastructure operators are financial, health, and transport service providers.

²⁶ In the eIDAS, the trust providers are telecoms service providers, financial institutions, or any organisations involved in electronic identification and trust services, including universities.

ICO, will also need to be notified of the DBI. Depending on the type or **nature of the organisation** and also the **nature of the security breach**, other authorities will also need to be notified e.g. the national law enforcement or security authorities. These EU data protection and privacy related Regulations and Directives (**EU data laws**) are complex, with strict breach notification criteria and requirements that are difficult to navigate and comply with. Speakers at a BCS event expressed that GDPR is complex for organisations to comply with²⁷.

Figure 2-4 p 34 sketches the EU data laws that have provision for personal data breach notification, and the circle to show GDPR i.e. the context for this research in terms of breach notification. The GDPR circle in Figure 2-4 p 34 also highlights the identified topics/themes (i.e. data harm, breach notification and incident response) investigated in this research. In essence GDPR is at the core of all the EU data-related laws for the protection of privacy or data privacy of individuals through the *processing of personal data*. Hence, it is the future *DNA of EU privacy law* (Schwartz and Peifer, 2017). The GDPR widens the scope on processing of personal data of *data subjects who are in the Union by a controller or processor not established in the Union* (GDPR Article 3(2)). In data-linked cyberspace, this makes GDPR difficult to navigate when faced with a DBI.



2.2.3 What constitutes a DBI and breach notification under the GDPR? (RO1-a)

Although Howard and Gulyas' (2014) description for personal record and data loss incident is generic in an organisational setting, the GDPR Article 4(12) description for personal data breach incident (DBI) – *personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed* – serves as the main reference for breach notification and privacy harm. Furthermore Howard and Gulyas (2014) did not examine privacy harm and breach notification and also the concept *personal data incident* is not yet a research theme (as shown by the search results in Appendix C, Figure C- 2 p 211 and Figure C- 3 p 212).

Besides the conceptual, contextual issues with *personal data*, there is no universal definition of *incident* and incidents can be of many types and come from many sources (David, 2003). According to Salomon and Elsa (2004), security spans a wide range of activity *covering design and engineering, across*

²⁷ BCS ISSG 17th Annual Legal Day on 22 January 2016, London.

daily operations, to theoretical risk management and policy-making. As such, activities associated with DBI such as breach notifications and privacy harm assessment (PHA) in organisations will also span across these areas. Furthermore, PIA and breach notifications are new concepts (Custers et al., 2018). As regards breach notification and incident response, ENISA uses the term *reporting* for *reporting incident to relevant data authorities*, and *notification* is for *notification to individuals/consumers* (Dekker et al., 2012). In this research, the term **notification** is used to report the incident and to notify the individuals.

2.2.3.1 GDPR: beyond the data principles

The data principles in GDPR constitute the *rules* of the game for data breach determination, and with the new accountability principle (Article 5(2)) this raises the bar on the protection and the processing of data. Most interestingly it also changes the rules of the game for breach notifications and data privacy or the privacy rights of the data subjects (individuals).

Although the GDPR did not introduce any new data protection principles (data principles), it brought in accountability principles and introduced a phased approach for breach notifications. There is also the transparency principle (GDPR Recital 58) for individuals to exercise their rights²⁸. In terms of data breaches and notifications, the accountability and transparency principles were examined as there is no *right to know* or *right to be informed*²⁹ of the data breaches. Instead, the accountability principle applies to breach notifications. The GDPR accountability principle applies to data controllers and processors and includes the need to *demonstrate data compliance*³⁰.

As highlighted in the ICO guide on the GDPR (ICO, 2018), the accountability principle *specifically requires organisations to take responsibility for complying with the principles, and to have appropriate processes and records in place to demonstrate that you comply*. This is a *catch-all* GDPR principle which extends beyond the data principles. Organisations in breach of the data principles are held accountable with fines and other penalties. *What are the data principles?* Figure 2-5 p 36 is extracted from the ICO (2018) which shows the six GDPR principles against the DPA 1998³¹. The transparency principle is added to principle (a). When an incident occurs and principle (f) is breached, this is a security breach. If the security breach involves *personal data* it is also a personal data breach. If principle (f) (security) is not breached but it breaches any of the other data principles and it involves personal data, it is a *personal data breach*.

Hence a security breach is different from a personal data breach (DB), also noted by ENISA (2012). The description for DB is as follows: *a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed* (GDPR Article 4(12)). This means that if *personal data* is not protected/secured (breach of

²⁸ These rights are not principles-driven and hence are subject to other competing rights.

²⁹ E.g. a *subject data request* – an individual exercising the *right to be informed* (transparency principle).

³⁰ The *processor* also needs to demonstrate consent – a burden placed on the *controller* Article 12(5). The boundaries of responsibilities/accountabilities are blurry in the processing of data in cyberspace. Hence *joint controllers* specified in Article 26.

³¹ This is now repealed by the UK DPA 2018 which also has the six data protection principles. Hence the ICO mapping of the UK DPA 1998 reflects the DPA 2018 data principles.

security) and results in the personal data being compromised (i.e. loss, alteration etc.³²), it is a personal data breach.

What's new under the GDPR?	
The principles are broadly similar to the principles in the Data Protection Act 1998 (the 1998 Act).	
1998 Act:	GDPR:
Principle 1 – fair and lawful	Principle (a) – lawfulness, fairness and transparency
Principle 2 – purposes	Principle (b) – purpose limitation
Principle 3 – adequacy	Principle (c) – data minimisation
Principle 4 – accuracy	Principle (d) – accuracy
Principle 5 – retention	Principle (e) – storage limitation
Principle 6 – rights	No principle – separate provisions in Chapter III
Principle 7 – security	Principle (f) – integrity and confidentiality
Principle 8 – international transfers	No principle – separate provisions in Chapter V
(no equivalent)	Accountability principle

Figure 2-5 GDPR Data Principles (ICO, 2018)

The DB description tried to describe the data principles focusing on the data incidents. As data incidents are nuanced, the DB description should be read as *an example of a security breach*. A notable change is that *rights* of the individuals are not principle-based. This signals and raises the bar on *rights and freedoms of natural persons which is protected under the accountability principle i.e. a catch-all principle*.

Although security breach³³ is outside the scope of breach notifications³⁴, the scope of what constitutes a data breach that requires notification also needs to address the security of the data. Hence, data breach notifications reinforce another fundamental principle of data privacy, which is the principle of data security (Esayas, 2014). The breach notification to individuals is triggered *when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons* (GDPR Article 34(1)) and only if the organisation has not *implemented appropriate technical and organisational protection measures, and those measures were not applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption*³⁵. The security protection principles (Howard, 1997) are *confidentiality, integrity and availability (CIA)*³⁶. *Confidentiality* falls under GDPR data principles (a), (b) and (f); *integrity* is (c), (d) and (f); *availability* is (a), (d), (e) and (f). *Availability* now needs to cover a wider spectrum of *rights of data subjects*³⁷. *Confidentiality* now needs to address transparency principles. The GDPR makes

³² GDPR Article 32(2) i.e. level of security risks and data principles (d) & (f).

³³ i.e. in breach of principle (f).

³⁴ *In the case of personal data breach...* (GDPR Article 33) & *When the personal data breach is likely ...*(Article 34).

³⁵ GDPR Article 34(3) (a) and also (b) & (c).

³⁶ *Confidentiality* requires that information be accessible only to those authorised for it, *integrity* requires that information remain unaltered by accidents or malicious attempts, and *availability* means that the computer system remains working without degradation of access and provides resources to authorised users when they need it.

³⁷ GDPR Article 12-23. E.g. new rights - data portability, right to erasure & automatic processing right. Note: Data minimisation is a principle.

the balancing of *rights of data subjects* in the realms of *processing of personal data* a complicated act. The GDPR *rights of data subjects* are not absolute including the *right to privacy*.

With the introduction of accountability principle³⁸ and the need to address the *rights and freedoms of natural persons (right to privacy)*, the data security principles will need to go beyond CIA to include new paradigms outside the data security protection domains. Besides, preventative actions are not sufficient, and an incident management capability is therefore necessary (Hove and Tårnes, 2013). As noted by Schneier (2014) incident response starts with *people to take the necessary actions, and this decade is one of response*.

2.2.3.2 Breach notification and notification fatigue

Esayas (2014) in examining the data breach notification rules in the various EU data laws, pointed out that besides the administrative and financial burdens of such compliance, it is not always easy for an organisation to determine when a breach is considered to have occurred, whether the breach affects personal data, and whether the conditions for notifying the authorities and the individual have been fulfilled. Responding to a data breach incident is not something that can be ignored by organisations where data and/or the processing of personal data are protected by law e.g. the GDPR.

In major countries around the world, notably in the EU, in the US, Australia and Canada (Burdon et al., 2012) there are laws requiring organisations to report or notify data breaches to the relevant stakeholders, including data authorities/agencies. As raised in Bergman and Verlet (2006), even without breach notification law within the data subject's jurisdiction, there may be other reasons why organisations will choose to notify. Besides, organisations will be unable to simply brush data protection breaches under the carpet, as the penalties for doing so, or attempting to do so, will be damaging. They will have to declare them (Pearlgood, 2012) by notifying the affected individuals especially the *higher the risk of damage or distress*, the more appropriate it will be to report (Caldwell, 2012).

Breach notification law, in compelling organisations to provide notice of a breach, is a specific example of regulation through disclosure which is associated with the communities' *right to know* – developed from environment laws. Organisations need to be transparent – transparency principles – when they have a DBI and to notify affected individuals as they have *the right to know*. The *right to know* is a phrase used by researchers e.g. Maurushat (2009) and Daly (2018) to describe data breach notification laws that require organisations to notify individuals when a breach of security leads to the disclosure of personal information. In essence, breach notification laws enact the transparency principles with the *right to know of data breaches*. Such transparency is the *prerequisite for enabling affected individuals to take appropriate steps to protect themselves against malicious impacts resulting from a breach* (Muntermann and Roßnagel, 2009). Furthermore, the *right to know* may raise data breach *notification fatigue* issues. Notification fatigue issues have been highlighted by BEUC (2011), ENISA (2011) and Esayas (2014).

³⁸ Accountability is one of the eight principles espoused by The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data:
<http://www.oecd.org/internet/ieconomy/oecdguidelinesonthe protection of privacy and transborder flows of personal data.htm> [Accessed 29-December-2018].

Businesses in the US have complained about the burdens and inefficiency of complying with the patchwork of laws including the data breach notification laws (Hardy 2014, p 20). In the US data breach notification laws have been in place since 2003. Also, indiscriminate general breach notification obligations are recognised as an administrative burden on organisations in the EU (Danagher, 2012; Esayas, 2014). One approach – from the EU policy makers – to avoid indiscriminate general data breach notification and hence prevent notification fatigue, is: *To prevent notification fatigue to data subjects, only in cases where a data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, for example in cases of identity theft or fraud, financial loss, physical harm, significant humiliation or damage to reputation, should the data subject be notified* (Albrecht, 2012). This is translated into GDPR Article 34(3) which stipulates the conditions under which breach notification to individuals is not required. In security terms³⁹, Daly (2018) pointed out that if the compromised data is *unsecured* or unprotected such that it has not been rendered *unusable, unreadable or indecipherable* to unauthorised individuals, notifications to affected individuals are needed. However, in privacy harm avoidance terms, GDPR Article 34(3)(b) offered this: *the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1⁴⁰ is no longer likely to materialise*. This is interpreted as: to notify the affected individuals without undue delay and to avoid notification fatigue, only those data incidents that are likely to be *high risk to the rights and freedoms of data subjects* need to be notified. **This then requires assessment of the impact of the data incidents in terms of data privacy harm to the affected individuals.**

As noted by Rotenberg and Jacobs (2013), *timely* notification can allow individuals *to take significant steps to reduce potential personal harm*. This is because when a DBI happened, the genie was out of the bottle out in the wild, the harm was already done. According to Holm and Mackenzie (2014) any notification of breach must be timely to be effective, given the *speed in which misuse of data* can take place.

Public opinion/sentiment (US) on the aftermath of a data breach has been surveyed by the Ponemon Institute (2014). Bolson (2014) observed that the data notifications themselves and the laws that mandate them may be contributing to data breach fatigue. ENISA (2011) suggests that breaches should be categorised according to specific risk levels to prevent notification fatigue. The rationale is that the seriousness of a breach should determine the level of response. However, like any crisis incident that needs to be coordinated and managed, organisations need to handle and coordinate the response activities in such a way that establishing the seriousness of a breach can be performed using processes or frameworks that can be communicated and acted upon in a timely manner. Hove and Tårnes (2013) conducted an empirical study on how organisations perform information security incident management in practice. Amongst the issues identified was the poor communication and collaboration between the incident response team and teams from other organisational areas during the incident handling processes

³⁹GDPR Article 34(3)(a): The controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption.

⁴⁰ GDPR Article 34(1): *When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.*

(see also Tøndel et al. (2014)). Salomon and Elsa (2004) emphasised that even assuming efficient processes and good communication, the sheer scale of many corporate security organisations makes effective and timely security countermeasures difficult.

2.2.4 How to assess data harm for breach notification? (RO1-b)

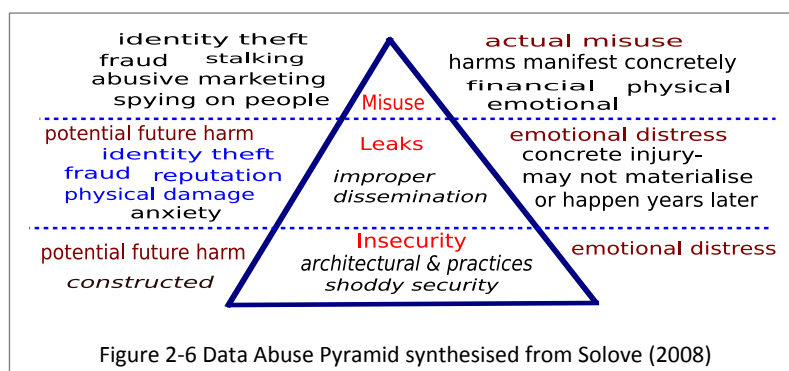
Discussion around data privacy invariably touches on the nebulous concept of privacy. Privacy is contextual (Nissenbaum, 2004) and the *differing definitions* of privacy makes discussions of privacy *more complicated* (Haynes, 2015). Back in 1990, in its first report on privacy in the UK, Calcutt (1990) reported: *nowhere have we found a wholly satisfactory statutory definition of privacy*. This led to a privacy definition: *The right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information*. Although privacy or data privacy is not defined in GDPR, this is embedded under *rights and freedoms of natural persons (i.e. a right to privacy)*. As pointed out by Bygrave (1998)⁴¹, the basic principles of data protection laws *may be read into provisions in human rights treaties proclaiming a right to privacy*. The European Convention of Human Rights – an international treaty – grants the individual a *right to respect for his private and family life* (Article 8) and this is enshrined into the GDPR as expression of privacy principles (Schwartz and Peifer, 2017). Such a *right to privacy* is enshrined in the *catch-all* accountability principle. Organisations are accountable for breach of any of the data protection principles including the *rights and freedoms of natural persons*.

Businesses and societies i.e. organisations that are in constant digital connectivity have such complex interconnection of issues touching on multiple interacting layers – *standards, infrastructure, data and derived knowledge*. These interconnected issues have outpaced the adaptive ability of the world's *governance response* (World Economic Forum, 2014, p 4, p 40). Although accountability principles have appeared in IT governance standards and frameworks, and also in a privacy framework – ISO/IEC 29100:2011 – these standards and frameworks for addressing the processing of personal data appears not to be widely used or referenced in existing literature or by industry. Moreover, Calder and Moir (2009, p 97) commented on the ISO/IEC 38500:2008 - *IT Governance* that while it provides guidance for boards, it does not help organisations simultaneously to deploy any of the other standards or frameworks. Standards in the interlinked business relationships or *data relationships* (Sir Tim Berners-Lee in TED.com (2009)) are insufficient. Complex business and data relationships were examined by Bonner (2012) with the focus on data privacy. Bonner (2012) points out that there is general lack of transparency surrounding most organisations and the need to re-examine the data privacy perspectives of the various parties (reinforced by Goodman and Lin, 2007, p 164, and the ethical aspects of the inter-relationship exchanges. Examining such inter-relationship exchanges in organisations is complex, involving conflicting and competing regulatory requirements and business objectives. This is so under the EU data law landscape especially with GDPR.

⁴¹ Examined two human rights treaties (Art 17 of the International Covenant on Civil and Political Rights (ICCPR) and Art 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)) and basic principles of data protection laws.

2.2.4.1 On privacy harm

To date, there is privacy harm related literature, but these are primarily written by legal scholars and are mostly US-driven. For example, two notable legal authors on privacy harm are Professor Daniel Solove (Solove) and Professor Ryan Calo (Calo). Similar to the pyramid structure as outlined in *The Pyramid of Pain*⁴² (from a security aspects), Solove has developed a *data abuse pyramid* (data loss and privacy aspects) with which to think about information abuses, the causes and the way they should be remedied (Solove, 2008). The *data abuse pyramid* has been also used by Budak et al. (2013) for a data protection survey on both public and private sector practices in Croatia. The limitation of the *data abuse pyramid* is that: *the pyramid is meant to be a rather simple model, and it is not designed to represent all information abuses* (Solove, 2008). Although Solove's (2008) data abuse pyramid is structured primarily on the US legal system, it discusses (with US cases) the types of privacy harm affecting individuals and the issues (or generic attributions) that caused these. Privacy harm appears at all three levels: (1) Misuse (actual⁴³ harm due to data misuse), (2) Leak⁴⁴ (improper dissemination by organisations) and (3) Insecurity⁴⁵ (results from architectural issues and shoddy security). As suggested by Solove (2008), *effective approach* means to focus on the bottom of the data security pyramid, not the top as shown in Figure 2-6 p 40. The data abuse pyramid is represented with key points extracted from Solove (2008). The Albrecht (2012) privacy harm cases are also in the diagram: *identify theft, fraud, reputation harm/damage and physical damage*.



Data misuses cause concrete injuries: financial losses, emotional distress, and even physical violence. *Leak* and *Insecurity* generate potential future harm that a person could suffer: identity theft; harm to reputation; being hindered in obtaining jobs, loans, or licenses; emotional distress and anxiety. *Anxiety* arises from the inability to recover the data and to prevent further abuses. The psychological harm associated with the loss of individuals' ability to control information about themselves (privacy) can be devastating. These potential future harms due to *Leak* and *Insecurity* are where problems emerge not

⁴² The Pyramid of Pain has been referenced in ENISA Threat Landscape 2014:

<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2014/> [Accessed 29-December-2018].

⁴³ The term *actual* is to denote the concrete materialised/manifested financial, physical and emotional harm as these harms are easy to understand unlike the potential future harm.

⁴⁴ Information leaked or disseminated improperly, and it is now somewhere beyond the control of the entity that leaked it.

⁴⁵ *Insecurity* is a problem of architecture or information infrastructures which also includes computer code and the manner in which data is accessed.

only as legal response challenges for dealing with information abuses but also incident response challenges for organisations. An effective DBI response playbook will need to **minimise the potential future harm to individuals**. An approach is to notify individuals affected by the DBI. Schwartz and Janger (2007) note that an often-overlooked function of data breach notification is that it can help both customers and business entities **mitigate the harm** caused by a leak. Minimising or mitigating harm using breach notification has been cited in Lane et al. (2010)⁴⁶, Rotenberg and Jacobs (2013)⁴⁷ and Daly (2018)⁴⁸. On data privacy, most articles – including Solove’s – take a position or perspective based on the legal concepts attached to privacy. Fuchs (2011) discussed the diversity of such legal concepts and challenged the liberal notion of privacy. In so doing, Fuchs (2011) also challenged Solove’s (2006) concept of privacy and his privacy typologies. Fuchs’s (2011) critique runs along this line: *The problem of these privacy typologies is that they are arbitrary: there is no theoretical criterion used for distinguishing the differences between the categories. The different definitions are postulated, but not theoretically grounded. A theoretical criterion is missing that is used for distinguishing different ways of defining privacy*. Kitkowska et al. (2018) in pointing out that there is no clear definition for privacy and privacy harm, took a multidimensional notion for harm and adopted De and Le Métayer’s (2016b) definition for privacy harm and also used Solove’s (2006) taxonomy to investigate privacy perceptions and behaviours. Kitkowska et al. (2018) showed that people express *privacy concerns differently* from the perceptions identified by Solove, and people tend to perceive privacy concerns as *comprehensive and simplified models*. Moreover the authors in privacy harm literature state that legal scholars discuss privacy harms and technical papers talk about feared events, threats and vulnerabilities (De and Le Métayer, 2016b). It is worth pointing out that De and Le Métayer changed their 2016b description for privacy harm in their 2017⁴⁹ paper which used this phrase – *privacy breach* – in their revised description. Henriksen-Bulmer et al. (2019) examined Solove (2006) and the extensive multi-dimensional analytic privacy mapping framework by Mulligan et al. (2016) and pointed out that both authors’ frameworks do not consider in *any depth* the *human element* i.e. *how people behave and perceive privacy and how the context within which data is shared may be affected by those behaviours, values and norms*.

Although Clarke (2013) identified a set of five categories of harm, these are harm to data⁵⁰. He further outlined kinds of harm that can be caused to organisations – which he refers to as direct harm. The other (indirect) harm to the interests of a variety of dependent parties also needs to be taken into

⁴⁶ Discussed the Australian Privacy Act: The primary purpose of notification is the *mitigation of damage* caused by a breach, rather than the provision of some sort of mechanism of reputational sanction.

⁴⁷ Cited the EU ePrivacy that giving users timely notification of a potential data breach can allow users to take significant steps to *reduce potential* personal harm.

⁴⁸ Cited the Californian breach notification law (2003) that the early notification allows consumers to protect themselves against identity theft and *mitigate damages* resulting from unauthorised access to their information.

⁴⁹ Their 2017 privacy harm description is in Section 1.1.3. Their 2016b description: *A privacy harm is the negative impact on a data subject, or a group of data subjects, or the society as a whole, from the standpoint of physical, mental, or financial well-being or reputation, dignity, freedom, acceptance in society, self-actualization, domestic life, freedom of expression, or any fundamental right, resulting from one or more feared events*.

⁵⁰ The five categories of harm to data are: data loss; data inaccessibility; unauthorized data modification/loss of data integrity; unauthorised data access; and unauthorised data replication. These are specifically for when selecting among cloud sourcing options.

consideration. It is not specifically stated whether individuals are the other *dependent parties*. However, in describing an example for an airline affected by loss of data, an individual to whom data relates may be harmed by ill-informed decision-making by a corporation or government agency. Again, the harm listed⁵¹ focuses on organisations, not on an individual. The harms listed do have this feature: *negative privacy impact on individuals* (e.g. customers, employees), including personal safety.

Solove's (2006) privacy taxonomy (Solove Taxonomy) has been examined by Massey and Antón (2008) by comparing and contrasting it with the Antón-Earp Taxonomy⁵². In Massey and Antón (2008), the focus was exclusively on mapping the vulnerabilities outlined in the Antón-Earp Taxonomy to privacy harms in the Solove Taxonomy. Their study found that the vulnerabilities in the Antón-Earp Taxonomy, even though they targeted narrowly the specific web-based privacy policies, map to multiple harm categories in the Solove Taxonomy. Mapping of security vulnerabilities to privacy harm is complex, as privacy harm, as defined in the Solove Taxonomy, is driven by legal constructs, unlike systems vulnerabilities studies, which have primarily been *systems goal-driven* or *stakeholders' goal-driven* (as done in requirements engineering). As highlighted by Massey and Antón (2008), the Antón-Earp Taxonomy emphasises concerns that must be considered to increase requirements coverage as well as reducing vulnerabilities in web-based information systems. Privacy harm is not readily definable as *systems goal* specified by systems engineers. Moreover, privacy harm that affects individuals whose personal data has been compromised may arise not from vulnerabilities in systems. There are **data-human issues** i.e. those related to administrative errors and/or the use, misuse, abuse of personal data.

2.2.4.2 On privacy harm assessment

Clarke (2013) examined the Ackermann security risk items and dimensions and gave a schematic representation of a variant of the conventional security model. In the model one of the propositions was: *A Stakeholder's perception of the value of an Asset may be harmed by a Security Incident*. Furthermore, on the concept of risk the convention within the professional security community is very specific, and somewhat counter-intuitive. Risk is a measure of the likelihood of *harm arising from a specific threat*. Clarke (2013) emphasised that risk, defined in terms of harm and threat is used as a guide *in prioritising the Safeguards (controls) that an organisation's inherently limited resources should be invested in*.

Also, De and Le Métayer (2016b) observed that there is often a lack of clear distinction between the concepts of privacy harm and security risks or indeed a clear relationship among them. Moreover, the De and Le Métayer (2016b) approach to privacy harm (i.e. privacy harms of smart grids) is driven by a privacy risk analysis, whereby the identification of the potential harms needs to be appropriate for the system under consideration and its severity. The authors also listed the privacy harms types and taxonomy for smart grids and constructed a *harm tree*. A tree structure is adopted instead of a pyramid, as similar tree-based structures have been used extensively by security researchers. Tree-based structures have

⁵¹ The kinds of harm that can be caused to organisations (of direct and indirect kinds) when data is subject to a security incident: degraded operational capacity; degraded customer service quality; reduced asset value; reduced revenue; increased costs; damaged reputation, including confidence of customers, investors and regulators; negative privacy impact on individuals; non-compliance with obligations or commitments.

⁵² The Antón-Earp Taxonomy is split between one classification that describes measures to prevent harms and another classification that describes measures that could lead to privacy harms. The Solove Taxonomy classifies only privacy harms because Solove's goal is to outline all possible privacy harms.

been used to categorise security and cyber related incidents and attacks. In a widely cited paper by Howard and Longstaff (1998), whereby computer security incidents are examined from a process perspective, the incident-attack-event categories are listed like a tree structure. Similarly, in Uma and Padmavathi (2013) and in Simmons and Dasgupta (2014), the cyber-attack taxonomy is captured and shown in a tree structure. Also as noted by De and Le Métayer (2016b), very few privacy papers have been published on this topic on attack trees or the use of tree-structures for privacy harm.

However, none of the current literature on PIA and/or harm trees or pyramids investigates personal data harm in the context of DBI or privacy harm to individuals. They have primarily focused on design and engineering, theoretical risk management, policy-making and not on the operational aspects. For example, the terms *privacy harm*, *privacy damage* and *privacy consequence* are mentioned in articles related to technical protection measures for privacy issues (e.g. identification/linkability). These focus on specific devices/architectures or security features (i.e. the design and development aspects). These articles are Krishnamurthy and Wills (2009), Zhu et al. (2009), Song et al. (2011), and they do not offer further references or descriptions as to what constitutes these privacy harm, damages or consequences especially for organisations or individuals. Krishnamurthy and Wills (2009) introduced the concept of secondary privacy damage and found that existing privacy protection techniques have limitations in preventing privacy diffusion which results in secondary privacy harm. This secondary privacy harm is related to the notion of secondary data leakages and arises when data privacy related to other users are either deliberately or inadvertently leaked.

Based on the above observations, any assessment framework for privacy harm needs to adopt a theoretical legal foundation that is also pragmatically presented using a visual tree-structure for the intended context (namely incident response) and users (namely organisations faced with personal data breach incidents).

A possible pragmatic approach is described in *The Boundaries of Privacy Harm* (Calo, 2011). This paper has been cited mostly by other legal scholars, but it has also been referenced by Wright and Raab (2014) and De and Le Métayer (2016a, 2016b). The Calo (2011) approach to privacy harm is to provide a working definition of privacy harm by proposing two categories of privacy harm: (a) unwanted observation, and (b) the use of a person's information against them. This working definition of privacy harm, besides giving courts and regulators criteria to identify privacy harms and rank the severity of privacy harm, also provides a *rule of recognition* to identify new privacy harms as they emerge. As regards the legal basis of privacy harm, distress or moral damage or non-pecuniary loss as a result of data breach has been now been recognised by the UK Court.

Privacy harm can present itself in different ways as tangible and quantifiable, for example as financial loss, or as intangible and non-quantifiable, for example distress. Identifying, classifying and quantifying such harms is usually addressed under privacy risk assessments or more formally using PIA. PIA has established itself as an important tool since the mid-1990s (Clarke, 2009). According to Clarke, (2009), PIA is different from *processes such as compliance checks and privacy audits because of its anticipatory, positive and risk-management orientations*.

In terms of PIA this research was not intended to re-design or to apply PIA frameworks or methodologies which have been outlined or published by practitioners, regulatory bodies and researchers.

Oetzel and Spiekermann (2014) conducted a detailed study on PIA which found that *existing PIA approaches cannot be applied easily because they are improperly structured or imprecise and lengthy*. Furthermore, Henriksen-Bulmer et al. (2019) highlighted that the PIA framework (used in six countries) by Wright et al. (2013a) does not address *existing data or processes*. Instead it is for *assessing privacy risks to a new project, process or system so that appropriate mitigation and security strategies can be incorporated into the design and/or implementation*. In GDPR Article 35, PIA is denoted by DPIA and is compulsory for any high-risk data processing and the scope may include examining privacy risks for existing processes or data. Accordingly, GDPR requires *practitioners to consider privacy risks, not from the perspective of the organisation but from the perspective of the individual (i.e. the data subject) and how the risk might impact the data subject* (Henriksen-Bulmer et al., 2019⁵³). However, PIA frameworks and methodologies were examined for risk indicators and processes that touch on privacy harm, ethical principles, and the DBI response activities. One such PIA methodology is the Privacy Risk Analysis Methodology (PRIAM) by De and Le Métayer (2016a). De and Le Métayer (2016a) pointed out that existing research on PIA does not address the technical implementation aspects of PIA and hence proceeded in designing a privacy risk analysis methodology (PRIAM). In the PRIAM, privacy harm is one of seven components. It describes privacy harm as the negative impact of the use of the information system on a data subject, or a group of data subjects – society as a whole – from the standpoint of physical, mental, or financial wellbeing or reputation, dignity, or any fundamental right. Furthermore, it adopted the categories of harms from Calo (2011) and Solove (2006). These categories are: (1) *physical harms like physical ailments, death, or injury*; (2) *economic harms such as loss of benefits or robbery*; (3) *mental or psychological harms such as fear of misuse of personal data, fear of being treated unfairly, anxiety, or mental distress*; (4) *harms to dignity, reputation such as embarrassment or humiliation* and (5) *societal harms like chilling effect due to surveillance*.

Investigation into privacy harm is challenging not only because privacy is conceptual and there is no universally accepted PIA, but researchers also use *prejudicial effect* rather than *privacy harm* as referred to by De and Le Métayer (2016a). Legal scholars have used *privacy injuries* and *privacy-impairing* in discussions of privacy tort law (Citron, 2010). In GDPR Recital 85, the term *damage* was used: *A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material **damage** to natural persons...*

As made evident by Wright and Raab (2014), for a PIA to be fully effective, it needs to *address all types of privacy and the associated privacy principles, and the risk of harm to a wider array of rights*. According to the ICO, the *core principles of PIA can be applied to any project which involves the use of personal data, or to any other activity which could have an impact on the privacy of individuals* (ICO, 2014).

The above referenced security-related literature on PIA primarily addresses the prevention of harm in relation to technical measures or system development. Although this research is not entirely on risk assessment methodologies, it has been recognised by Johnson (2014, p 66) that risk management, as well as risk and business impact assessments, forms the basis for determining the priority of resource protection and response activities. In terms of risk for any organisation, breach or loss of personal data

⁵³ The authors referenced incorrectly GDPR Article 25, which is not on DPIA.

should be regarded as a *distinct risk for any organisation* (Wright et al., 2011). However, Shamala et al. (2013) made it clear that although there are numerous available risk assessment methodologies, there is a lack in agreed reference benchmarking, as well as in the comparative framework for evaluating these information security risk methods, to assess the information security risk. Furthermore, Poller et al. (2014) in examining risk assessment in information security, exposed that the traditional asset modelling approach used for modeling security requirements of IT systems does not easily allow assets (e.g. intangible assets such as *privacy*) that are externally owned by various stakeholders to be modelled.

2.2.5 What are the characteristics of existing incident response frameworks? (RO1-c)

Research findings indicate that there is hardly any literature on personal data incident response frameworks (as shown in Figure C- 2 p 211). In reviewing existing incident literature on security, forensics and personal data, for example in Barron et al. (1999), Pollak et al. (2004) and Pieterse (2011), *framework* appears to be a loosely used term, unlike in Beebe and Clark (2005) whereby framework principles are exposed and built into a generic framework. A generic, abstracted framework model is needed to tackle the complex incident phases and processes. Also, in order to tackle the dynamic variety in digital data, there is the need to abstract the evidence model and analyse its characteristics before further challenges can be identified (Raghavan, 2013). Hence digital forensics literature were examined to identify the characteristics of evidence model and the underlying digital forensics framework theory as described in Section 2.2.5.2.

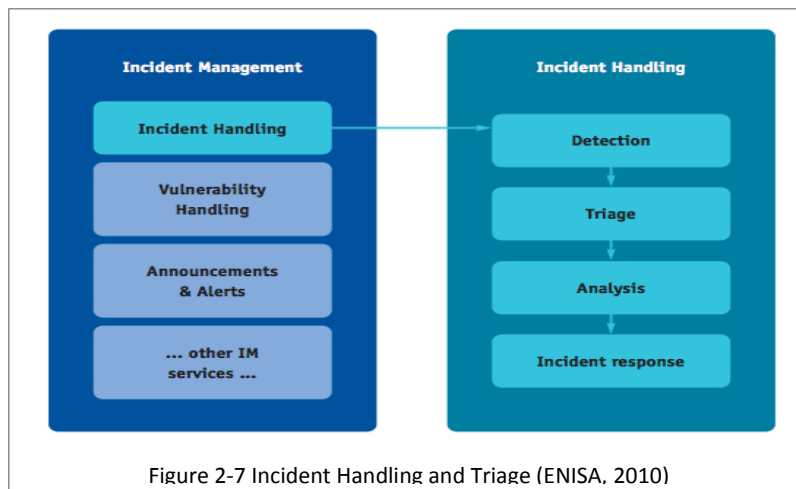
2.2.5.1 On incident management/handling and triage

On incident management, SEI-CME, regarded as an influential organisation on organisation business processes and models, has published an article, *An Incident Management Ontology* (Mundie et al., 2014) and most recently *An Insider Threat Indicator Ontology* (Costa et al., 2016). Although there is now an incident management ontology which includes a simple visualisation tool, this has not yet been applied to a real-world individual/organisation (Mundie et al., 2014). Interestingly, triage incident – appears as an initial response activity – is noted but not described in the SEI-CME ontology paper. This triggered this researcher to examine **triage as an initial response activity**.

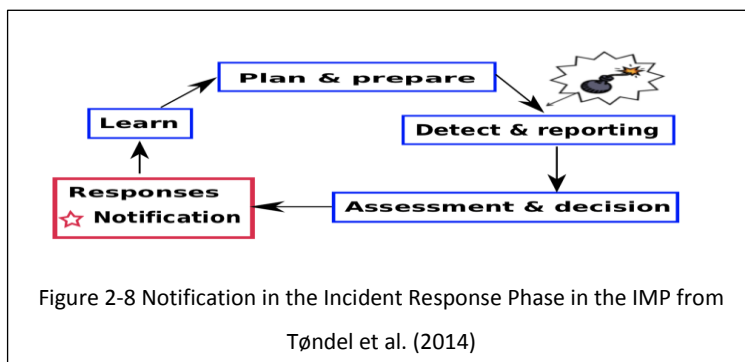
In Europe, ENISA has produced reports and guidelines for Computer Emergency Response Teams (CERTs or CSIRTs), primarily for critical infrastructure protection. It has also published several reports in collaboration with industry partners on privacy and data breach notification. Although ENISA did not mention triage in their data breach papers, it did mention triage under their CERTs scheme and in incident handling for CERTS (ENISA, 2009). Furthermore, ENISA (2010) described the incident handling as: *Incident handling has four major components (derived from CERT concepts), which are given here in the order in which incidents occur. First, an incident is reported or otherwise detected (detection). Then the incident is assessed, categorised, prioritised and is queued for action (triage). Next is research on the incident, what has happened, who is affected and so on (analysis). Finally, actions are taken to do all that is necessary to resolve the incident (incident response)*. As shown in Figure 2-7 p 46, triage is part of incident handling which forms the core service carried out by most CERTs.

The incident management phases (**IMP**) provide a high level view of the main stages associated with incident management, extracted and shown in Figure E- 1 p 214. Tøndel et al. (2014) studied (using

the Kitchenham and Charters (2007) approach) current practice and experiences with incident management, covering a wide variety of organisations using ISO/IEC 27035⁵⁴ and also synthesised the incident management process as described in ISO/IEC27035 and NIST SP 800-61⁵⁵. Their synthesised IMP was re-drawn to show just the high-level processes as shown in Figure 2-8 p 46.



Although triage is mentioned it did not describe the activities or processes associated with triage. Instead it highlighted that *an incident is detected and considered in a triage before a report is generated. Then there are the states of analysis, obtaining contact information, providing technical assistance, and coordinating information and response, before the incident is finally resolved.* The Response stage in Figure 2-8 p 46 has three phases: *notification; responses; recovery.* This research focused on the Responses stage, namely an incident has been detected/reported and incident handling activities, in particular breach notifications, are triggered.



⁵⁴ Tøndel et al. (2014) used ISO/IEC 27035:2011 which has been revised in 2016. Information technology. Security techniques. Information security incident management. Principles of incident management: <https://www.iso.org/standard/44379.html> [Accessed 29-December-2018].

⁵⁵ National Institute of Standards and Technology (NIST), US Department of Commerce (NIST) - Computer Security Incident Handling Guide. NIST SP 800-61 is a special publication which aims to assist organisations in mitigating risks from computer security incidents by providing guidelines on how to respond to incidents effectively and efficiently. <http://www.csirt.org/publications/sp800-61.pdf> [Accessed 29-December-2018]. The revised edition is not available on nist.gov.

2.2.5.2 Digital investigative processes (DIP) and framework standardisation

Fundamentally all the DIP phases centred on the *computer forensic science maxim* outlined by Noblett et al. (2000). Pollitt (2007) presented the three-level hierarchical model (**3LevelModel**) in analysing existing forensics frameworks. The results back in 2007 revealed little consensus among professionals and collective scientific and empirical experience. This researcher⁵⁶ provided a review on an article for a journal, and also conducted a review on previous work on related digital forensic frameworks/models. The analysis of these frameworks has proved to be a time-consuming exercise. It appears that the digital forensics roadmap framework that was produced at DFRWS⁵⁷ (DFRWS, 2001) has been widely referenced in literature in the discussion on incident handling and forensics. There are corpus forensics frameworks all using their own terminologies and descriptions for the activities, and most do not clearly state the principles or representation approaches underlying their frameworks. However Beebe and Clark (2005) took a different approach, still following the DFRWS (2001) *Theory, Abstract, and Purpose* guidelines, and developed a generic, tiered (hierarchical) framework that is *objectives-driven* (principles-based) instead of tasks-driven. It also addressed the *usefulness* aspect in highlighting that the framework provides *a mechanism for including the layers of detail needed by its users*. Tasks and standard processes can be complex in nature. *A framework whether forensic in nature or not, requires scientific rigor, and must be based on objectives*, rather than tasks to ensure the framework is robust. *The robustness of a framework is a function of its usability and acceptability* (Beebe and Clark, 2005). The Beebe and Clark (2005) framework⁵⁸ (which mentioned triage in the case study on the framework), shown in Appendix F p 215, achieved these features by simplifying the complex tasks and processes with objectives for levels of phases/sub-phases.

One observed challenge is: where and when does the forensic examination starts or be identified as a phase for examination of the digital evidence? Examination requires *analysis* and also *identification, evaluation or authentication*. A widely cited paper by Carrier et al. (2003) has this: *In this field, there are many interpretations and meanings of key words*. This lack of standardisation issues is raised by several researchers as noted in Montasari et al. (2015). Furthermore, increasingly, digital forensics are used in more diverse contexts, such as criminal and civil cases, as well as in incident response (Moser and Cohen, 2013). Traditionally, computer forensics⁵⁹ are conducted in forensics laboratories (off-scene investigations). In this era where digitisation appears not only in organisations but also in our homes and in our daily lives, digital evidence can be anywhere in cyberspace, in the dark or deep web, or embedded in devices. Pollitt

⁵⁶ This researcher attended the 10th Annual International Conference on Global Security, Safety and Sustainability, ICGS3-15, London in September 2015. Subsequently this researcher was invited to review an article for publication in the International Journal of Electronic Security and Digital Forensics (IJESDF).

⁵⁷ According to the DFRWS website, it has global reach: <https://www.dfrws.org/about-us> [Accessed 29-December-2018].

⁵⁸ The Beebe and Clark (2005) framework was applied on two cases studies and it is applicable to forensic and non-forensic investigations.

⁵⁹ In early days, digital forensics was called computer forensics since the evidence collected was restricted to computers. In the late 1990s and early 2000s with the increasing usage of computers and the Internet, digital forensics was established as an independent field (Raghavan, 2013).

(2013) called for a new forensics approach⁶⁰ to address this new paradigm – *vast increase in digitally stored information, and the disparate uses to which humans employ digital technologies*. However, in highlighting the systematic failure of both the digital forensic process and digital forensic software, although privacy protection was not mentioned, Pollitt (2013) recognised that *data is more about human interactions and interpersonal relationships than on technology*. This resonates with Sir Tim Berners-Lee's quote *data is relationship*.

2.2.6 What is triage and how does it work? (RO1-d)

This research was not a historical research into triage; nevertheless the way triage started in the battlefield during the Napoleonic war (circa 1812) (Iserson and Moskop, 2007), and how triage was applied in the medical field may shed some light as to why triage is practical for incident handling, in particular, DBI and the underlying theory or principles behind triage. The French origin of triage (tier) Edwards, 2009) means *to sort* or in another word *to prioritise*. As reported by Iserson and Moskop (2007), the distinguished French military surgeon Baron Dominique-Jean Larrey articulated this: *a clear rule for sorting patients for treatment: Those who are dangerously wounded should receive the first attention, without regard to rank or distinction. They who are injured in a less degree may wait until their brethren in arms, who are badly mutilated, have been operated on and dressed, otherwise the latter would not survive many hours; rarely, until the succeeding day*.

2.2.6.1 Incident triage and medical triage

SEI-CMU described triage as: *the process of sorting, categorising, and prioritising incoming incident reports or other CSIRT requests. It can be compared to triage in a hospital where patients who need to be seen immediately are separated from those who can wait for assistance* (Killcrece et al., 2003). Although the Killcrece et al. (2003) handbook discussed triage and incident response, it only addressed damage caused by incident to systems/networks and/or infrastructures. It stressed this: *When an incident occurs, the goal of the CSIRT is to control and minimise any damage, preserve evidence, provide quick and efficient recovery, prevent similar future events, and gain insight into threats against the organisation*.

ENISA used the term *triage* and also discussed *prioritisation* (ENISA, 2009). The ENISA (2009) report stressed that incident reporting is a resource intensive task and provided three means that may be used to prioritise incident: *reporting thresholds; reporting categories and human actor review*. Also, according to ENISA (2009), when the reporting party decides to submit a report to the data authority, prioritisation starts and it is the first step in the incident response. In another report, ENISA (2010) described triage as *classifying, prioritising and assigning incidents*. The triage is part of incident handling which forms the core service carried out by most CERTs as shown Figure 2-7 p 46. Hove and Tårnes (2013) in referencing ENISA (2010), described triage as: *This stage consists of the three phases verification, initial classification and assignment*.

Furthermore, although triage has been viewed as a strategic resource allocation tool (O'Laughlin and Hick, 2008; Domres et al., 2010; Roussev et al., 2013), triage is a dynamic process (Vayer et al., 1986;

⁶⁰ Instead of focusing on the geology and archaeology of computers and on the extraction and interpretation of data in a historical context in the current computing environment, better paradigms might be anthropology and sociology (Pollitt, 2013).

Eaton, 2003; O'Meara et al., 2007), to get the full benefits it also requires teamwork (Seefeld, 2008). Vayer et al. (1986) state that triage is a process of determining *priorities for action*, the process is dynamic, as it is responsive to the changing clinical condition of the patient, available resources, time, and personnel. The dynamic nature of triage is that the general theory of triage has remained relatively constant: *to allocate scarce resources in a manner that will provide the greatest good for the most people with minimum consumption of those resources*. Vayer et al. (1986) further state that *depending on circumstances*, the three major variables that influenced triage decisions, each assigned differing weights are: *the good or benefit realised by an action (quality measure); the number of people benefitting as a result of an action (quantity measure); and the net loss or diminution in terms of both tangible and intangible resources*. However little literature on digital forensics and incident response has adopted the general theory of triage and the three influencing variables in triage as outlined by Vayer et al. (1986). Also according to Pollitt (2013), triage is a **practical** solution for both investigators and examiners. Beyond practicality there is hardly any literature on the theory or principle underlying the practicality of triage as applied in digital forensics investigation or for security incident handling.

As noted by Moser and Cohen (2013) in referencing Iserson and Moskop (2007), triage is a process commonly applied in the medical field in order to ration limited resources and to maximise their overall effectiveness. It is not clear how or when triage came into use in digital forensics under the name of computer forensics which dated back in the 1970s (Pollitt, 2010; Kohn et al., 2013). Perhaps the practitioners have been applying triage even without them knowing that they are triaging when computer forensics started.

The existence of guidelines for communication and **prioritisation of incidents** is one of the most important parts of incident management (Cichonski et al., 2012; Hove and Tårnes, 2013). Prioritisation in triage as drawn from the medical field is mentioned by Moser and Cohen (2013), who cited Hogan and Burstein (2007) and also Parsonage (2009). Moser and Cohen (2013) applied the same medical triage approach in that prioritisation of evidence acquisition and analysis are possible once the potential systems are classified into categories (adopted *three categories for classification*). In applying a similar medical triage approach, *the goal of digital forensic triaging is to prioritise evidence for acquisition and analysis in order to maximise case throughput*. In Parsonage (2009) the triage dictionary definition in a medical setting was amended for application during digital forensics. Parsonage (2009) viewed triage as a resource allocation process for sorting enquiries into groups based on the need for or likely benefit from an examination in which limited resources must be allocated.

The triage dictionary definition used by Parsonage (2009) is: *A process for sorting injured people into groups based on their need for or likely benefit from immediate medical treatment. Triage is used in hospital emergency rooms and at disaster sites when limited medical resources must be allocated*.

2.2.6.2 Triage ethical principles

In the medical field, the underlying ethical principles that drive triage (and the classifications for triage) are rooted in medical ethics developed over centuries and founded upon humanitarian law⁶¹ (Domres et al., 2010) e.g. the Hippocratic maxim: *first, do no harm* (Enemark, 2008). According to Domres et al. (2010), besides being used as a strategic tool in the case of a disproportion between needs and resources (*resource triage* by O’Laughlin and Hick (2008)), triage implicitly leads to the ultimate question of the *worth of human life* and thus touches upon the core ethical dimension of disaster medicine. For a DBI response, the question of the *worth of human life* may not be at the same level of urgency or criticality as those in medicine but the consequences of privacy harm may raise such ethical questions which will demand privacy harm triage that strikes a humanitarian response. Ethics in forensics investigation or incident handling have not been debated or researched unlike in the medical domains, examples by Domres et al. (2001), Hartman (2003), O’Laughlin and Hick (2008) and Aacharya et al. (2011).

There are distinctions regarding the setting or the context of where triage is used. In a clinical setting, triage is referred to as conventional triage, unlike triage in a disaster or mass-casualty incident – disaster triage. In both settings triage is the first step in a dynamic decision-making process where the *determination of priorities for action*, decisions are made that may affect the extent and quality of patient care. In a disaster or mass-casualty incident this may be difficult, and triage methods have been found to be only about 80% accurate in determining a patient's needs (Kennedy et al., 1996). This is where ethics in triage comes into conflict. In a disaster incident, there are often the moral dilemmas and *tragic choices* (i.e. public choices involving life and death situations) that arise during the response phase, when time is scarce, decisions are pressing, essential resources must be rationed, and individual interests may be subordinated to the public interest. Jennings and Arras (2016) further remarked that in such situations, reflections on ethics will not provide clear-cut rules or directives. Ethics need to be part of the overall adoption and application of triage. As discussed by Moskop and Iserson (2007): *Whether the choice of a triage system for a particular setting is justifiable will depend on an evaluation of the specific system itself, its underlying values and principles, and the setting in which it is applied*. The authors further state that: *Most triage systems are designed to serve the values of human life, human health, efficient use of resources, and fairness. Nevertheless, given the variety of specific triage settings and goals, there is no single “correct” way to perform or to justify triage*.

Ethical principles, if embedded into the practice of triage, should support the *tragic choices* between the *greatest goods for all or greatest net benefit* and the individual’s (the triage practitioner) conscience in times of crisis or disaster. This is the *intuitive humanness response* decision making in *times of crisis* or disaster.

Researchers in the medical domain have raised ethical issues in the performance of triage (e.g. Domres et al., 2010; Good, 2008). Ethics have surfaced as topics under the information security domains

⁶¹ A comprehensive report on the humanitarian law:
https://www.redcross.org/images/MEDIA_CustomProductCatalog/m3640104_IHL_SummaryGenevaConv.pdf
[Accessed 29-December-2018].

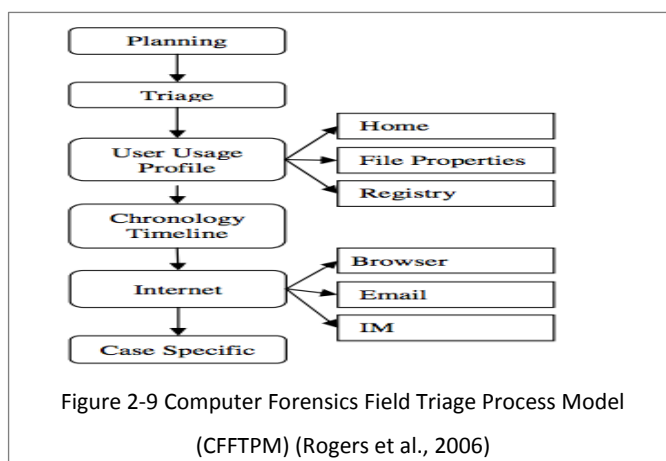
(e.g. Marx, 1998; Greenwald et al., 2008; Matwyshyn et al., 2010) but little in the incident response domains.

2.2.6.3 Triage in digital forensics

In the existing forensics frameworks, little is discussed about privacy protection, besides Hong et al. (2013). Casey (2013) identified that the legal perspective on privacy is one of the more complicated issues related to triage in digital forensics. It also pointed out that triage involving using the minimum information necessary up front is justified, particularly when someone is falsely accused. Making early determination using triage is crucial especially as there is pressure to obtain information quickly, in ever-increasing quantity and diversity of computer systems holding large amounts and varieties of data. However, there is lack of consensus in the digital forensics field regarding what exactly constitutes triage. Although there is no consensus, Pollitt (2013) described this as: *triage is often understood as a way to maximise the use of scarce resources by prioritisation. For example, triage in digital forensics is often used to describe attempts at limiting the volume of data or devices which are exhaustively examined.*

In terms of decision support, the forensic processing requires a primary goal of **early extraction of information** from digital evidence sources (commonly referred to as triage) to advance a digital investigation more effectively (Casey et al., 2013). However, triage is not widely mentioned or depicted in existing forensics frameworks. Montasari et al. (2015) analysed 26 models against 53 components (phases/subphases/tasks) and listed these in a table. Triage and/or prioritisation were not among the 53 components even though Rogers et al. (2006) has a dedicated phase for triage as shown in Figure 2-9 p 51. Currently, this is the only digital forensics model that specifically addresses and describes triage.

Rogers et al. (2006) defined the computer forensics field triage process model (CFFTPM) as: *Those investigative processes that **are conducted within the first few hours of an investigation**, that provide information used during the suspect interview and search execution phase. Due to the **need for information** to be obtained in a relatively short time frame, the model usually involves an on-site/field analysis of the computer system(s) in question.*



In formalising triage into the CFFTPM forensics framework, Rogers et al. (2006) have highlighted the role and advantage of triage: *The triage phase is fundamental to the process model and along with proper planning it is the foundation upon which the other phases are built. Being able to conduct an examination and analysis on scene, **in a short period of time** and provide investigators with time sensitive*

leads and information provides a powerful psychological advantage to the investigative team. Also, CFFTPM was developed in reverse of most other models in the area, namely instinctive approaches based on actual trial and error, cases, court decisions and the direction from prosecutors are aggregated, and articulated into a more formal methodology; still maintaining the investigative essence and the key components that have been battle tested (Rogers et al., 2006).

As noted by Shiaeles et al. (2013) the importance of prioritisation (as done with triage) prior to moving into the collection of the various system and user data is a key feature of CFFTPM. This **prioritisation** done in the initial early phase in the CFFTPM is what distinguished triage as an important step for **timely action that may be important to hold criminals accountable for their actions or to protect others from further harm**. Rogers et al. (2006) referred to this as **speedy initial triage** in the CFFTPM.

An attempt to describe triage in digital forensics has been given by Pearson and Watson (2010): *it is a procedural model for the investigation of digital crime scenes including both traditional crime scenes and the more complex battlefield crime scenes*.

Digital forensics investigation is a complex activity not only because of the technological and environment factors it needs to address and operate on, but also the legal imperatives as set by the courts of law. Montasari et al. (2015), in conducting a detailed examination of the forensics frameworks literature, revealed that there is no comprehensive DIP model that is widely accepted by the digital forensic community and courts of law. ACPO (2012) has this: *it is important that people who work within the arena of digital forensics do not just concentrate on the technology, as essential as that is, but that the processes we use are fit for the purpose*. Representing the processes or activities with phases and tasks and communicating these visually with text in a diagram seems to be the common approach taken by the forensics research community. However, it seems this approach is not meeting the *fit for the purpose* or the usability of these forensics frameworks is being challenged e.g. Garfinkel (2010).

It appears that researchers have applied on-scene triage inspection for mobile investigations. As highlighted, on-scene triage inspections are distinct from, and potentially a precursor to, forensic analysis in digital forensics laboratories (Mislan et al., 2010). Mislan et al. (2010) also outlined the on-scene mobile triage processes and pointed out that triage inspections have a role in large-scale digital investigations, including security breaches within an organisation and electronic discovery in civil cases. It also states that one of the benefits of the triage process is that it can mitigate the risk of privacy violations resulting from a digital investigation. Mislan et al. (2010) besides restating Casey et al. (2013) that the primary purpose of on-scene triage inspections is to use the digital evidence to support any kind of investigation, state that a side benefit of this process is economic. One other benefit of triage is the ability to assess the perpetrator's *danger to society* (Casey, 2013) and (Rogers et al., 2006). This is so as triage is conducted within the *early phases or the first few hours of an investigation* (Rogers et al., 2006).

2.2.7 What visual methods provide meaningful and practical support for triage processes? (RO1-e)

2.2.7.1 Timely initial phased response

An initial review indicates that a data breach incident response needs to be addressed differently using a phased or tiered approach, unlike the traditional or established incident handling mechanism for security incidents. A phased approach is suitable when there are *unknowns* (e.g. where identification of

the sources or causes are difficult) and time is of the essence. A phased approach is similar in concept to an iterative approach as commonly used in agile software development, where scoping and prioritisation of features (unknown/uncleared/risky features) for early or *quick* delivery is essential for successful delivery of the intended outcomes. The recommendation of a phased approach is to enable organisations to comply with the stringent 72 hours breach notification as required by the GDPR⁶². Again, under the GDPR Recital 85: *Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it...*

This research was not concerned with how to design or what is required for an agile organisation. From examining the various literature sources reviewed by Sherehiy et al. (2007), the *quickness* characteristics i.e. *reacting quickly* or the flexible ability to *quickly change from one course to another* appeared as common agile characteristics mentioned by the various authors. However the descriptions offered by Sharifi and Zhang (1999), which are related to organisational operational capabilities, are: *Responsiveness is considered as the ability to identify changes and respond quickly to them, reactively or proactively, and to recover from them. Quickness is the ability to carry out tasks and operations in the shortest possible time.* Agile characteristics denoted as *responsiveness* and *speed* are among the core and global characteristics of agility that can be applied to *all aspects of an enterprise* (Sherehiy et al., 2007).

For DBI purposes, to be agile is to be *competent* and *flexible* such that organisations can react or *respond quickly in a timely manner* when faced with a DBI. When using terms which describe the temporal dimensionality of flexibility⁶³ or agility, careful wording is required, as references must not include absolute speed as a measure of success. Use of the words *in a timely manner* illustrates that the speed of response is important but it is relative to the *nature of the change* that is required or being made (Conboy, 2009). Hence to respond quickly in a timely manner requires examining and taking into consideration *the nature or the context of the DBI*. However, this research adopted this premise: the primary driving consideration in responding to a DBI is to minimise the likely privacy harm to the affected individuals. It is not only to comply with the GDPR notification requirements, but the responsiveness and/or quickness are also needed to minimise the likely privacy harm to affected individuals. In GDPR Recital 85 uses the wording *timely manner*: *A personal data breach may, if not addressed in an appropriate and **timely manner**, result in physical, material or non-material damage to natural persons...*

Also, processes for conducting a full forensic investigation that require *timely results* do not simply refer to *speeding up tasks, but delivering useful information at crucial decision points to support more effective case management and digital investigation* (Casey et al., 2013). Although not specifically addressing triage process, Shiaeles et al. (2013), in examining triage tools, argued that in order to achieve a suitable tradeoff between the speed of the triage process and the appropriateness of the collected data, the triage tool needs to have *adaptiveness* capabilities. In *responding quickly* (in a *timely manner*) to DBI,

⁶² Phased approach in GDPR Article 33(4).

⁶³ The terms *flexibility* and *agility* are very similar and have often been used interchangeably throughout the literature (Conboy, 2009; Agarwal et al., 2006).

the agile processes for DBI need to ensure **usability and purpose** as outlined in DFRWS (2001) on *useful* and *purposeful entities*.

However, the development of any agile framework and the application of these agile features (or attributes) to such complex structures as an enterprise presents a serious challenge. This is so, as each of the components – organisation, people, and technology – of the enterprise is multidimensional and complex itself (Sherehiy et al., 2007).

2.2.7.2 Design principles and visual representation

One approach to simplify the investigation and the design of a DBI framework is to separate the interests of the organisations (data controllers) and those of the individuals (data subjects). De and Le Métayer (2016a) recognised that the interests of the data subjects and the data controllers are generally different (and even conflicting) and it is better to separate the issues. Separating these two groups and using a *phased DBI response* should simplify not only the design of such a framework but also give a lighter DBI response playbook that ought to be *practical to use*.

As stressed by Beebe and Clark (2005), a framework, whether forensic in nature or not, requires scientific rigor and must be *based on objectives*, rather than tasks to ensure that the framework is robust. Tasks and standard processes can be complex in nature. Moreover digital evidence permissibility laws in courts change (Mocas, 2004; Raghavan, 2013) and these are not easy to design into a forensics framework. Such a framework needs to be flexible and generic to accommodate the complex nature of digital forensics. To address these issues, Beebe and Clark (2005) proposed a hierarchical, objectives-based framework which is generic as it allows complex process simplification by allowing users to conceptually focus in on higher ordered tiers (levels). The generic objective-based frameworks by Beebe and Clark (2005) are extracted and shown in Appendix F p 215. As forensics and DIP constitute important aspects for incident handling, and DIP are in the incident management lifecycle, the development of any triage solution for DBI response needs to address *The Theory, Abstraction and Results entities as noted in the DFRWS (2001) scientific forensics roadmap framework*.

In using triage for DBI response, the triage process as part of the digital forensics life cycle, where collection of evidence may be presented in a court of law, needs to adhere to forensic principles for evidence admissibility (Shiaeles et al., 2013). When designing a framework Beebe and Clark (2005) outlined several goals: *achieve scientific rigor and relevance; amplify complex processes to facilitate understanding of the underlying structure; retain enough granularity, or the flexibility to incorporate granularity needed to exploit the framework in unique situations; and delineate standard assumptions, concepts, values, and practices*. Tools to test these goals, which tend to be decision trees in structure, have proved to be challenging. In a clinical setting, Moll (2010), together with other researchers, has observed that most clinical prediction rules provide diagnostic or prognostic probabilities, **using a score or risk stratification algorithm, and only a few are translated into decision rules**.

Visualisation techniques and approaches have been used by researchers for examining or searching for digital evidence (e.g. Vlastos and Patel, 2007; Olsson and Boldt, 2009; Raghavan, 2013). These authors have applied data visualisation in forensics, for example; *Visual triage* – using data visualisation to elucidate qualitative information for the forensics examiner as appeared in Haggerty et al. (2013; 2014) and Koven et al. (2016). Montasari et al. (2015) commented on the use of *visual and formal representation*

(the use of sequential logic notation) as a technique for their forensics framework. However, the design and representation of the reviewed *forensics framework itself* – represented in visual diagrams – have not been given much attention or focus by researchers in the design of the forensics framework. However, using visualisation theory and techniques for representing, communicating and interpreting the complex forensics and incident handling processes have not appeared in the major VizSec Conferences⁶⁴. In a detailed study on visualisation techniques designed around the analysis of network traffic data by Erbacher et al. (2006), they revealed this: *There, a majority of the available tools incorporate only simple visualisation techniques (i.e. graphs), and one key concept with visualisation is that no single visualisation can solve all problems or is appropriate for all tasks*. Visualisation provides one type of representation - a powerful tool/technique/concept - that have been acknowledged and adopted by visualisation aficionados especially in Big Data analytics.

Not everyone with reasonable knowledge on the subject though can interpret or make sense of the colourful visual maps or graphs or pictures and agree upon and/or act upon the intended meaning or the rationale supposedly conveyed by the designer or producer of the visual artefacts. This is a challenge well understood by marketing and advertising practitioners (especially those that use semiotics⁶⁵) in making use of visual techniques to entice or seduce their audience. It is now fairly established that visualisation *works* and these are the reasons outlined by Lowman and Ferguson (2010) in referencing other researchers:

The human visual system is able to perceive graphical information such as pictures, videos and charts in parallel, but text only sequentially (Hendee and Wells, 1993).

Images are interpreted much faster than textual descriptions as the brain processes visual input much earlier than textual input (Teelink and Erbacher, 2006).

Visualisations are only effective when the right kind of pictorial representation is chosen and can be manipulated to show useful information.

However, the above would be useless or impractical if the **human visual system** has no visual capacity e.g. involving a blind or visually impaired person or the *human visual system* has visual capability but it was not the **kind of representation** that delights or appeals if that person is not inclined or interested enough to want to view the images i.e. they are not **right** for that person. Context strengthens not only the **effectiveness** of the **images** but includes other non-visual aspects of the **human visual system**. Semiotics, namely Peirce semiotics, has a role to play to help bridge the contextual and representation issues.

In a similar vein, computer modeling researchers have adopted Domain Specific Modeling approaches and visualisation techniques to simplify complex frameworks/models. Moreover, as highlighted in Li's thesis (Li, 2010), business modeling approaches and the associated modeling tools are in the main complex. These are not user-friendly to use in practice by non-modeling or technical people. This is reinforced by Becker et al. (2000), who summarised that the growing number of different purposes

⁶⁴ VizSec Conferences: www.vizsec.org [Accessed 29-December-2018].

⁶⁵ Examples of semiotics used by practitioners: <https://rwconnect.esomar.org/meaning-of-health-illness-in-todays-culture/> and <http://www.creativesemiotics.co.uk/> [Accessed 29-December-2018].

for business process modeling, as well as the comprehensive modeling tools, complicates process modeling. The business modeling domains have evolved to such a level of complexity that it is difficult to assess how well all these models have been put to practical use⁶⁶. One widely cited modeling approach is the i* developed by Yu (2011). It is discussed in Santillan (2014) for conceptual modeling of business process technology. The i* has been extended by many designers and modelers for a multiplicity of domains, including for security as in i*/Tropos. As given in Komoto et al. (2011) the SecureTropos methodology and language are applied to develop a modeling framework to support internal control. However, on initial evaluation of i* and SecureTropos, these modeling approaches were discarded as the construct and the visual aspects are not intuitive or adaptive or lightweight or agile. Although there are modular constructs available, it is difficult to use these to faithfully model complex incident handling tasks or processes.

Among the many characteristics that make a model useful, one that this research will adopt is to make it *visually intuitive* as studied in Li (2010); that is lightweight in features/functions to be implemented and used by the intended business domain experts. Although this research was not focusing on *visualisation* as a subject topic of investigation, it is worth highlighting that visualisation is more than pretty pictures. Besides ensuring it is more than *pretty pictures*, there are many visualisation approaches and techniques as listed in Ghanbari (2007). For the purpose of this research, as *symbols* and *icons* were used for the graphical displays in the conceptual framework, the inherently analytical ideas and data abstractions need to harness the rich capabilities provided by any visualisation techniques, and its intended benefits.

2.3 What did the SSM studies reveal? (RO1)

2.3.1 Identified issues

The IT security threat environment changes rapidly, and to comply with the GDPR breach notification requirements, organisations will need to respond appropriately to such incidents. As not all security incidents result in personal data breach, one of the challenges is to identify those security incidents/breaches that result in a DB. Breach notification fatigue may result if all security breaches are notified to relevant individuals. Moreover, there are compliance requirements that specify what must be reported or notified in the event of a personal data breach. One indicator of a DB is that the compromised personal data may result in privacy harm to the affected individuals.

Based on the above exposition, the driving motivation was to find a way to help organisations in the UK to respond to DBIs. The response activities should include data privacy harm assessment (PHA). As revealed in this chapter, the usability or practicality of existing forensics and incident response frameworks face issues stemming from context-related issues. Privacy is contextual, the consequence of data breach to affected individuals, i.e. the privacy harm, has no boundaries as the context is *subjective*. An individual's personal data may not be *personal data* under the purview of the data controller or the ICO or the courts of law.

⁶⁶ This researcher discussed the state of the art of business modeling in industry with a consultant, Mr. Phillippe de Valliere on 5-August-2015 from <http://www.sofismo.ch/> [Accessed 29-December-2018]. Mr de Valliere shared his many years of industry experiences and academic collaborative work in business modeling.

With regard to incident response, the term *personal data breach incident* (DBI) has not yet been researched extensively as a topic in the computer science domain literature. The following listed observations have raised issues leading to identification of gaps, and suggestions for further research:

- (a) Future research directions should strive to better understand business challenges related to the impact caused by incidents (Silic and Back, 2014).
- (b) An information security incident does not necessarily entail a personal data breach and vice versa (ENISA, 2012).
- (c) ENISA recommends that incident reporting procedures should be easy and quick to apply. It suggests adopting a two-staged approach, where brief reports with impact estimates are sent within hours, while longer reports with exact figures are sent days after the incidents have been resolved (Dekker et al., 2012).
- (d) Standards and frameworks driven by IT governance are deemed to be insufficient or overly complex for organisations to use or handle data-human issues.
- (e) Organisations' accountability for data-human issues also extends to notification of personal data breach or the right to know about breaches. However, data-human issues are beyond accountability principles. Instead, ethics – covering not just accountability – are necessary for dealing with data-human issues. This is indicated in conferences/workshops⁶⁷ featuring digital ethics or ethics as topics of discussions in data protection and privacy harm.

In general, organisations are reluctant to disclose information on security breaches, and personal data incidents are commercially sensitive in nature. Hence most security incident data are viewed as incomplete or misleading and any assessment or quantification of risks needs to address this issue. Muntermann and Roßnagel (2009) highlighted that organisations under-report computer security incidents in order to avoid loss of confidence, or over-report the value of incidents in order to get the police interested. Investigation of security incidents is hampered by general mistrust of any outsider who wants to obtain data on an organisation's information security issues. This issue imposes scoping and limitation challenges for this research which involves DBI response in organisations.

In terms of potential solutions to explore, the initial literature search indicated that triage is used by CERTs/CSIRTs in incidents (Mundie et al., 2014), and in digital forensics investigation (Rogers et al., 2006). In digital forensics, one of the primary responsibilities of investigators is to protect people and organisations from further harm (Casey, 2013).

Also, this researcher is interested in visual frameworks, especially a visual framework incorporating a semiotics approach/methodology. Semiotics have, in recent history, been used by researchers (Liu and Li, 2015) in the health care fields. Such studies have stimulated this researcher's interest in employing Peirce semiotics for DBI response studies.

⁶⁷ This researcher attended a workshop for data protection and privacy and ethics: 4-October-2016 GDPR Workshop Series: The GDPR and privacy impact assessments: http://www.brusselsprivacyhub.org/Resources/BPH_GDPR_Workshop_DPIA_Agenda_041016.pdf [Accessed 29-December-2018]. From talking with other researchers, ethics is featuring in PhD research topics covering data privacy (PIA) and security, though not in incident response frameworks.

At a privacy related workshop⁶⁸, privacy and ethics are key themes in projects⁶⁹ involving researchers and industry practitioners⁷⁰. For examples in the iTrack project⁷¹, *avoiding harm* is listed under key notions in ethics and data protection and privacy. The notion of *avoiding harm to people* whose personal data has been compromised or lost in a DBI or a security incident appears not to be an area of research in the computer science and security incident domains. Even back in 1998 Brownlee and Guttman (1998, p 15) listed *damage to systems* under categories of incident. The human or people aspects have not been the major focus then and even in this age of digitisation. As highlighted by Sir Tim Berners-Lee (TED.com, 2009) and Pollitt (2013), people are heavily interlinked and interweaved by data, especially personal data in technology.

Research studies about information security incident frameworks or models have mainly focused on the security protection principles of confidentiality, integrity and availability (CIA) (Howard, 1997). *CIA are necessary – but insufficient – conditions for information privacy* which also involves the ethical and legal use of the information (Burkert, 1997; Reddy and Venter, 2009). Hence information privacy has a wider range of potential violations and incidents (Reddy and Venter, 2009).

Moreover, even with security and process standards, procedures and policies to serve as overarching data governance principles, data breach incidents are not prevented from happening. This is shown in the Target data breach incident in which despite being Payment Card Industry Data Security Standard (**PCI-DSS**) compliant, and also with sophisticated security detection and monitoring systems in place, a major data breach was not prevented. Hardy (2014, p 51), states that Target's FireEye software detected the data malware and decoded the destination of the servers where the stolen credit cards were exfiltrated and stored. However, the detected alerts were ignored or disregarded by the security team (Cyphort, 2014). One reason given is that there were too many alerts generated on a daily basis, creating an alert overload.

In forensics investigation the principles of examination (e.g. the 3LevelModel) and also the principles as laid out in ACPO (2012) have been documented and cited. The 3LevelModel encompasses the design principles and guidelines for a forensics framework. The principles underlying triage in digital forensics investigations, although not mentioned in the reviewed literature, would have to meet the fundamental forensic principles as laid out in the forensic processes and procedures such as those identified in the 3LevelModel. Based on the reviewed literature, and with so many different frameworks and lacking standardisation, it is not clear whether researchers incorporated the 3LevelModel to include the triage principles when designing the forensics framework.

⁶⁸ The EU GDPR Privacy Impact Assessment, Brussels Privacy Hub workshop, 4 October 2016.

⁶⁹ The iTrack project: <http://www.itrack-project.eu/> and the Satori project: <http://satoriproject.eu/> [Accessed 29-December-2018].

⁷⁰ Researchers at <http://www.brusselsprivacyhub.org/> and practitioners at <http://trilateralresearch.com/> [Accessed 29-December-2018].

⁷¹ At the Brussels Workshop, a PhD researcher described a Data Protection Impact Assessment (DPIA) approach for the iTrack project. According to the presenters the DPIA approach has also been applied in other projects.

2.3.2 Ethical triage for DBI response

Triage, if applied in the early phases of DBI, should also enable organisations to assess the *data harm to individuals* affected by the data breach or data loss. A triage playbook then is intended for use in the early or initial stages of a DBI.

This researcher views **to sort (to prioritise)** to be the **third or final step** in triage. First there is **to verify** (*who needs treatment – dangerously wounded?*) then **to assess** (*the degree of injury or wound?*) and finally **to sort** (*who gets immediate treatment?*). *How do these translate into practice in a DBI scene?* A DBI scene in a commercial organisation shares similar incident characteristics to a clinical scene in a hospital⁷². Both are *on-scene* if viewed in terms of *where the incident occurred or where the investigation starts*.

Context: Sorting patient for treatment in a hospital; ***sorting privacy harm to individual for incident response and notification in an organisation*** (DBI in ***bold italics***)

These characteristics or conditions are:

- (a) There is an element of urgency; (prognosis⁷³ for immediate treatment; ***the right to know – notification to individuals***).
- (b) People are involved; (injured/sick patient; ***individual's personal data***).
- (c) Scarce resources (medical staff/resources vs number of patients (potentially exceed staff) and/or diagnostic tools/medicine are not available; ***speedy notification required (e.g. 72 hours under GDPR) and little and/or Big Data scenarios i.e. trustworthy or reliable incident information not easily obtainable or available during the early stages or hours of incident response***).

The triage activities of *to verify, to assess and to prioritise* (**Triage DBI response**) are shown in Figure 2-11 p 61. Hong et al. (2013) raised the need to address privacy protection which varies in different countries, and the demand for a triage model that protects privacy, and at the same time supports the needed decision making. In the case of DBI, personal data when compromised or lost, is no longer under the control of the rightful (Layton and Watters, 2014) or legitimate owner(s). In conducting triage especially where personal and sensitive data are involved, the benefits of using triage may be trumped if the processing of such personal data are deemed to have fallen foul under the GDPR⁷⁴. or other mandated rules on handling of personal or client/customer data Before GDPR, ENISA (2012)⁷⁵ examined breach notification and recommended a procedure for handling personal data incidents. Their flowchart was extracted and shown in Figure G- 1 p 216. In the same document, a flowchart for *Information security event and incident flow*, showed three main stages⁷⁶ i.e. *Detection and Reporting, Assessment and Decision*, and *Response*. The *Response* stage gets triggered when the information security incident is

⁷² For simple analogy of these two entities, assume that the organisation and the hospital have the same level of maturity for people, process and technology, and both have a triage plan in place. Kerrigan (2013) researched a capability maturity model for digital investigations.

⁷³ In clinical practice, triage is used as a decision rule to predict urgency of care (prognosis) (Moll, 2010).

⁷⁴ Article 6 (c), (d) were relied on for *lawfulness processing* of incident response processing by organisations.

⁷⁵ The ENISA (2012) report was for the ePrivacy Directive which stipulated a 24 hrs breach notification.

⁷⁶ The last two stages are *Review* and *Improve*. The flowchart was not extracted as it did not show anything about DBI.

confirmed. Although there was no mention of triage in the document and in the flowcharts, the *Assessment and Decision* stage has a two steps *information collection* and *Assessment* phases. This was similar to an initial triage with questions leading to subsequent triage before the *Response*. It appears that ENISA (2012) implicitly⁷⁷ applied the triage incident description outlined by Brownlee and Guttman (1998). However, the triage incident description as shown in the flowchart in Figure G- 1 p 216 was primarily for responding to a security incident rather than for assessing privacy harm to affected individuals.

Although there is no literature concerning triage for DBI, there are several data breach solution providers⁷⁸ offering DBI response-related services. Most of them offer incident handling and incident response management-related services with little discussion on the use of triage. CISCO⁷⁹ has described triage in: *Initial Analysis and Response; The first phase of incident response is to verify that the event is an actual security incident... After the event is confirmed, take quick action to limit the damage. Again, the purpose of triage is to limit the damage.*

2.3.3 Synthesised triage processes (RO1-1)

As stated in Figure 2-1 p 30, one of the aims of the SSM was to synthesise existing incident frameworks/models or incident approaches. A list of incident stages and phases as shown in Figure 2-10 p 61, has been extracted and aggregated from the synthesis of existing forensics frameworks, standards and best practice guidelines. The main sources were from SEI-CMU in Killcrece et al. (2003), ENISA (2012), ICO (2012a), and the incident lifecycle management process from NIST SP 800-61 and ISO/IEC 27035-2011 as reported in Tøndel et al. (2014).

In Figure 2-10 p 61, the phases below the dotted red horizontal line are the response activities. An initial list of triage DBI entities (Triage DBI response) was also synthesised from the literature review as shown in Figure 2-11 p 61. The research methodology is discussed in the next chapter.

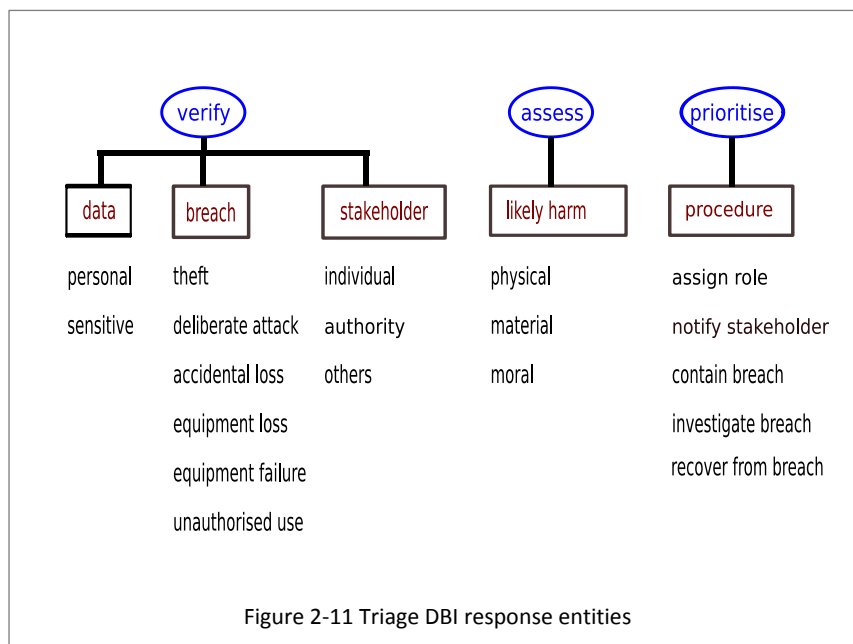
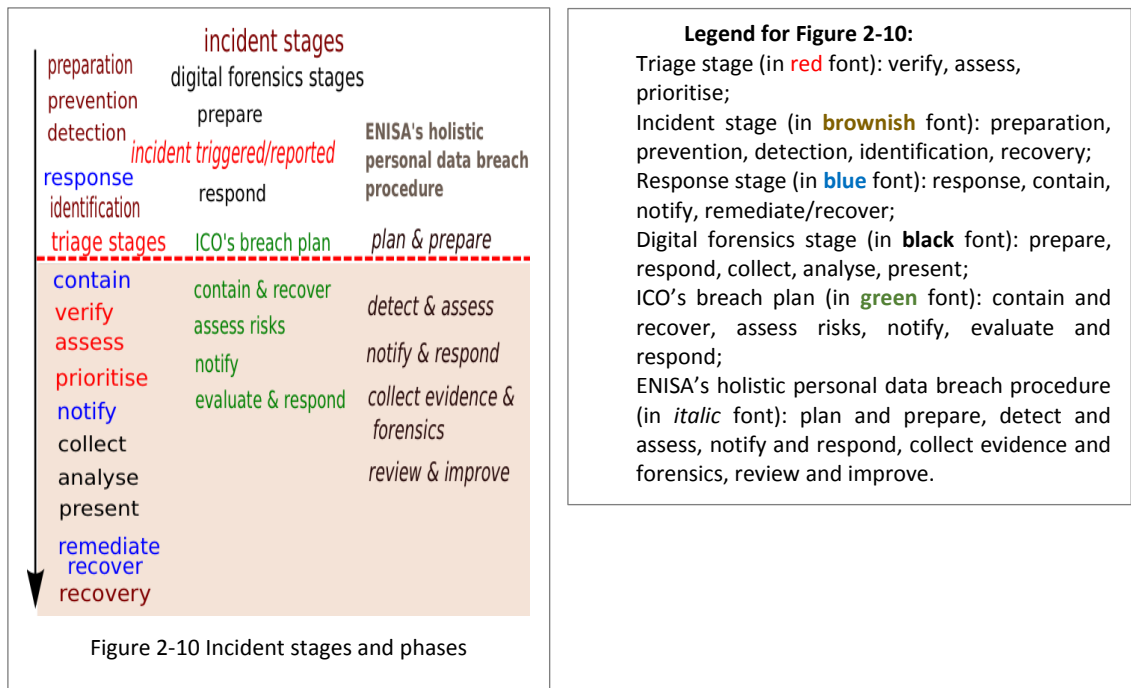
⁷⁷ No specific mention on triage and/or references to triage principles or descriptions.

⁷⁸ For examples [Accessed 29-December-2018]; Resilient Systems: <https://www.ibm.com/security/intelligent-orchestration/resilient>

AlienVault: <https://www.alienvault.com/resource-center/ebook/insider-guide-to-incident-response>

Kroll: <http://www.kroll.com/en-us/what-we-do/cyber-security/investigate-and-response/incident-response-management>

⁷⁹ <http://www.cisco.com/c/en/us/about/security-center/worm-mitigation-whitepaper.html> [Accessed 29-December-2018].



Chapter 3 Research Methodology

This research adopted a research methodology i.e. Design Science Research (DSR) that has been driven by the nature of the research question, aim and objectives. Also, motivation as discussed in Chapter 1 underlines the practical business problem addressed in this research. As the nature of this research direction was not focussed on collaborating or working in partnerships with a specific organisation⁸⁰ to address that organisation's concerns or goals, the alternative to DSR i.e. Action Research was examined but not adopted. Furthermore to address the research question, DSR addresses practical problem through design and the outcome is an artefact; Action Research does not require an artefact to be part of the solution (Johannesson and Perjons, 2014, p 83) and normally conducted and evaluated within a specific organisation or client (Iivari, 2007).

For an overall research methodology, the DSR framework (Section 3.3) by Vaishnavi et al. (2017)⁸¹ provided the lens for guiding, structuring and describing the various research activities and processes. Also, DSR frameworks may include a research process and are more generally used *to establish a research base and contribute to the augmentation of the knowledge base through scientific investigation* (Offermann et al., 2009). Besides the DSR methods (activities and processes), the ontological and epistemological assumptions, i.e. the philosophical grounding of DSR are explicitly presented in the DSR methodology as described by Vaishnavi et al. (2017).

The DSR methodology provides the guiding principles orientating on *problem relevance* (Hevner et al., 2004) with the focus on developing technology-based solutions to the important and relevant business problems (Venkatraman et al., 2016). To address the business issues, this research created a conceptual model to include the people or organisational elements into DSR. DSR is discussed in Section 3.2. However, DSR has been criticised for its lack of focus on *problem situation* (O'Keefe, 2014), and also for not addressing societal issues (Fink and Nyaga, 2009). Similarly, Myers and Venable (2014) pointed out that in all the current DSR guidelines and methods, none engage in *ethical considerations*. Instead the focus has been on the *viability, efficiency, and effectiveness of artifacts*. In any research, including DSR, ethics and other values are invariably present i.e. not *value-free* (Iivari, 2007). Vaishnavi et al. (2017) recognised and stressed that little attention is given to the different or diverse *values* – the axiology – that each researcher and community brings in the pursuit of knowledge. Axiology⁸² is significant for this research, involving data privacy, whereby diverse stakeholders, including this researcher, attached their own or collective values to privacy and privacy harm. Axiology is the study of values i.e. *what values does an individual or group hold and why?* (Vaishnavi et al., 2017).

Besides, Iivari (2007) examined the five stages of Nunamaker et al.'s (1990)⁸³ process model for systems development research with the theory building, experimentation and observation activities

⁸⁰ E.g. ENISA was contacted in December 2015 with the intention to do collaborative action type research, but this did not materialise.

⁸¹ Their 2011 version was used by Wilson (2013). Piirainen et al. (2010) cited their 2004 version. Also, the authors claimed they have a combined 70+ years of DSR experience.

⁸² Search on *axiology and design science* in Scopus.com retrieved a total of two papers; *axiology and design science research* in city.ac.uk/library retrieved 11 papers. None in IEEE. Little discussion on axiology and privacy. [Accessed 25-August-2018].

⁸³ A widely cited paper and also examined by Hevner et al. (2004) for their influential DSR paper.

found in other research activities. livari (2007) pointed out that only the *first* and the *last* stages of the five stages: *construct a conceptual framework, develop a system architecture, analyse and design the system, build the (prototype) system and observe and evaluate the system*, are related to other research activities. Furthermore, the first stage is where relevant disciplines for new approaches and ideas are studied.

Given that the outputs from this research consisted of various types of exploratory and investigative data i.e. interview results, questionnaire results, transcripts and prototype dashboard, a hybrid Thematic Analysis (Chapter 4) and a multi-method user evaluation (UES) approach (Chapter 6) were adopted. Furthermore, Venable et al. (2012) in highlighting that there is an *evaluation gap*, proposed a comprehensive DSR evaluation framework, they then suggested that *further research is needed to gain more experience* to use it. In adopting the DSR framework from Vaishnavi et al. (2017), their evaluation (and validation) method – which is a *crucial* activity, requiring *thorough evaluation* of the artefacts (Hevner et al., 2004) – *can vary and can range from logical arguments to experimentation or mathematical proof*.

In the UES approach, storytelling was used to account for the users' stories (deductive-inductive) about the prototype dashboard. The users' stories were also interpreted and reflected in Chapter 7. In using a prototype in the iteration with users, new ideas emerged which were reflected upon. Prototyping and emergent knowledge processes in DSR have appeared in literature, e.g. Markus et al. (2002) and mentioned by Hevner et al. (2004) and Vaishnavi et al. (2017). Reflection on the outputs/results that have emerged is an essential part of circumscription⁸⁴ in DSR (Vaishnavi et al., 2017).

The focus of this research was not on design theory or building a theory for design or a theory for DSR. Research theorising and Charles Saunders Peirce (Peirce)'s pragmatism were discussed (Section 3.1) to justify the adoption and application of DSR methodology (Section 3.4) and the pre-theory framework by Baskerville and Vaishnavi (2016) (Section 3.3.2).

3.1 On Research theorising

What has been challenging was to find research theorising on the nature of this research. This researcher's professional background has primarily revolved around seeking for practical applications of technological solutions to business problems. Applying this practical need into research theorising proved to be challenging in terms of finding a theory that encompasses and straddles across the interdisciplinary nature of this research.

In reviewing the research approaches mentioned in the literature reviewed in Chapter 2, one striking pattern that emerged was that there is no one single research theory or philosophy that has been used by researchers in the security incident and privacy domains. Although triage has been used in digital forensics, there is little research done on the use of triage for dealing with DBI response. Moreover, changes in technology meant that the practical application of triage is domain specific – specific to the types of technological developments and specific to the digital evidential standards set by courts of law.

⁸⁴ The circumscription process is especially important to understanding DSR process because it generates understanding that could only be gained from the specific act of construction. It assumes that every fragment of knowledge is valid only in certain situations and it contributes valuable constraint knowledge to the understanding of the always-incomplete-theories that abductively motivated the original research (Vaishnavi et al., 2017).

These contextual issues are challenging for incident and forensics framework designers as shown by the lack of standardisation and design approaches which have been driven by researchers' understanding of specific issues in specific domains or situations. Hence frameworks and models, for example the i* framework and the digital forensics frameworks have been extended or re-designed by other researchers based on their own understanding of specific issues or domains.

Then there are the issues with the different approaches to privacy harm with its own legal constructs or nuances and the different approaches for addressing privacy protection via system vulnerabilities in system design and risk driven PIA. Although the digital forensics principles provide the scientific rigor for the forensics investigations, the incident response processes or activities are based on the collective experience and practice of the community of incident practitioners and researches. In particular, the triage concepts and principles are based on humanitarian law and medical ethics. In this research, triage was conceptually derived from the literature review. The interview study revealed triage, though not fully described, is used during DBI. Peirce's semiotics and ternary (Section 3.1.2) were explored to describe and structure triage such that it can be designed or operationalised for use during DBI response.

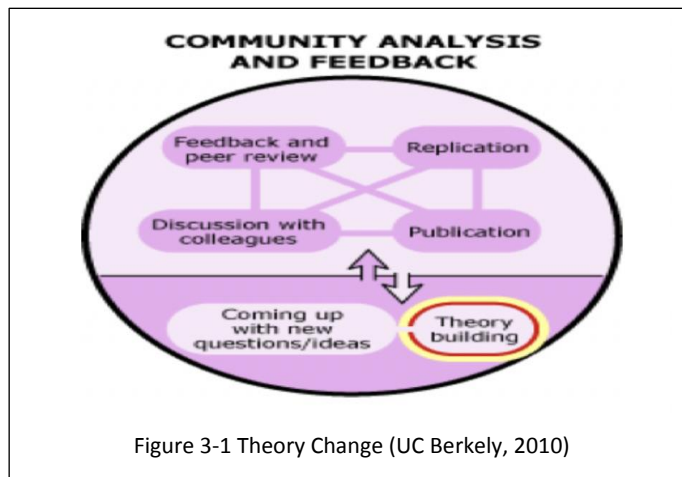
Finding a theory that can be applied across these disciplines – scientific and social-humanity – is itself too advanced as a research topic. This was not attempted here as Hunter (2006) has already examined works of well-known philosophers ranging from Jameson to Derrida and argues that *it is fruitless to begin a history of theory by trying to identify its common object or shared language because there is none*. The full extent of Hunter's (2006) work was not reviewed here but Lorenz (2011) has reviewed Hunter (2006) and agrees with the observation that there is no unified *common object* of theory, and there is no unified shared language of theory.

Although the word *theory* is not universally interpreted in the context of design theory in DSR, Chatterjee (2015) offer this: *A theory describes a specific realm of knowledge and explains how it works*. Another comes from Johannesson and Perjons (2014, p 31): *Theories are key instruments for structuring and organising large bodies of scientific knowledge*. In adopting DSR for this research, these *theory-knowledge* descriptions provided an anchor when discussing knowledge contributions or the epistemology of this research. In particular Baskerville and Vaishnavi (2016) provide a pre-theory design framework which describes the pre-theory processes used for the conceptualisation of the triage playbook. Using the pre-theory approach, the triage playbook is a pre-theory design framework (Section 3.3.2) with the potential to emerge into a design theory. Furthermore, Vaishnavi et al. (2017) pragmatically expressed that (full) theory creation is not expected from a single DSR project as it requires a community effort. Baskerville and Vaishnavi (2016) also said that *for theory to be eventually generated the research community needs to dabble in pre-theory design frameworks*.

Although Offermann et al. (2010) pointed out that no consensus exists about which epistemology and ontology should be assumed in DSR, the epistemology of DSR as described by livari (2007) was acknowledged by Hevner (2007). Being a pragmatic researcher, a *no consensus* view is expected as also expressed by Vaishnavi et al. (2017): *depending on the type of knowledge contribution and the state of knowledge in the area of research, the expectations on the nature and depth of knowledge contribution outputs can vary*.

Cross (2001) on Design Science⁸⁵: *refers to an explicitly organized, rational, and wholly systematic approach to design; not just the utilisation of scientific knowledge of artifacts, but design in some sense as a scientific activity itself also stresses the need to focus on the designerly ways of knowing, thinking and acting.* Similarly, Rossi et al. (2013) state the need to balance the *doing and thinking* about DSR – which aligns with the pragmatism paradigm (Section 3.1.1).

One observation is that theory (scientific and non-scientific) needs to change with the changing nature of the phenomenon under observation/investigation. In this research the phenomenon under investigation is interdisciplinary in scope and finding a *common object and a shared language* needs a theory that *communicates or transcends* across the diverse community of practitioners and researchers. On the nature of theory, UC Berkely (2010) offered *theory change* which describes a *community process of feedback, experiment, observation, and communication.* It usually involves *interpreting existing data in new ways and incorporating those views with new results.* The *theory change* diagram, as shown in Figure 3-1 p 65, describes the community approach as seen in the DFRWS (2001) and in the many forums/workshops/events of community of knowledge and theory building.



Pursuing this researcher's interests in visualisation and practical solutions led to the discovery of semiotics⁸⁶, in particular Charles Saunders Peirce (Peirce) semiotics and ternary (Peirce semiotics-ternary). In investigating visual communication theory, Professor Sandra Moriarty (Moriarty) pointed out the only consensus is that there is confusion, not only about what the phrase visual communication means, but what it represents to us as a field. Moriarty also recognised that the tension between theory and practice is one of the assets of the area/discipline of visual communication, one that also crosses over all the borders and divisions of our various disciplines (Moriarty, 1995). Although there is no universal visual communication theory and no single theory or philosophy that has been used by researchers in the security incident and privacy domains, Peirce semiotics-ternary has been used by researchers across domains or disciplines. As this research cuts across disciplines, Peirce semiotics-ternary was adopted for

⁸⁵ Design Science also used for DSR as noted in Hevner et al. (2004) i.e. design science, sciences of the artificial or a design-science paradigm. *Design research (DR) is research about design whereas DSR is primarily research using design as a research method or technique* (Vaishnavi et al., 2017).

⁸⁶ This researcher's blog on why semiotics at <http://jollyvip.com/research/2016/08/12/why-semiotics/> [Accessed 29-December-2018].

this research (Section 3.1.2). Interestingly, the community approach in the theory change is what underlies Peirce's pragmatism and his three modes of inquiry or inference i.e. abduction, deduction and induction (Section 3.1.1), and these are embedded in the DSR methodology which are described in Section 3.2.

3.1.1 Peirce's pragmatism and modes of inquiry

Peirce in the 1870s proposed that pragmatism is a method of inquiry and an account of meaning. The crux of Peirce's pragmatism is that for any statement to be meaningful, it must have practical bearings. This is because the practical bearings then play the role of context and meaning comes from context. Peirce saw the pragmatic account of meaning not only as method aiding scientific inquiry, but also as *a method of sorting out conceptual confusions by relating meaning to consequences*⁸⁷. Peirce described his pragmatism as the philosophy of the laboratory scientist whereby the search for knowledge, *inquiry*, arises from the need to settle *doubt* arising from normal inquiry. The method to alleviate the *doubt* involves a *fallibilistic process in which a community of investigators puts forward theories, tests them and revises them in light of falsifications* (Baggini and Stangroom, 2004, p 182). Vaishnavi et al. (2017)⁸⁸ illustrated this view with an example of community driven DSR outputs⁸⁹.

Peirce's view on the scientific method of inquiry⁹⁰ or inference is stated as: the testable consequences derived from an explanatory hypothesis constitute its concrete meaning. This determines the admissibility of a hypothesis as a possible (meaningful) explanation (Audi, 1999, p 652). Furthermore, according to Peirce: *our ideas and theories must be founded in experience and linked to the practicalities of that experience. It is the nature of that link and its significance of human understanding and knowledge that are the focus and business of pragmatism* (Plowright, 2016, p 14-15). Creswell (2003) expressed pragmatism as *what works and a practice for solutions to problems*.

As this exploratory research involved qualitative inquiry i.e. interview study and user evaluation study, where data were collected and analysed, Sandelowski (1986) pointed out that a scientific approach to qualitative inquiry emphasises the standardisation of language, rules and procedures for data collection and analysis, for ensuring the replicability and validity of findings, and for presenting the results. A key point in adopting a data collection method is the quality criteria: a) replication (study is capable of replication – rare in qualitative type research according to Bryman and Bell (2015, p 50)), b) validity (integrity of the conclusions), and c) reliability (repeatable results) provide the guiding criteria for business research (Bryman and Bell, 2015, p 48). Besides the data collection method, the data analysis used in this research followed the DSR modes of inference which are based on Peirce's three modes of inference: *abduction – the initial formulation of the hypothesis to explain the phenomena; deduction – the deriving of consequences from this hypothesis; and induction – the testing of the hypothesis against experimental evidence* (Baggini and Stangroom, 2004, p 182).

⁸⁷ <http://www.iep.utm.edu/peircepr/> and <http://mesosyn.com/peirce.html> [Accessed 29-December-2018].

⁸⁸ They also gave an exemplar of IS DSR.

⁸⁹ Outputs include the DSR artefacts and also the research objectives, the proposal and requirements.

⁹⁰ According to Pierce, inquiry is always dependent on beliefs that are not subject to doubt at the time of the inquiry, but such beliefs might be questioned on some other occasion (Audi, 1999, p 652).

There are various interpretations and ongoing⁹¹ debate on Peirce's abduction (e.g. Flach and Kakas, 2000; Paavola, 2005; Åsvoll, 2014). In terms of Peirce's ternary, Åsvoll (2014) offers this: *abduction (Firstness) plays the role of generating new ideas or hypotheses; deduction (Secondness) functions as evaluating the hypotheses; and induction (Thirdness) is justifying of the hypothesis with empirical data.* According to Åsvoll (2014) the three asserted relations are: *one (melting) version among many which, therefore, represents simplifications. For example, abduction, induction and deduction are also modes of inference that permit patterns in our experience to be thought about.*

3.1.2 Peirce semiotics-ternary

[...] it has never been in my power to study anything, - mathematics, ethics, metaphysics, gravitation, thermodynamics, optics, chemistry, comparative anatomy, astronomy, psychology, phonetics, economics, the history of science, whist, men and women, wine, metrology, except as a study of semiotics – (Peirce, 1953).

The above quote is a testament of the relevance of the study of semiotics as nowadays Peirce's semiotics have been used by researchers across domains or disciplines. Some examples: law (Pearson, 2008) and (Beebe, 2003); visual communication (Moriarty, 1994a); information and organisational semiotics by Ronald Stamper (Gazendam and Liu, 2005) and works by Mingers and Willcocks (2014); computing/computation (Tanaka-Ishii, 2015); education (Plowright, 2016); a dedicated website i.e. Peirce Edition Project⁹² and others.

Peirce semiotics is itself described by Peirce as a theory of inquiry. It has inspired various semiotics enabled or derived theories such as visual semiotics theory (Moriarty, 2005), a semiotic theory of information and a theory of semiotic engineering highlighted in Mingers and Willcocks (2014). Although Peirce semiotics have not appeared in privacy and incident response literature, Moriarty (2005) discussed it for visual theory development, analysis or interpretation and also in Moriarty and Sayre (2005). Visual ethics theory has been discussed in Newton (2004) and in Newton and Williams (2010). In both articles, although written with visual journalism and visual media in mind, the power of visual has been tapped to make visible in some way that which has been previously invisible – the ideas, expressions, judgments and stories (Newton, 2004). Newton and Williams (2010) referenced Peirce semiotics indirectly via Moriarty (1994b), and developed visual ethics around the study of *how images and imaging affect the ways we think, feel, behave, and create, use, and interpret meaning, for good or for bad.*

The wide applicability of Peirce semiotics is attributable to the study of signs or semiotics which has been referred to as the multidisciplinary study of information, meaning, communication, interpretation, sign systems and evolution, texts, interactions, organizations, cultural and social transformations, sense-making and all other topics that may emerge from future research, models and theories⁹³.

Peirce semiotics differs from semiology (also a study of signs) which has its foundation laid down by Ferdinand de Saussure (Saussure), a Swiss-French linguist (1857-1913). Saussure semiology centered in the study of language and the two-part sign relationship between a signifier and its signified. Saussure

⁹¹ One reason for the controversies is attributable to Peirce's mind change (Flach and Kakas, 2000).

⁹² Peirce Edition Project by Indianapolis University - Prudue University Indianapolis: <http://peirce.iupui.edu/> [Accessed 29-December-2018].

⁹³ The Semioticon Community at <http://semioticon.com/> [Accessed 29-December-2018].

semiology primarily focuses on how meaning is created through words and his work as well as that of his followers largely concentrates on linguistic based theories and forms of analysis (Moriarty, 1994b). Peirce, an Anglo-American philosopher and scientist (1839-1914) enhanced and extended Saussure's two-part sign (dyadic) relationship between a signifier (the form which the sign takes) and signified (the concept it represents) into a tripartite or ternary system of sign (triadic) relationship between a representamen, an object and an interpretant. The introduction of an object into the study of signs changed not only the interpretant relationships with the representamen (and vice-versa) but also widens the scope and power of Peirce semiotics beyond the field of linguistics. In the words of Peirce:

A sign (representamen) is something which stands to somebody for something in some respect or capacity. It addresses somebody, that is, creates in the mind of that person an equivalent sign, or perhaps a more developed sign. That sign which it creates I call the interpretant (Peirce used the term, Thirdness) of the first sign. The sign stands for something, its object (Secondness). It stands for that object, not in all respects but in reference to a sort of idea, which I have sometimes called the ground of the representamen (Firstness) (Peirce, 1931-1958, 2.228, original italic emphasis) (Mingers and Willcocks, 2014).

However according to Chandler (2007) there is considerable disagreement about the details of the triadic analysis even among those who accept that Peirce's three elements/components (Peirce ternary) must be taken into account. Such disagreements are not examined here⁹⁴, instead instances of work in information systems and computer science that have referenced, and applied, Peirce's semiotics are commented on here.

Oliveira and Loula (2015) in clarifying that: *a sign is defined as something that refers to something else, an object (which the sign represents in some respect) and produces an effect (interpretant) in the interpreter*, applied Peirce's semiotics as their theoretical background to define and classify representations in neural networks of creatures in a previously proposed experiment on the emergence of communication. Mingers and Willcocks (2014) in developing an integrative semiotic framework for information systems, rejected Saussurian-based post-structuralist uses of semiotics and argued that Peirce's semiotics in including the referent provides a more aligned theoretical and philosophical integration. Furthermore, according to Everaert-Desmedt (2011), the Peirce ternary of three categories of *Firstness*, *Secondness* and *Thirdness* is necessary and sufficient to account for all human experience. These three categories can be found to be present (at different levels) in every phenomenon i.e. the three universal categories that underlie Peircean semiotics which he called *pragmatism*.

3.1.2.1 Peirce ternary

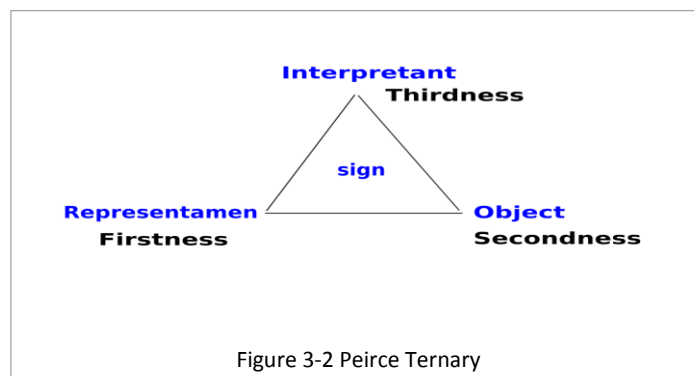
Peirce's insights on signs: *we think only in signs and nothing is a sign unless it is interpreted as a sign*⁹⁵. Anything can be a sign as long as someone interprets it as *signifying* something – referring to or standing for something other than itself. We interpret things as signs largely unconsciously by relating them to familiar systems of conventions. It is this meaningful use of signs which is at the heart of the

⁹⁴ Disagreements are around the different philosophical underpinnings.

⁹⁵ The source is from Chandler (2007) who cited: Peirce, C. (1931-1958). *Collected Papers of Charles Sanders Peirce* (8 Volumes) Cambridge: Harvard University Press.

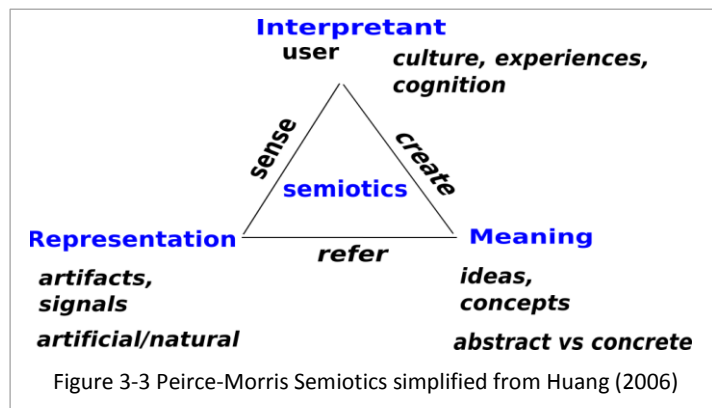
concerns of semiotics (Chandler, 2007). Semiotics studies the processes that lead signs to have particular meanings, and the ways in which such meanings are communicated and have effects (Mingers and Willcocks, 2014)⁹⁶. These interpretation and meaning-making processes (semiosis) revolve around the way each of the triadic relationships are continually interpreted or communicated. To show this semiosis, Peirce developed elaborate logical taxonomies of types of signs. The Peirce sign is based on three dimensions – the *representamen* itself, its relation to the *object* and its relation to the *interpretant*. Peirce classed these dimensions as *Firstness*, *Secondness* and *Thirdness* (commonly referred to as Peirce’s triad or ternary), and these dimensions or categories have been used to generate ten further categories (Everaert-Desmedt, 2011; Mingers and Willcocks, 2014). Lazanski and Kljajić (2006) use Peirce’s ternary for complex systems modeling and provide a comprehensive description⁹⁷: *Firstness is the mode of being of that which is without reference to any subject or object. Firstness may be manifested by quality, feeling, freedom, or multiplicity and is a quality but not a relation. Secondness is the mode of being of that which is itself in referring to a second subject, regardless of any third subject. Secondness may be manifested by action, reaction, causality, reality, actuality, or factuality. Thirdness is the mode of being of that which is itself in bringing a second and a third subject into relation with each other. Thirdness brings firstness and secondness into relation with each other and mediates between them. Thirdness is the mode of being of signs, in that signs mediate relations between their objects and their interpretants. Thirdness may be manifested by representation, thought, continuity, order, unity, or generality.*

Also the Peirce sign has been represented pictorially by a triangle as shown in Figure 3-2 p 69 by Mingers and Willcocks (2014); Everaert-Desmedt (2011); Lazanski and Kljajić (2006) and more comprehensively by Huang (2006). Huang’s (2006) diagram of the Peirce-Morris semiotic framework was examined and simplified as shown in Figure 3-3 p 70.

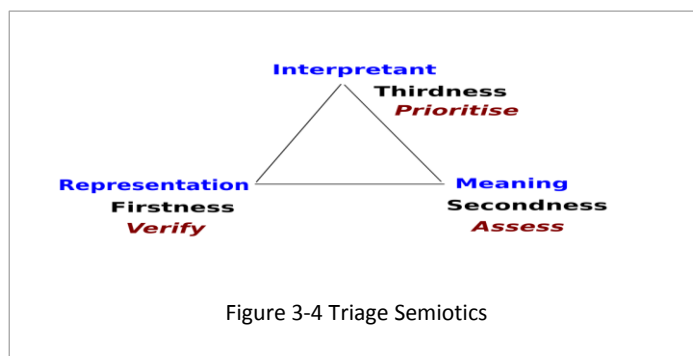


⁹⁶ There are many references on studies that have used semiotics, for examples in business, Human Computer Interface, IS and IT.

⁹⁷ Synthesised from Peirce’s work: The Essential Peirce: Selected Philosophical Writings.



Using Peirce ternary and the simplified Peirce-Morris semiotic framework, the identified (Chapter 2) triage activities of *verify*, *assess* and *prioritise* are aligned and mapped as shown in Figure 3-4 p 70 Triage Semiotics.



The Triage Semiotics show the order of the triage sequence of steps i.e. verify, assess and prioritise. This sequence of steps was used in the triage playbook for conducting the initial DBI response activities.

3.2 Design Science Research (DSR)

DSR is a design-science paradigm that has been used in computer science (Eze, 2013), information systems (e.g. Hevner et al., 2004; Peffers et al., 2007; March and Storey, 2008), engineering and medical sciences (Souza De Souza, 2015). Furthermore, DSR supports the creation and evaluation of IT artefacts with the intention to solve identified organisational problems (Hevner et al., 2004). In adopting DSR, artefacts can be abstracted and generalised such that the artefacts constitute a new scientific knowledge contribution (Eze, 2013).

DSR was chosen as it provides systematic and rigorous methodology for producing novel research artefacts which can be building blocks towards solving both practical and theoretical Computer Science problems (Eze, 2013). As succinctly stated by Souza De Souza (2015): *DSR methodology is based on the development of solutions to solve practical problems*. Besides, van Deursen (2013) in adopting DSR for developing a risk method for assessing socio-technical information security risks, argued that *information security is a multi-disciplinary and socio-technical topic of study, characterised by the entanglement of people, organisations, information and communication technology (ICT), and the environment*. On the

other hand, Fink and Nyaga (2009)⁹⁸ raised a *significant* limitation of DSR in that its narrow perspective excludes societal issues. This is so as the *people or elements of organisations* is excluded in the DSR definition/description and *in the process by which such artefacts evolve over time* (Hevner et al., 2004). Hevner et al. (2004) though acknowledged this: *IT artifacts not as independent of people or the organizational and social contexts in which they are used but as interdependent and coequal with them in meeting business need*. O’Keefe (2014) highlighted the need to address the *problem situation* and to *ask critical questions about the value of the system across those with differing values, beliefs, philosophies and interests* i.e. the axiology⁹⁹ aspects. In practical terms, Johannesson and Perjons (2014, p 3-4) beside providing a simple description of *artefact* also offer a way to represent the artefacts and their environments which include the people aspects. Their artefact diagramming approach was used to draw the high-level conceptual view of the triage playbook (Figure 5-3 p 113). This then ensures that the artefacts are conceptually designed with the intention of addressing the people or organisational aspects in specific domain¹⁰⁰ situations or *problem situation* driven modelling.

As noted by Hanid (2014) and O’Keefe (2014) there are many different models of DSR, and the starting challenge for this research was to find a specific DSR approach (Gregor and Hevner, 2013) that allows the aim and objectives of this research to be achieved. *What is the philosophical grounding of DSR?* This is discussed in the next section.

3.2.1 Philosophical grounding of DSR

Hevner (2007) associates DSR with pragmatism¹⁰¹ as a school of thought that considers practical consequences or real effects to be vital components of both meaning and truth. The author also emphasised that DSR is essentially pragmatic in nature due to its emphasis on relevance; making a clear contribution into the application environment. As regards the philosophical grounding of DSR, Hanid (2014)¹⁰² in an extensive analysis of DSR, stated that the research paradigm¹⁰³ – positivism, interpretivism, realism, critical theory, hermeneutics and phenomenology – are not centered toward practical problem solving which is DSR. Instead of examining these research paradigms, Vaishnavi et al. (2017) examined the philosophical assumption of three research perspectives i.e. positivist, interpretive and design under four basic beliefs i.e. ontology, epistemology, methodology and axiology. Their Philosophical Assumption of Three Research Perspectives diagram was extracted and shown in Figure 3-5 p 72. According to their synthesis, as research progresses through the DSR research cycle, the ontological and epistemological viewpoints also shift. This researcher also shared the same viewpoints in that Peirce’s pragmatism and the iterative *action-practical-feedback* nature of DSR aptly describe and address the shifting multi-world-states view of the nature of the phenomenon of this research. Hence, Amrollahi et al. (2017) adopted a

⁹⁸ Also raised by other authors.

⁹⁹ In O’Keefe (2014), axiology included ethical, aesthetic and spiritual consideration.

¹⁰⁰ This is a characteristic of domain-specific modeling to address complexity in transdisciplinary settings.

¹⁰¹ The author cites pragmatism as discussed by other DSR researchers, without mentioning Peirce's pragmatism. Vaishnavi et al. (2017) mention Peirce without further discussion.

¹⁰² Hanid (2014) did not develop or build the artefact from her conceptual model/framework.

¹⁰³ In this thesis, the terms are used as follows: Philosophy: the study of knowledge; paradigm: a way (approach) of looking at the world or problems (viewpoint/perspective); theory: system of ideas or beliefs or models.

multi-paradigm methodology which included DSR. Vaishnavi et al. (2017) also pointed out that by definition, DSR changes the state-of-the-world through the introduction of novel artefacts.

Basic Belief	Research Perspective		
	Positivist	Interpretive	Design
Ontology	A single reality; knowable, probabilistic	Multiple realities, socially constructed	Multiple, contextually situated alternative world-states. Socio-technologically enabled
Epistemology	Objective; dispassionate. Detached observer of truth	Subjective, i.e. values and knowledge emerge from the researcher-participant interaction.	<i>Knowing through making</i> : objectively constrained construction within a context. <u>Iterative circumscription</u> reveals meaning.
Methodology	Observation; quantitative, statistical	Participation; qualitative. Hermeneutical, dialectical.	Developmental. Measure artifactual impacts on the composite system.
<u>Axiology</u>	Truth: universal and beautiful; prediction	Understanding: situated and description	Control; creation; progress (i.e. improvement); understanding

Figure 3-5 Philosophical assumption of three research perspectives (Vaishnavi et al., 2017)

As can be seen, not all DSR researchers hold/share all the perspectives or aspects embedded in DSR methodology. Hanid (2014) in evaluating and synthesising five excellent DSR models (including Hevner's Three Cycles (2007)) into a three steps DSR process, also identified one critical shortcoming with DSR methods namely *method has not much to say from where the suggestion, or concept, for the solution comes, and how it will be developed towards the practically functioning artefact*. Hanid (2014) then proceeded by adapting DSR models by Vaishnavi and Kuechler (2007)¹⁰⁴ and Hevner (2007). However, in the recent DSR paper by Vaishnavi et al. (2017), Hanid's identified shortcoming was explained as: *suggestions for a problem solution are abductively drawn from the existing knowledge/theory base for the problem area*¹⁰⁵. For Vaishnavi et al. (2017), such suggestions make the problem a research problem as *they may be inadequate for the problem or suffer from significant knowledge gaps*. In Hanid's (2014) work, the shortcoming of DSR was justified with Peirce's abduction i.e. *the process of forming an explanatory hypothesis and it is the only logical operation that introduces any new idea* (Peirce, 1997) and the philosopher Laudan's (1978) hallmarks of scientific progress i.e. *the transformation of anomalous and unsolved empirical problems into solved ones*. Peirce provided abduction for logical thinking and explaining *facts* based on *observations*. This mode of abductive reasoning is commonly referred to as *inference to the best explanation* (Alturki and Gable, 2014)¹⁰⁶. However, theorising in DSR encompasses not only abduction but also deduction and induction as raised by Gregory and Muntermann (2011) and

¹⁰⁴ There is now a later 2015 edition. This was pointed out by Prof. Vaishnavi in an email exchange with him and also with Prof. Baskerville during 15 September - 8 October 2018.

¹⁰⁵ The authors cited an earlier (1931) Pierce paper, which was not mentioned by Hanid (2014).

¹⁰⁶ The authors cited Peirce's papers and another paper.

Lee et al. (2011)¹⁰⁷. In this research, abductive, deductive and inductive reasoning were used even though the adopted Vaishnavi et al. (2017) framework did not discuss induction under *Logical Formalism* as shown in Figure 3-6 p 74 DSR Framework.

As regards Laudan's (1978) contribution, it is the identification of conceptual problems that are generated in solving empirical problems (Smith, 1985). Furthermore, Laudan (1978) sees science as an enterprise essentially devoted to solving problems, rather than seeking truth (Gutting, 1980). This aligns with Peirce's pragmatism and abductive reasoning. *How can Peirce's abduction be applied for an observation?* Peirce's abduction:

The surprising fact, C is observed;

But if A would be true, C would be a matter of course;

Hence, there is reason to suspect that A is true.

Is privacy distress (a privacy harm) true as discussed in literature and interview results? In following Hanid's justification approach, and taking a real-world event, namely the TalkTalk DBI whereby victims have reported distress (Johnston, 2015), and using Peirce's abduction:

*The surprising fact, **TalkTalk victim's distress** is observed;*

*But if **privacy distress** would be true, **TalkTalk victim's distress** would be a matter of course;*

*Hence, there is reason to suspect that **privacy distress** is true.*

Furthermore, the UK Court under the DPA 1998¹⁰⁸ has recognised *distress* as a claimable damage (White & Black Ltd, 2016).

As noted by Hanid (2014), in Laudan's (1978) problem-solving model¹⁰⁹ the first step before addressing an ontological component is to address the conceptual problem. Hence the *Suggestion* phase as shown in Figure 3-6 p 74 and Figure 3-7 p 75 was the construction of a *conceptual model* (described in Section 5.1.1) for the proposed triage playbook. These figures and the adopted DSR framework are discussed next.

3.3 DSR Framework

Although Hevner et al.'s (2004) first canonised a set of principles for doing DSR, they did not address in detail the theory (Venable, 2006; Gonzalez, 2009; Vaishnavi et al., 2017) and/or knowledge i.e. the theorising aspects of DSR. Instead, they stressed the acting part with the rigorous DSR principles and a set of guidelines for performing and evaluating DSR to achieve relevance. In Vaishnavi et al. (2017)¹¹⁰ they reinforced the *theorising aspect* of DSR. In adopting Vaishnavi et al.'s (2017) DSR framework¹¹¹, as shown in Figure 3-6 p 74, with the corresponding outputs, the acting or doing and theorising aspects of DSR were addressed. Furthermore, the DSR framework has inherent process and activity cycles to ensure

¹⁰⁷ Search on *Theorizing in Design Science Research* in Scopus.com retrieved a total of four papers. [Accessed 24-August-2018]. These three modes of reasoning, although embedded in DSR are not fully discussed by most DSR researchers.

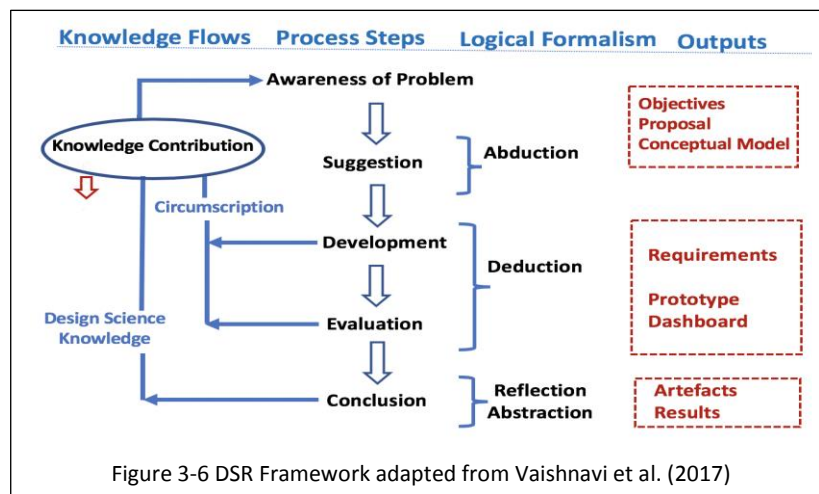
¹⁰⁸ Vidal-Hall v Google [2015] EWCA Civ 311 and TLT & others v Secretary of State for the Home Department and the Home Office [2016] EWHC 2217.

¹⁰⁹ Laudan's (1978) work/book was not examined by this researcher.

¹¹⁰ Their 2011 version was used by Wilson (2013). Piirainen et al. (2010) cited their 2004 version.

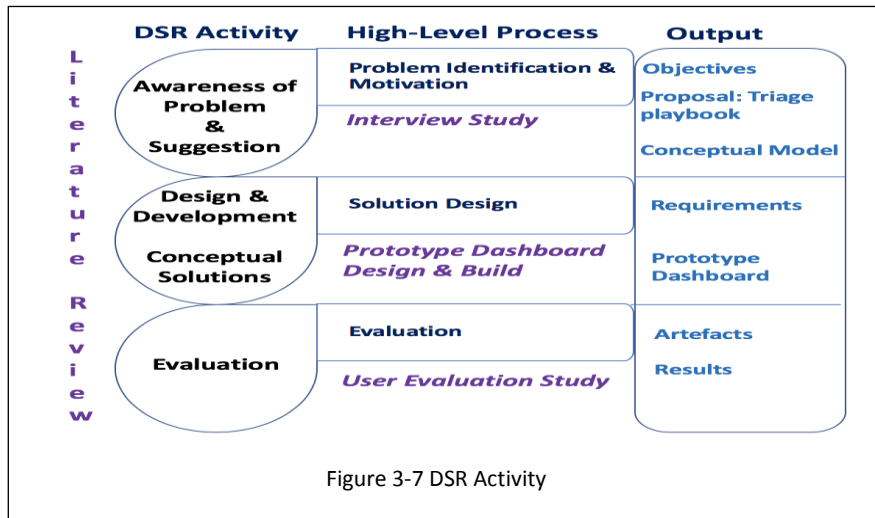
¹¹¹ The small red arrow is the conclusion of a research effort which needs to be appropriately positioned and research reported and make a strong case for its knowledge contribution (Vaishnavi et al., 2017).

rigor and relevance and also for emergent design properties in terms of pre-theory (Baskerville and Vaishnavi, 2016) as discussed next.

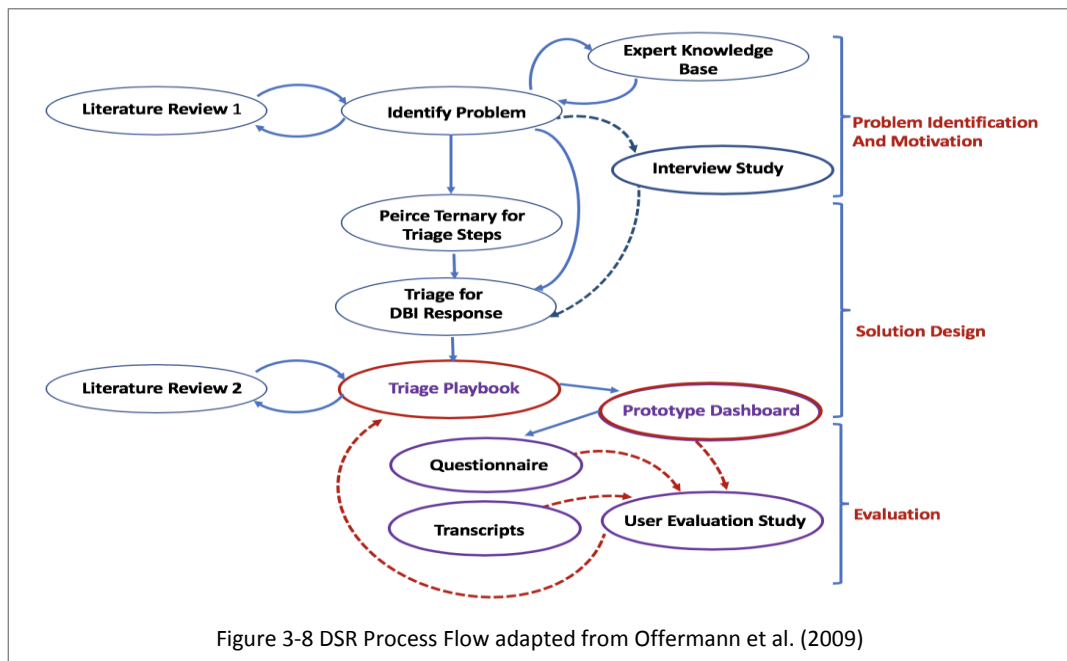


3.3.1 DSR activity and process

To show the iterative nature of the DSR process steps and the high-level activities, Figure 3-7 p 75 DSR Activity was created. This mapping of the DSR activity-process-output was synthesised from the *three cycle view* of DSR as described by Hevner (2007), Briggs and Schwabe (2011), and Chatterjee (2015). Briggs and Schwabe (2011) define three cycles for DSR: *a) the Relevance Cycle for gathering requirements and field testing; b) the Design Cycle for building and evaluating design artifacts and processes; and c) the Rigor Cycle for grounding design efforts in the knowledge base and contributing*. Chatterjee (2015) characterises DSR as three activities: *1) Discover Problems and Opportunities; 2) Design and Build Artifacts and Processes; and 3) Validate Artifacts and Processes*. In a DSR project, Hevner (2007) stressed that these three cycles i.e. *the Relevance Cycle, the Rigor Cycle and the Design Cycle* must be present and clearly identifiable. Without these three cycles, the intended rigor and relevance aspects of DSR may not be met. The interlinked and inherent cycles are described as: *The Relevance Cycle bridges the contextual environment of the research project with the design science activities. The Rigor Cycle connects the design science activities with the knowledge base of scientific foundations, experience, and expertise that informs the research project. The central Design Cycle iterates between the core activities of building and evaluating the design artifacts and processes of the research* (Hevner, 2007). In essence rigor was ensured by applying suitable methodologies and foundations i.e. the SSM literature review, the RITE approach and Peirce semiotic-ternary, and relevance was ensured by feedback from application in the appropriate environment i.e. the interview study and the User Evaluation Study (UES).



To provide clarity on the execution of the interlinked cycle of processes and activities, Figure 3-8 p 75, was adapted from Offermann et al. (2009). This approach was also pursued by Wilson (2013)¹¹² for his process flow for building a cloud-based simulator. In Figure 3-8 p 75, besides indicating the order of iterations, all data analysis flows top to bottom, with the bottom flow (shown in dotted red lines) being the final set of iterations for design, testing and evaluation of the dashboard. The interview study (methods in Sections 4.2 and 4.3 in Chapter 4) flows are shown in dotted blue lines. How these processes were applied is described in Section 3.4. One important feature of the cyclical processes in DSR is the emergent nature of the research (Baskerville and Vaishnavi, 2016). This is discussed next.



3.3.2 Pre-theory knowledge and framework

As raised by Vaishnavi et al. (2017) the activities carried out within the DSR phases (or cycles) and those in the design process (e.g. the Design and Build of the prototype Dashboard) are considerably

¹¹² In his Thesis, the referencing pointed to an incorrect paper by the same authors, Offermann et al.

different. The main difference is that contribution of new (and true) knowledge needs to be a key focus of DSR (Vaishnavi et al., 2017). The iterative and cyclical processes allow different levels of new knowledge or ideas/concepts to emerge and be validated (Baskerville and Vaishnavi, 2016). As observed by Iivari (2007), research into conceptual information modeling in the 1970s and into object-oriented systems development in the 1990s involved incremental improvements to existing artefacts.

Baskerville and Vaishnavi (2016) in theorising DSR process and structure, introduced the concept of pre-theory design frameworks (pre-theory frameworks). Their use of the term, pre-theory, has a broader meaning than that used to describe results of a research effort that are theoretically formative. Pre-theory in their design frameworks proceeds from a particular scientific effort such as in a single DSR project. In Baskerville and Vaishnavi's (2016) pre-theory framework, pre-theory concepts that are regarded *as not quite constituting theory* are considered as *promising basis for building a design theory*. Such pre-theory concepts are organised collectively into the pre-theory framework. According to Baskerville and Vaishnavi (2016) such frameworks are useful to guide DSR activities prior to the development of proper theory. Their pre-theory framework straddles between the *creative jumps from fragmented solution* to nascent design theory.

What makes their pre-theory framework relevant for this research is that they examined not only DSR design theorising authors but other design research¹¹³ approaches including agile DSR methodology and organisational problem settings. They also examined the DSR framework and processes as described by Vaishnavi et al. (2017) where they also discussed DSR theorising using a diagram¹¹⁴. For completeness, Vaishnavi et al. (2017) outputs of DSR were extracted and shown in Figure 3-9 p 76. Furthermore, Baskerville and Vaishnavi (2016) also described theorising for a *problem state* (i.e. O'Keefe's (2014) *problem situation*) with the use of prototype experimentation. Such prototype experimentation i.e. *in prototyping lab environment and the outcome of ongoing practice with the resulting artifacts, each of which may represent a progressively improved artifact-driven transformation of an environment from a problem state to a solution state* (Baskerville and Vaishnavi, 2016).

	Output	Description
1	Constructs	The conceptual vocabulary of a domain
2	Models	Sets of propositions or statements expressing relationships between constructs
3	Frameworks	Real or conceptual guides to serve as support or guide
4	Architectures	High level structures of systems
5	Design Principles	Core principles and concepts to guide design
6	Methods	Sets of steps used to perform tasks—how-to knowledge
7	Instantiations	Situated Implementations in certain environments that do or do not operationalize constructs, models, methods, and other abstract artifacts; in the latter case such knowledge remains tacit.
8	Design Theories	A prescriptive set of statements on how to do something to achieve a certain objective. A theory usually includes other abstract artifacts such as constructs, models, frameworks, architectures, design principles, and methods.

Figure 3-9 Outputs of DSR (Vaishnavi et al., 2017)

¹¹³ E.g. adapted from Offermann et al. (2009).

¹¹⁴ Their DSR theory diagram i.e. *Figure 6. Design Science Knowledge Hierarchy* was adapted from another author.

Their line of reasoning and the description of their pre-theory processes and framework mirrored closely the way the triage playbook was conceptualised i.e. the triage playbook is essentially a pre-theory framework. Baskerville and Vaishnavi (2016) in referencing other authors described the pre-theory processes: *For DSR, a pre-theory framework can be recognized as a formative collection of concepts that arises in early stages of design work as a preliminary means to negotiate the relationships between a messy set of requirements and a formative set of solutions. They involve accurate discrete functional explanations that justify each design feature vis-à-vis its requirements but retain a degree of incoherence as a collective. The collection is likely to be somewhat incomplete, include somewhat irrelevant concepts, and lacking a full understanding of the interrelationships among the concepts.* To show the level of knowledge contribution, Figure 3-10 p 77 was extracted from Baskerville and Vaishnavi (2016). As this research posited a claim that the triage playbook is a pre-theory design framework – based on the Baskerville and Vaishnavi (2016) description and their pre-theory concepts – a diagram was created to show the various triage concepts and the expository instantiation which collectively form the pre-theory framework. In order to show where the pre-theory framework aligns with the Vaishnavi et al. (2017) framework¹¹⁵, Figure 3-11 p 77 was created.

	Contribution Types	Example Artifacts
More abstract, complete, and mature knowledge ↕ ↕ ↕ ↕ More specific, limited, and less mature knowledge	Level 3. Well-developed design theory about embedded phenomena	Design theories (mid-range and grand theories)
	Level 2. Nascent design theory—knowledge as operational principles/architecture	Constructs, methods, models, design principles, technological rules.
	Level 1. Situated implementation of artifact	Instantiations (software products or implemented processes)

Figure 3-10 Levels of contribution in DSR (Gregor and Hevner, 2013)

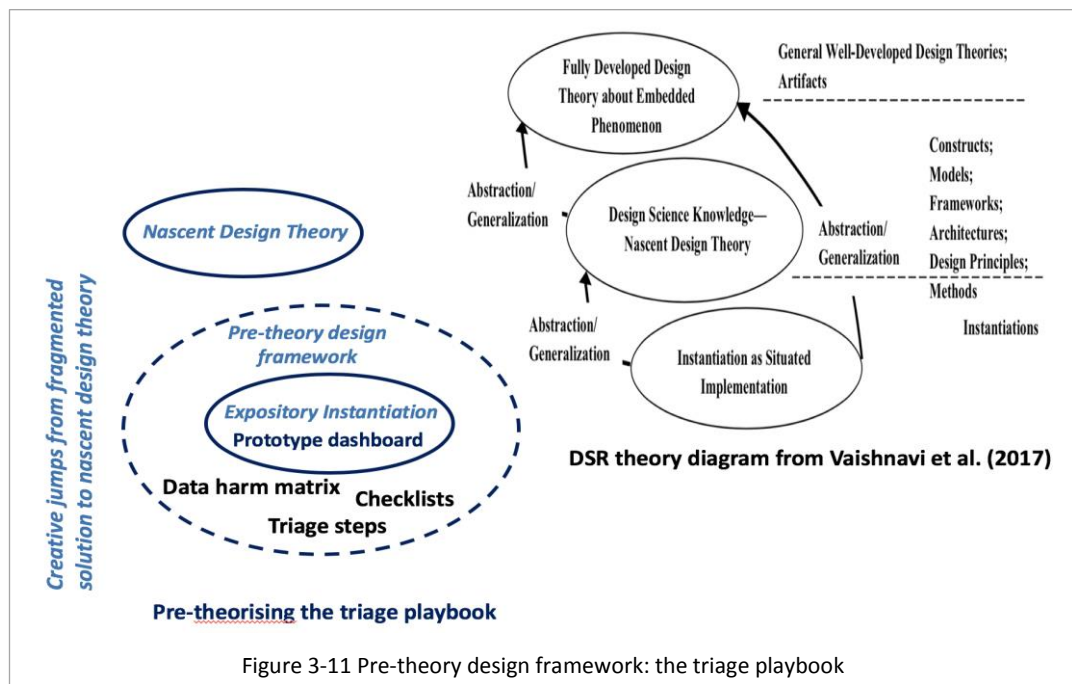


Figure 3-11 Pre-theory design framework: the triage playbook

¹¹⁵ Their Figure 6. Design Science Knowledge Hierarchy was extracted to show the alignment with the pre-theory framework.

Vaishnavi et al. (2017) describe *expository instantiation* as: *Includes an instantiation (possibly situated implementation) that can be used for exposition of the theory and/or for testing the theory*. This aptly describes the testing of the application of Peirce semiotics-ternary as embedded in the triage playbook and instantiated in the prototype dashboard. Their views on instantiation – *with no or minimal contribution of abstract artifacts* – constitute *a possible interesting partial or even an incomplete design theory with potential for further work* i.e. a pre-theory knowledge contribution in the form of pre-theory framework.

Hevner et al. (2004) provide a clear exposition of artefacts instantiation. Instantiations show that the artefacts, e.g. the conceptual triage playbook, can be implemented in a *working system* e.g. the prototype dashboard. As the dashboard was a *concrete* artefact, it *demonstrated feasibility* and its *suitability to its intended purpose can be assessed* i.e. demonstrate *proof-of-concept* and *proof-of use*. In the instantiation and the assessment, researchers are able to learn *about the real world, how the artifact affects it, and how users appropriate it*. The various pre-theory concepts i.e. the triage steps, checklists and data harm matrix were incorporated into the triage conceptual model in the application of DSR, which is described next.

3.4 Application of DSR

The structure of this research followed the *High-Level Process* in Figure 3-7 p 75, with the details of the processes and the artefacts as shown in Figure 3-8 p 75, driven by motivation and the broad research aim (i.e. *Awareness of Problem/Motivation*), then *Problem Identification* during the SSM literature review (Chapter 2) which led to a comprehensive interview study (Chapter 4).

The initial SSM literature review identified that triage has been used for digital forensics investigation and also little research on DBI response and privacy harm. An artefact, a synthesised triage steps (Chapter 2), was formulated from the literature review and described and verified using Peirce semiotic-ternary (Section 3.1.2). Although the concepts and principles for triage are established in the medical domain, there appeared to be little formalisation of what constituted the steps of triage in digital forensics or incident investigation and response. Besides, triage is used by IS/IT professionals to gather and obtain actionable outcomes (Chapter 4). Other ideas were also deduced and induced from the interviews (Chapter 4). Upon reflection on the interview findings, a key problem, also a gap in research is that data privacy harm (data harm), especially the data harm to affected individuals as a consequence of DBI, has received little attention from researchers. Furthermore, there is no PHA approach and/or DBI response framework that addresses data harm to affected individuals.

As described in Chapter 5, a triage playbook was conceptualised, and a list of requirements formulated. In essence in designing a prototype dashboard for the triage playbook, the prototype dashboard was an instantiation of a conceptual model (an artefact). The triage steps during initial DBI response constituted the crucial initial steps for taking appropriate actions during DBI response. As clearly stated by Kennedy et al. (1996): *Triage is an area in which decision makers must know what they are doing, why they are doing it, which actions to take to achieve a satisfactory outcome*. The application of the proven or widely used Peirce semiotics-ternary (as discussed in Section 3.1.2) for triage then provided a rigorous validation for the initial conceptual model.

Furthermore, in organisational settings and in light of the stringent GDPR breach notification requirements, assessment of privacy harm to affected individuals during DBI response will be needed to prioritise breach notifications i.e. whether to notify the individuals or not. The GDPR requires organisations that notify the ICO where there is a *risk to the rights and freedoms of individuals*, and *only notify the individuals where there is high risk*. These were posed as research issues as these *risk criteria* are not defined in the GDPR. A data harm matrix was created, using data harm entities extracted from reports (i.e. from ICO and GDPR publications). Inspired by the interview study, a checklist approach using questions and answers was designed and integrated into the triage sequence of steps.

Further literature review (as shown in Figure 3-8 p 75) indicated that although checklists have been discussed and used in various domains, and similar to triage, there is little research on checklists for use during DBI response. ENISA (2012) has discussed the use of various privacy and security-related indicators but these have not been operationalised into practice or examined by privacy and security researchers. Furthermore, the identified indicators are not specifically tailored for assessing privacy harm to individuals.

For operationalising the triage playbook, a conceptual model was designed which formed the initial design steps for building a prototype dashboard. The prototype dashboard was developed and tested during the *Solution Design* phase. The RITE approach was used to construct a prototype dashboard of the triage playbook. This RITE approach (Section 3.5) is aimed to provide relevance and rigor. As pointed out by Hevner (2007): *The internal design cycle is the heart of any design science research project. This cycle of research activities iterates more rapidly between the construction of an artifact, its evaluation, and subsequent feedback to refine the design further. This **action-practical-feedback** was reinforced by Gregor and Hevner (2013) and Nenonen et al. (2017).*

3.5 Rapid Iterative Testing and Evaluation (RITE)

The Rapid Iterative Testing and Evaluation (RITE) approach besides being used in practice¹¹⁶ in industry, has also been studied by researchers e.g. (Medlock et al., 2002; Medlock et al., 2005; Patton, 2008; McGinn and Chang, 2013). It provides a *light*¹¹⁷ agile development approach that supports prototyping of the dashboard (Dashboard). The iterative cycle of development and testing with users meet the *action-practical-feedback* approach that underlies DSR and pragmatism.

The steps in RITE were adapted from Shirey et al. (2013) and shown in Figure 3-12 p 80. For Shirey et al. (2013), the ability to *iterate quickly on the design reduced their fear of failure because they could try something out and, if it didn't work, try again*. This research tried RITE with a developer in a company which did not work out. The second attempt with an independent developer provided the required Dashboards. RITE is an agile method; hence it is flexible to be adapted to meet tight delivery timescales. However, as pointed out by Medlock et al. (2005) and McGinn and Chang (2013) the testing/verification is hard to estimate as each iteration can take up to two week or more to complete (depending on the number of users and fixes¹¹⁸ in each iterations). On RITE, McGinn and Chang (2013) offered this: *Central*

¹¹⁶ Michael Medlock and his colleagues at Microsoft coined the phrase RITE (Patton, 2008).

¹¹⁷ *light* to mean *simple to use* and requiring minimal resources/tools or modeling constructs.

¹¹⁸ Fixes to include changes/requirements and bug fixes.

to the RITE method is the notion that as few as one participant can complete a usability test session; problems are identified and fixed, and then another participant completes the same tasks with the updated system. After that session, the system under test may be modified again to fix problems observed in that second session, and the team continues to run participants and modify the system until they are satisfied that the biggest usability problems have been identified, been fixed, and that the fixes have been validated.

As this research involved an external developer to develop and build the Dashboard, an overall project approach was set up to track progress of the design and build (include development and testing/verification). Figure 3-13 p 80 shows the overall prototyping activities. A small pilot was done before the first iteration with users using DashboardV1. During the first iteration with users, users' feedback was reflected on and explored to discover any insights that are relevant to the nature of this research as specified in the requirements for the Dashboard (Requirements List in Appendix M p 231). Such new insights were done to add new features, and this was part of *micro-evaluation*¹¹⁹ in DSR. The developer was also actively involved in the iterative cycles as shown by the marked red activities in Figure 3-13 p 80. The application of RITE and the prototyping with developer(s) are described in Chapter 5 following the interview study described in the next chapter.

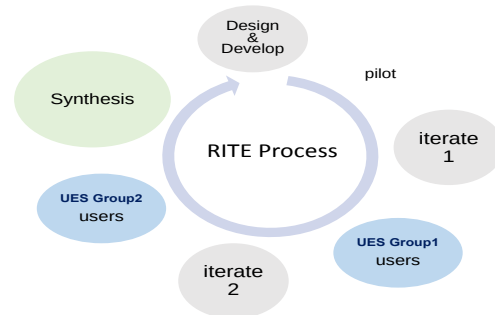


Figure 3-12 RITE Process adapted from Shirey et al. (2013)

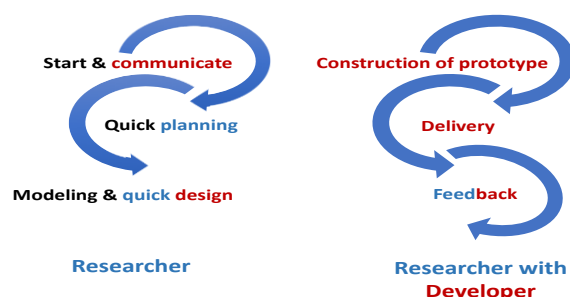


Figure 3-13 Prototyping activity

¹¹⁹ In Vaishnavi et al. (2017) the evaluations that occur at every design process are *micro-evaluations*. Such *micro-evaluations* (or verification/testing) are not the *formal* evaluation that occurred after the design has stabilised.

Chapter 4 Personal Data Incident (DBI) Interview Study

As shown by the SSM studies in Chapter 2, numerous forensics and security frameworks exist. Also, organisations have a wide range of incident processes and frameworks ranging from standards to best practice guidelines from various institutions. Although there are industry reports on DBI and services for responding to such incidents, it is not clear how organisations are responding to DBI. There is little research concerned with the personal data breaches. For example, *when faced with DBIs, are organisations using any specific incident frameworks or incident handling processes or procedures? Moreover, what are the concerns and views on notifications to individuals, and the associated likely privacy harm to affected individuals?* To answer these questions, an exploratory study using semi-structured interviews was conducted to collect industry DBI data.

The broad aim of this exploratory interview study (**study**) and the rationale for adopting and conducting interviews are described in Section 4.1. The planning, designing of the interview questions, the recruitment and selection of interviewees, and conducting of the interviews are outlined in Appendix H p 217. A summary of the study approach is given in Section 4.2. For this study, the combined deductive and inductive i.e. hybrid Thematic Analysis (TA) approach and an explanatory theme framework (**explanatory framework** by Fereday and Muir-Cochrane (2006)) were used for the analysis of the collected interview data and are outlined in Section 4.3. The results of the analysed data are reported in Sections 4.4 to 4.9.

4.1 Interview study aim and rationale

The main aim of this study was to address RO2 i.e. to gauge the extent and nature of DBI responses by organisations in the UK. To achieve this, an interview study was conducted to gather the viewpoints of practitioners who were willing to share their experiences and views of incident responses involving personal data breaches and also their views on privacy harm. In particular, explanatory questions were framed to address the aim of this interview study, as shown in Figure 4-1 p 81.

Interview Study Aim
To gauge the extent and nature of personal data breach incident (DBI) responses by organisations in the UK.
Explanatory Questions
(EQ1) <i>What frameworks/procedures/processes are being used for personal data breach incident response?</i>
(EQ2) <i>What are the concerns and views on personal data breach incident response activities?</i>
(EQ3) <i>What are the concerns and views on privacy harm to individuals?</i>
<i>What did the interviews expose? (RO2)</i>

Figure 4-1 Interview Study Aim and Explanatory Questions

4.1.1 Hybrid Thematic Analysis (hybrid TA) and explanatory framework

The explanatory questions were used for reporting the themes that were extracted from the study data. For this exploratory study, the combined deductive and inductive (hybrid TA) approach and an explanatory framework for the final analysis were used. Also, a dual deductive – inductive and latent – manifest set of themes was used together in high-quality qualitative work (Joffe, 2011). Åsvoll (2014) closely describes the deductive-inductive-abductive approach conducted in this study. This approach makes sense to this researcher, as the interview aim covered a broad spectrum of topics, and the final

analysis of the combined themes using an explanatory framework, provided a way to explain the overall themes from this study. Moreover, the use of an explanatory framework in hybrid TA provided concrete guidance that was required for higher level, interpretative analysis, which (an inductive) TA lacks (Braun and Clarke, 2013, p 180). Fereday and Muir-Cochrane (2006) described an *explanatory framework* used in the final step in their hybrid TA in this fashion: *The interaction of text, codes, and themes in this study involved several iterations before the analysis proceeded to an interpretive phase in which the units were connected into an explanatory framework consistent with the text.* This *explanatory framework* approach was adopted for the interpretative or descriptive qualitative analysis of the collected themes. The *explanatory framework* approach involved expressing the study aim into explanatory questions (EQ). The final analysis was abductive in the sense that it reveals the question: what did the interviews expose?

4.1.2 Justification for the interview study

A qualitative exploratory descriptive approach using semi-structured face-to-face interviews was chosen to most appropriately extract the practitioners' experiences in DBI. Interview methods were conducive for addressing the sensitive and qualitative nature of the topic under study. Hove and Tårnes (2013) pointed out the challenges with qualitative data analysis in that there exist clear conventions for quantitative data analysis, but there are fewer guidelines for analysing qualitative data. Besides Hove and Tårnes (2013), Werlinger et al. (2007) also conducted qualitative research studies using interviews for collection of their qualitatively-oriented research on security incident management.

However, getting access to organisational work practices around security-related incidents such as data breach incidents was very challenging. This is because most employees or individuals were not allowed to disclose such inside information, as it was deemed commercially sensitive. Despite the challenges, this fact makes this particular study a valuable contribution to researchers¹²⁰. Gillham (2000a, p 11) said that the easier it is to get data, the less valuable they are. Interviews offer high gains, but are difficult to obtain, involving a great deal of work, and the information gained is always suspect to some degree (Berger, 2016, p 208). However, Hove and Tårnes (2013), believed that building trust with interviewees face-to-face gave better and more elaborative answers. The high gains are possible with face-to-face interviews as there are opportunities to clarify and elaborate questions, unlike in survey questionnaires and also phone interviews. Burns (2000, p 424) also revealed that semi-structured rather than structured interviews permit flexibility in particular with respect to clarifying responses, establishment of rapport, and more complete responses.

Moreover, by recording the interviews, the interviewer is free from taking notes during the interviews, and hence allowed time to focus on listening and asking follow-up questions. Furthermore, the recorded interviews enable better review and analysis of the answers. The recorded information also provides a form of recorded evidence which can be used for quality checking and reuse in other ways from those intended by the original researcher (Bryman and Bell, 2015, p 494).

¹²⁰ A senior lecturer from another university commented this when he responded via email to a BCS news announcement of this interview: '*In my experience, gathering data through interview can be a lot more meaningful than online questionnaires, which often get a very poor response rate*'. Email dated 27-April-2016.

As pointed out by Hickey and Davis (2003), in general it appears that interviews are widely used primarily to uncover new information and are essential with those with expertise or experience on the subject matter (subject matter experts), especially when the users/customers are not accessible. Thus, more thought and research went into finding a way to recruit candidates (Appendix H, Section H- 4 p 218) as well as designing (Appendix H, Section H- 3 p 218) that address the overall aim of the exploratory nature of this study. With this in mind, the target population for selection of candidates focused on subject matter experts. This constitutes basic purposive sampling of candidates.

4.2 Summary of interview study approach

As there was little research done on DBI, a qualitative semi-structured interview study was identified and justified as suitable to gauge the extent and nature of DBI responses by organisations in the UK. Given that this study constituted a major piece of data collection, the underlying study approach is discussed in Section 4.1.1. This researcher's worldview leaned towards the pragmatism paradigm, and also the underpinning research philosophy as described in Chapter 3 is founded on Peirce's pragmatism.

The pragmatic approach was revealed in the way the interview questions were constructed, the selection of the candidates, the sample size/population, and the reality of busy executives and/or subject matter experts that were needed for this interview study, all proved challenging aspects of conducting an interview study. The overall study approach is outlined in Appendix H, Figure H- 1 p 218. Although thorough literature review was done to gather information to help design the interview questions, as well as plan and conduct the interviews, challenges still emerged when the plan and interview scripts were put into practice. For example, after the practical experiences of conducting the planned scripts, the original plan, particularly on the planned sample size, were changed to ensure that the interview study aim could be achieved. Vogt et al. (2014, p 45) called this improvisation when faced with the unexpected. Hence the original interview script (Appendix I p 221) was changed to enable elicitation of interviewee's experience of DBI by prompting for hypothetical incidents (Appendix J p 223). Further details on the interview scripts are provided in Appendix H p 217.

Beside the issues with population sampling, Vogt et al. (2014, p 156) also re-confirmed other identified issues: *whom to interview, the recruitment methods, and how to conduct interview research*. These were the practical challenges that this researcher had to address. The '*whom to interview*' was addressed based on the researcher's understanding of the study topics, and the likely subject matter experts based on job titles, roles/responsibilities and/or their professional experiences in the fields. The *recruitment method* proved to be the most challenging due to the sensitive nature of the topics. Besides approaching professional friends/colleagues, and using all available social media channels, conferences were also attended to find potential candidates. Snowballing techniques were also used. In snowball sampling, a person, who is identified as a valid member of a specified group to be interviewed, is asked to provide the names of others who fit the requirements (Burns, 2000, p 389).

Challenges around confidentiality and privacy were factored into the way candidates were approached and selected, the planning and design of the interviews and questions, and even in coding of the transcribed interview texts. For example, all personal and company details were pseudonymised and/or removed from the transcribed texts. Such important messages were also conveyed to potential

candidates during the recruitment process, and also during the interviews especially when interviewees raised concerns on confidentiality.

In *conducting the interview* although a prepared interview script was used as a guide, an informal elicitation and dialogue type approach was adopted. Moreover, to build trust with the interviewees, and to maintain a dialogue with the interviewees, the approach taken was: to be present with the interviewees, be mindful and to show respect and interest in what the interviewees shared.

Before the interviews, practitioners were provided with brief notes about the nature of the interview, and a consent form which they must sign before the interview. They were also informed that the interviews would last not more than one hour, conducted preferably face-to-face in a private room or in their office. In total, 21 interviewees with relevant job titles and/or work experiences in the field, from across the industry sectors took part in the interview study. The face-to-face interviews took place in London between 23 May 2016 and 19 July 2016. These interview responses were then analysed using hybrid TA described in the next section.

4.3 Hybrid Thematic Analysis (TA) of interview responses

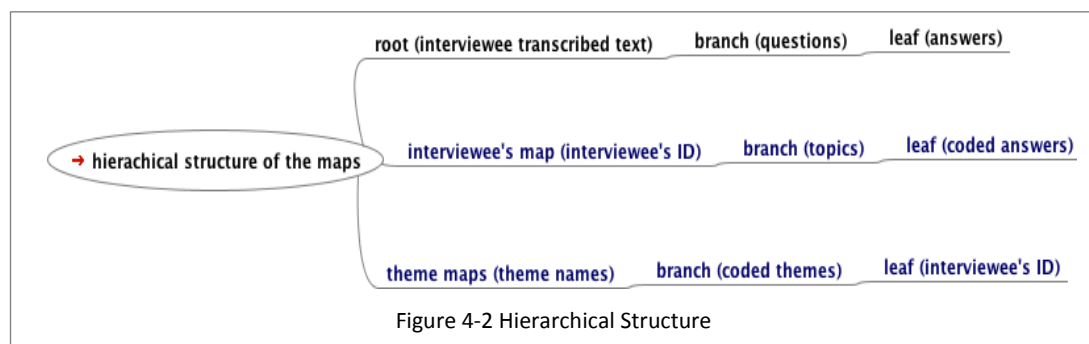
Braun and Clarke (2006) described thematic analysis (TA) as: *a method for identifying, analysing, and reporting patterns (themes) within data. It minimally organises and describes your data set in (rich) detail. It also often goes further than this, and interprets various aspects of the research topic.* In terms of analysing interviews, thematic analysis (sorting and classifying responses) also involves the search for and identification of common threads that extend across an entire interview or set of interviews (Cruzes and Dyba, 2011).

Content analysis¹²¹ sometimes treated as similar to thematic analysis – which is also suitable for analysing qualitative data – was not chosen, as this method tends to focus at a more micro level, targeting quantitative form for statistical analysis or frequency count (Braun and Clarke, 2006). As the nature of the data from the interview is primarily words, phrases or narratives, and the unit of analysis is qualitatively textual, the text being organisational work practices around incident response processes or frameworks, thematic analysis allows these initial qualitative data to be coded and analysed. Thematic analysis also enables quantitative measures e.g. frequency counts, to be applied following the initial coding of the textual themes (Joffe, 2011). Moreover, Vaismoradi et al. (2013) identified *drawing a thematic map* as a principal thematic approach, which was distinctively absent under the content analysis process lists. Thematic maps were mentioned in Braun and Clarke (2006), Attride-Stirling (2001) and Cruzes and Dyba (2011) as an approach for organising and showing the themes identified during the analysis process. For example, Cruzes and Dyba (2011) states that thematic analysis is also one of the most frequently used synthesis methods in software engineering, drawn on the principles of thematic analysis (based on Braun and Clarke (2006)) and conceptualised the thematic synthesis approach in software engineering as a scientific inquiry. The thematic maps visually outlined the conceptualisation of the thematic synthesis

¹²¹ Vaismoradi et al. (2013) showed the differences between thematic and content analysis in a diagram. They also pointed out that the boundaries between these methods have not been clearly specified, and they are often used interchangeably and there is confusion about their similarities and difference. However much of the analysis presented in published papers is essentially thematic but is either described as something else such as content analysis or simply not identified as a particular method.

approach. The usability of visual thematic maps for aiding thematic analysis was studied by Attride-Stirling (2001). This inspired this researcher to use visual thematic maps for this study. The Attride-Stirling (2001) thematic network approach allows linking of themes (assumed to be network-like structures) and developed from levels of interpretation and abstraction (i.e. from text to code to theme to model). However, as this interview study was not to develop a theoretical model, building hierarchies of themes was necessary and sufficient for this exploratory study. Building hierarchies of themes precedes the linking of themes into theoretical models (Ryan and Bernard, 2003). Ryan and Bernard (2003) outlined that analysing text involves several tasks: (1) discovering themes and subthemes, (2) winnowing themes to a manageable few (i.e. deciding which themes are important in any project), (3) building hierarchies of themes or code books, and (4) linking themes into theoretical models. The hierarchical structure of the thematic maps for this study is shown in Figure 4-2 p 85.

Cruzes and Dyba (2011), in referencing Braun and Clarke (2006), also pointed out that if visual thematic analysis is not used within an existing theoretical framework, it has limited interpretative power beyond mere description. Similarly, Bryman and Bell (2015, p 601) commented that thematic analysis lacks a clearly specified series of procedures. This is because the thematic analysis itself lacks a semiotic basis. The semiotic interpretation is discussed by Åsvoll (2014). Existing literature on thematic analysis discussed the deduction and/or induction logic used in qualitative analysis, but rarely discussed abduction logic or Peirce's semiotic theory. This was another limitation of the thematic analysis method/approach; hence a hybrid TA and the explanatory framework was adopted.



Bryman and Bell (2015, p 601) suggested the use of a framework, developed at the UK National Centre for Social Research (NCSR), for assisting thematic analysis, and the methods proposed by Ryan and Bernard (2003) for identification of the themes. Upon examination of the NCSR framework as described in Bryman and Bell (2015, p 599) and also in Ritchie et al. (2014, p 282), the thematic analysis (TA) described by Braun and Clarke (2006) provided a clear methodological structure to apply. Moreover, the NCSR framework implicitly relied on a matrix-based format (instead of thematic maps¹²²) for managing the data.

Braun and Clarke (2006) clearly state that coding can be performed either manually or using a software programme. As this researcher wanted to stay as close as possible to the raw interview data, a manual coding and data management approach were utilised.

¹²² Freemind tools allow not only hierarchical maps to be created but also various useful export features including generating matrix-based format (e.g. Excel worksheets).

4.3.1 Thematic phases and identification of themes

Braun and Clarke's (2006) thematic phases (Thematic Phases) and the generic processes were analysed to extract the executional steps which were required for the TA. These executional steps were added and highlighted (shown in red) in the column next to the processes as shown in Figure 4-3 p 86. The steps marked in *italic* in Figure 4-3 p 86 were related to indexing or labeling, searching or locating and selecting themes (thematic coding steps). In Phase (d) of the Thematic Phases, thematic maps were mentioned. Cruzes and Dyba (2011) cited other researchers who have also used mindmaps or tree-maps to organise and structure the TA processes. The mindmaps structure provides support for subsequent interpretation of the results. Based on this, mindmaps were used to create and show the thematic maps. However, such mindmaps for the thematic maps are structured hierarchically. Furthermore, Cruzes and Dyba (2011) listed these for consideration during coding: *Coding at a too general a level; Identifying what one wants to see and not what the text is saying; Coding out of context*

During the coding, even if the phenomenon appears only once, it still can be part of the analytical thematic maps (Ritchie et al., 2014, p 117). Identification of such phenomena requires identification of themes. Although the Braun and Clarke (2006) approach to TA is *essentially independent of theory and epistemology*, Willig (2013, p 58) in referencing Joffe (2011), suggested the need to be clear about the epistemology, and to define what constitutes a theme.

Phase	Description of the process	Executional steps
(a) Familiarising yourself with your data:	Transcribing data (if necessary), reading and re-reading the data, noting down initial ideas.	<i>Familiarisation with the data;</i>
(b) Generating initial codes:	<i>Coding interesting features of the data in a systematic fashion across the entire data set, collating data relevant to each code.</i>	Generate initial code; <i>Interesting features – mark/copy text;</i>
(c) Searching for themes:	Collating codes into potential themes, gathering all data relevant to each potential theme.	<i>Search for themes; collate themes</i>
(d) Reviewing themes:	Checking if the themes work in relation to the coded extracts (Level 1) and the entire data set (Level 2), generating a thematic map of the analysis.	<i>Review the themes;</i> Generate thematic maps; <i>Level 1 – coded extracts (1st pass coding);</i> <i>Level 2 – entire data set extracts (2nd pass coding);</i>
(e) Defining and naming themes:	Ongoing analysis to refine the specifics of each theme, and the overall story the analysis tells, generating clear definitions and names for each theme.	<i>Define/refine the themes;</i> Ongoing analysis; <i>Extracts;</i>
(f) Producing the report:	The final opportunity for analysis. Selection of vivid, compelling extract examples, final analysis of selected extracts, relating back of the analysis to the research question and literature, producing a scholarly report of the analysis.	Final analysis of extracts; Produce report.

Figure 4-3 Thematic Phases and Steps synthesised from Braun and Clarke (2006)

Identification of themes requires a theoretical status attributed to the themes that are identified; *these can be informed by a particular theory, or can be informed by the research question and the researcher's epistemological position* (Willig, 2013, p 59). In this study, the interview aim, and also this researcher's epistemological position in pragmatism both informed and provided the theoretical basis for the

identification of the themes. Following the recommendation by (Willig, 2013, p 60) a deductive and inductive (hybrid) TA approach was adopted for the identification of themes. A deductive TA relies on a priori template (latent code) to code the data and derive or extract the themes from it. In an inductive TA, the researcher relies on the raw data (manifest code); and these do not reflect the researcher's theoretical commitments i.e. themes emerge from and are grounded in the data. To identify themes emerging from the data, the *key word in context* (KWIC) approach described in Ryan and Bernard (2003) was adopted. In a KWIC approach, key words or phrases were identified and the corpus of text was systematically searched to find all instances of each key word or phrase. A copy of each instance of key word or phrase and its immediate context are noted. Themes get identified by physically sorting the examples into piles of similar meaning (Ryan and Bernard, 2003). This method is similar to the *selective* coding as described in Braun and Clarke (2013, p 206-207). For the deductive coding, the initial set of pre-coded interview questions provided the a priori template (latent code) to code the data.

There were also studies done where hybrid TA approaches have been used (Willig, 2013, p 60). Such a combined hybrid approach integrates the *a priori* codes and the newly emerged themes for the final analysis which involves a development of an explanatory framework to make sense of the phenomenon under investigation (Willig, 2013, p 60). Besides Fereday and Muir-Cochrane (2006), Willig (2013) and Ritchie et al. (2014, p 292) also mentioned the use of an explanatory framework as part of the overall abstraction and interpretation analytic approach. This analytic approach involved developing descriptive categories, *mapping linkages between parts of the data, accounting for patterns observed in the data, and formulating explanatory accounts* (Ritchie et al., 2014, p 292). Moreover, such an explanatory framework addressed the issues on *guidelines for analysing qualitative data* that were raised by Hove and Tårnes (2013). The following section describes an organising framework set up to manage and conduct the Thematic Phases and the hybrid TA.

4.3.2 Organising framework

As there were several visual maps generated during the TA, an organising framework as shown in Appendix K, Figure K- 1 p 225, was set up to track and index the various maps. This organising framework – which does not indicate any ordering or sequence of execution of the hybrid TA – provided an inventory and links to the various maps to be retrieved and analysed during the hybrid TA. As shown in Figure 4-3 p 86, Thematic two passes (or iterations) of coding i.e. 1st pass and 2nd pass coding were identified and conducted (Phase (d)) and a final analysis was made to report the findings (Phase (f)). The steps in Phase (a) to Phase (d) require further preparation steps for conducting and organising the coding for analysis in Phase (f). Freemind was used to generate the thematic maps (Phase (d)). Several coding maps were created to conduct the hybrid TA steps as shown in Figure 4-4 p 88 and described in Section 4.3.3.

4.3.3 Execution of hybrid thematic analysis (TA)

4.3.3.1 Set up coding approaches

The 1st and 2nd pass coding approaches are shown in Figure 4-5 p 88 and Figure 4-6 p 88. Section 4.3.3.4 describes the 1st pass coding and Section 4.3.3.5 describes the 2nd pass coding.

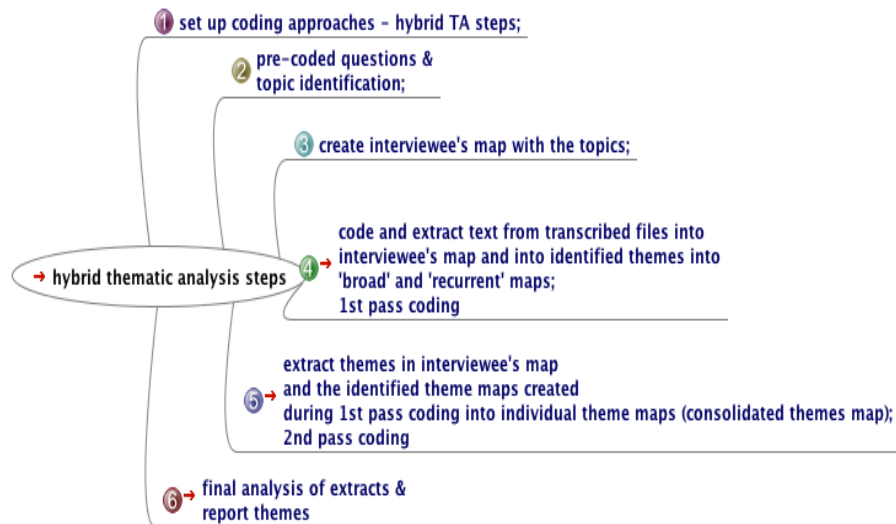


Figure 4-4 Hybrid Thematic Analysis Steps

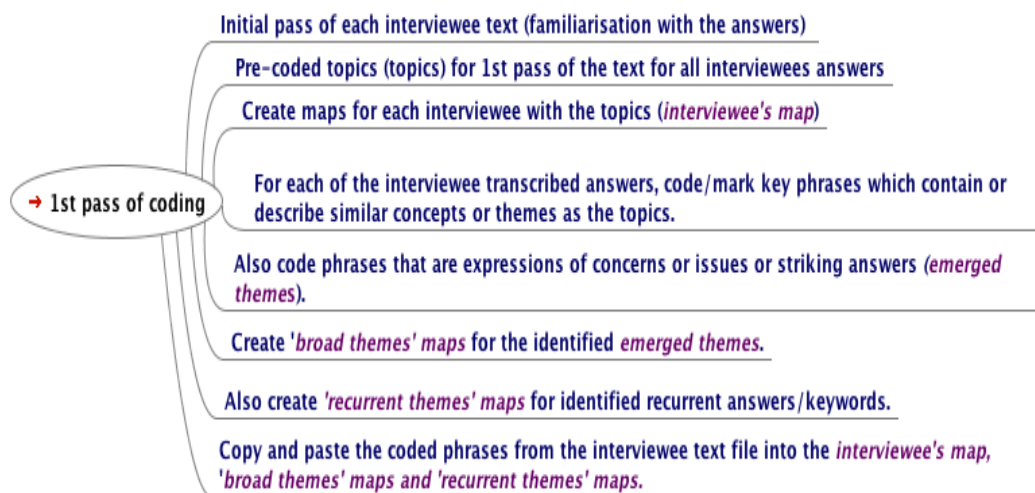


Figure 4-5 1st Pass Coding

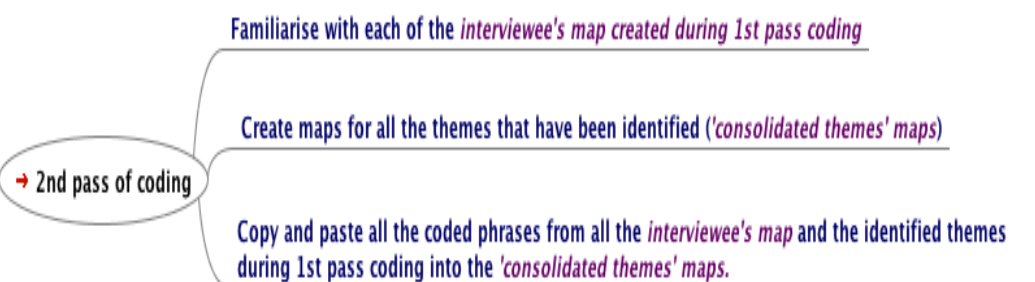


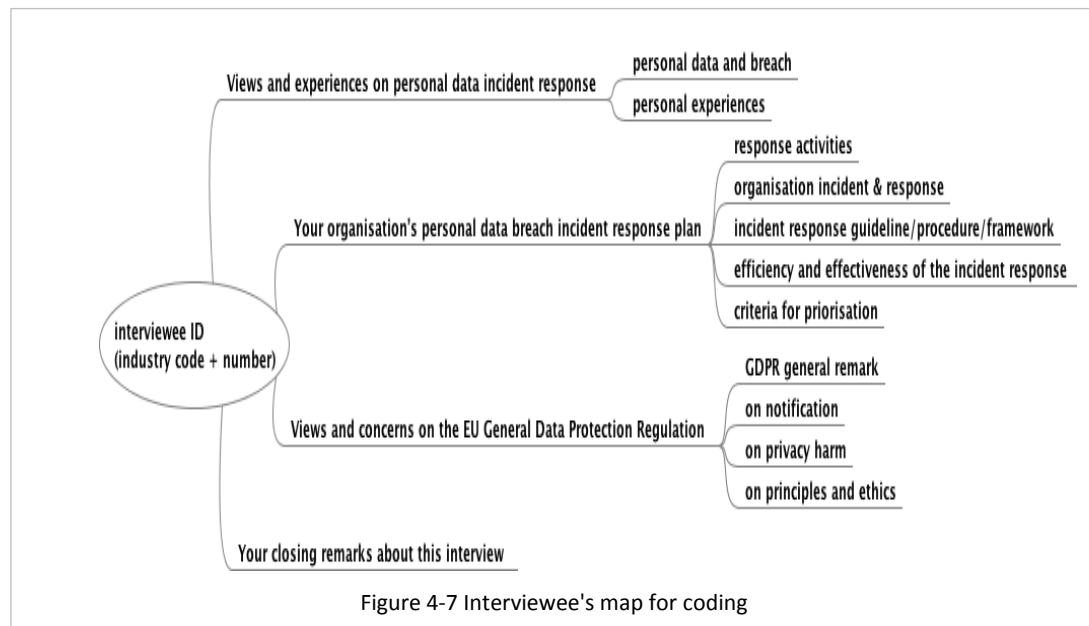
Figure 4-6 2nd Pass Coding

4.3.3.2 Pre-coded questions and topic identification

Based on the interview questions, which have been designed around the interview study aim, topics were identified for deductive coding as the starting point of the hybrid TA. The identified topics were shown in Figure 4-8 p 91.

4.3.3.3 Create interviewee's map with the topics

A map was created for all the interviewees with the topics to be examined in the interviewee's text files. In total, there were 21 interviewee maps created using the template as shown in Figure 4-7 p 89.



4.3.3.4 1st pass coding

1st pass coding: code and extract text from transcribed files into interviewee's map and into identified themes maps. During the familiarisation of the text, besides noting the consideration as offered by Cruzes and Dyba (2011) (Section 4.3.1). The following questions helped to focus on the coding and the identification of themes:

- What are these themes as framed by the pre-coded topics?
- How do interviewees classify or describe or name incident response frameworks and activities?
- What emerges from the interviewee's concerns or views or account of their experience?
- What are these themes that emerged from the data?

The 1st pass coding steps involved using the topics (deductive coding), and also examining concepts, concerns, issues in the text using the KWIC approach (Section 4.3.1) to extract themes (inductive coding). Besides the pre-coded topics, the following pointers also help to code themes:

- Note repeating or common key words or concepts (recurrent);
- The comments/answers were unexpected or surprising remarks (notable);
- The comments/answers were expressed strongly or discussed at length or stressed as important by the interviewees (issues or notable).

The interviewee's text was examined deductively using the topics. Selected text was colour marked in the text and at the same time the selected text was copied and pasted into the interviewee's map. The selected text was coded into the relevant topics in the interviewee's map, and also any emerged themes using the KWIC approach. These were also captured into *broad* themes. Also, any repeating text or common phrases/key words/concepts were copied and pasted into *recurrent* themes.

4.3.3.5 2nd pass coding

2nd pass coding: extract themes in interviewee's map and the identified theme maps created during 1st pass coding into individual theme maps (consolidated themes map). During the 2nd pass coding, familiarisation of all the interviewee's map and the identified themes were done. A theme map was created for each of the themes identified in the 1st pass coding. The themes identified in all the interviewee's map were consolidated into individual theme maps. The interviewee's ID was also marked into each of the consolidated theme maps. Figure 4-8 p 91 shows all the topics (identified in step 1) and the themes generated from the 1st and 2nd pass coding.

The overall aim of the 2nd pass coding was to reduce the corpus amount of collected codes and themes. This data reduction was needed to make sense of the data gathered (Bryman and Bell, 2015, p 13). Data reduction involves making decisions about which data chunks to code and which to pull out (Miles and Huberman, 1994, p 11) and (Silverman, 2013, p 247). Any concepts, issues, key words or phrases which were identified as outside the scope of this study (i.e. not within the objectives of this study or do not reflect the purpose of this study) were excluded during the final consolidation. For example, activities or issues or concepts associated with protection rather than response handling were outside the scope of this study, and hence have not been included for the final analysis. Also issues or concepts or themes that were not directly related to personal data breaches or the aim of the study as set out in Section 4.1 were excluded.

4.3.3.6 Final analysis of extracts and report themes

All the extracted theme maps created during the 1st pass and 2nd pass coding were captured and organised into various themes as shown in Figure 4-8¹²³ p 91. The various themes (e.g. the *broad* themes broken down into *issues*, *notable* and *quotable themes*) that have emerged from the hybrid TA of the interview data were captured in various maps. Also, relevant theme maps were exported into Excel worksheets and further analysed using MSD. The overall aim of using MSD was to support the answering of the explanatory questions through data analysis of the theme maps. Figures 4-9 p 94 to 4-13 p 97 were produced using MSD.

To report these themes, the explanatory questions (EQ1, EQ2, EQ3) in Figure 4.1 p 81 were used to guide the descriptive qualitative analysis of the extracted theme maps. In essence these explanatory questions provided a *prism*¹²⁴ to unravel the collected themes such that the stories and/or patterns in these themes can be reported.

4.4 Background on the interview results

Preparation for the thematic analysis started with manually transcribing and familiarising with the audio-recorded interview files for the 21 interviewees. Interviewees were from across industry sectors¹²⁵ although none in the Land and Property, and Justice sectors as shown in Appendix L, Figure L-1 p 226. Pseudomisation (Appendix H, H-5 p 219) was used to de-identify/identify the interviewee. E.g. an

¹²³ The texts marked in green and with the red arrows are nodes to more maps.

¹²⁴ The word, *prism* reflected the way various themes were examined using a stream of *questions* (light) to expose or unravel the hidden stories or connecting patterns (the spectrum of hidden lights) embedded subtly in the collected themes. The whole is more than the parts.

¹²⁵ Industry code listing from ICO: <https://ico.org.uk/action-weve-taken/data-security-incident-trends> [Accessed 29-December-2018].

interviewee from the finance sector was assigned an industry code e.g. F for finance and a number showing the interview sequence i.e. the first interviewee from finance was F1.

During the interview, interviewees were asked to share any notes or documents related to DBI guidelines, procedures or frameworks. Most of the interviewees were unable (no written procedures or frameworks) or reluctant (due to commercial reasons) to share the requested notes. Those that shared the notes are shown in Figure L- 2 p 226. These notes were also included during the final analysis.



These data were captured into MSD to show the interviewee industry experience based on their role/responsibility or job titles in their respective fields (field experience), and the number of years working in their field. In summary the number of interviewees and years of field experience were: two less than five years; 10 greater than five and less than or equal to 10 years; nine greater than 10 years. The shortest interview was 37 minutes and the longest was 96 minutes (G15 spread over two interviews). In Appendix L, Figure L- 3 p 227, the size of the bubbles/balls showed the years of experience of the interviewees. Figure L- 3 p 227, was plotted to show the overall pattern of the industry experience in years and the interview durations. Interviewee O10 was a CEO of a small-medium size organisation that suffered a data breach. The interview was long as he revealed in detail the nature of the incident, how it happened,

why it happened, and the ad hoc response steps during the breach, and also post the breach. The interview with G15 was disrupted due to changes in interviewee's circumstances and hence two interviews took place. Also, G15 was keen to share experience of his ten years of information governance officer role where he was exposed to several breach cases involving local authorities. Although the interview with B3 was short (less than one hour), it was a productive one as B3 was a victim to a couple of data breaches and also introduced other candidates who subsequently took part in this study. F16 (CISO with a global commercial bank) shared what the financial security communities are doing in the areas of cybersecurity. In terms of DBI response, this has not been a major focus for F16, but he raised that: *'especially now with the EU GDPR being approved, we are re-looking at the whole thing to see how we could further enhance that capability because we have the basic raw data but I think we need to fine tune the controls to ensure we meet the various requirements for the EU GDP'*. The shortest interview was with H8 who was supportive but not all the raised interview questions were discussed or answered.

Overall, the more experienced interviewees took longer to interview. Even the interviews under 60 mins e.g. with F21 a senior Underwriter for cyber and intangibles, and B9 Head of Business Continuity and responsible for security and data privacy, revealed insightful information. F21, besides assessing suitability of organisations for cyber insurance, had dealt with several data breach claims by organisations. He said: *'To be quite honest – we don't put 100% confidence in any of the guidelines that you'll be looking at because again it's their practical application that really comes through'*. B9 expressed: *'I'm actually happy to share some of our real incidents with you, because I think the world learns from real incidents'*.

All the interviewees shared their DBI experiences, views and concerns, identified and coded under the *broad, recurrent and consolidated* themes as shown in Figure 4-8 p 91. The findings are reported in the following sections.

4.5 On DBI response frameworks (EQ1)

During the discussion on personal data breach incident (DBI) and response frameworks, besides revealing their organisation's DBI (organisation DBI), interviewees also referenced data breach related cases (referenced DBI), and some interviewees also shared their experience of being a victim (personal DBI) of such data breach related cases. Although interviewees were asked to share hypothetical DBIs, H8 did not mention or share any. The rest of the interviewees referenced data breach related cases or said *other organisations* (e.g. as in insurance claim cases). C18 who said she can *talk about the aggregates of my experiences* expressed her concerns on the *mosaic* of linked/chained breaches: *'While the TalkTalk breach itself was huge in volume, it wasn't just that breach alone that resulted in the end consequences. I think we have got so obsessed with reporting individual leaks and nobody is looking at the mosaic, nobody is looking at the jigsaw effect because data is so hard to track. If LinkedIn breached - the LinkedIn breach results in somebody being able to pretend to be me to apply for a job or something, I can't prove that it was the LinkedIn breach. So, I think there's a lot of harm that's going under the radar and there's a lot of harm that is - cannot be attributed to a particular incident because they are just so many'*.

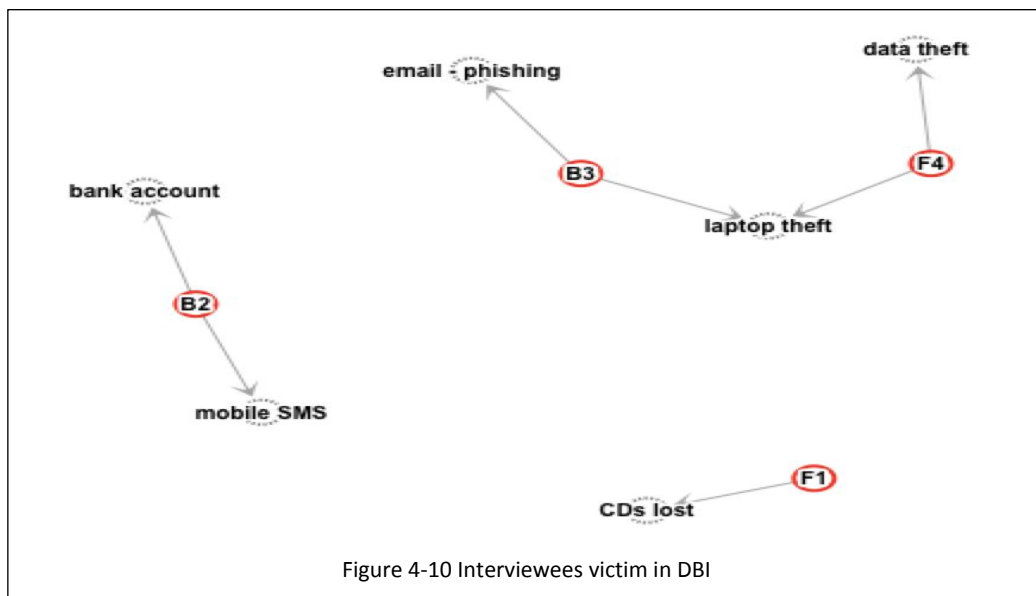
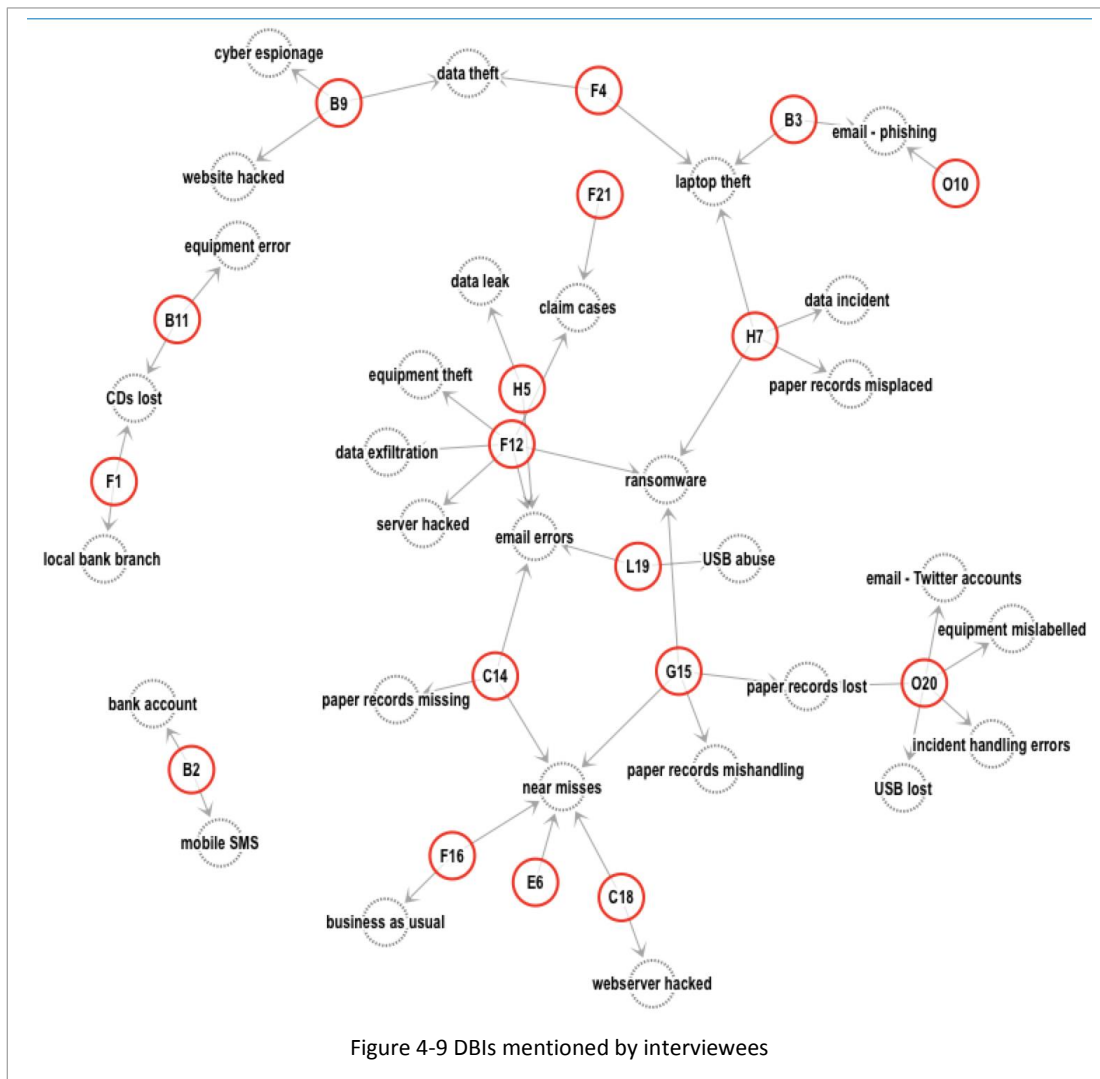
There were indeed many DBIs as mentioned by interviewees. Figure 4-9 p 94 revealed the various cases¹²⁶. Even *near misses* were mentioned (E6, C14, G15, F16, C18), and C18 expressed that *near misses* are an indicator of catastrophes to come. Moreover, F16 said: *'If someone says 'Oh, nothing happens' then either they are not aware or they are not just telling the truth. So, I think every organisation, you know, be it universities or be it schools or banks everyone gets influenced from malwares to DDoS attacks and various kind of data thefts happening internally and those kinds of things'. 'There have been a lot of breaches – and people are keeping quiet', said L19.*

B2, who experienced a DBI involving his bank accounts, reported that a lot of data breaches occurred at local branch level (banks) and these were not reported internally due to lack of branch level monitoring. Although not the same bank case as B2, F1 reported that her local bank branch, as shown in Figure 4-9 p 94, suffered a DBI. In connection with cases within local government, G15 who had direct involvement in information governance (IG) and fraud investigations, pointed out that *'the most important stuff (sensitive data) tends to be health and social care stuff gone missing'*. H7 also reported similar cases under *data incident* and *paper records misplaced* (reported missing to police).

4.5.1 Organisation, personal and referenced cases

To analyse these cases and report the themes these cases were grouped into *organisation cases* (O mentioned), *personal cases* (P mentioned) and also the *referenced cases* (R mentioned) (e.g. TalkTalk, Twitter etc). The *O mentioned* cases were those DBIs that interviewees had exposure to or experienced in their organisation (e.g. B9, O10, G15, O20) or have experienced in their field or role in other organisations (e.g. B11 in his consultancy role, F12 and F21 in their insurance field). F12 expressed this: *'I'm not aware of any personal data breaches from this company, but in terms of the claims that I've dealt with, we see data breaches in terms of the claims'*. F21 also stated this: *'Well I've been involved in many claims so I see those cases and I have advices on how we lead those claims'*. Cases whereby the interviewees were victims (P mentioned) e.g. F1, B2, B3 and F4 were also identified as shown in Figure 4-10 p 94. B3 was a victim in an email phishing incident in which O10 was the CEO of the organisation that suffered the DBI. This link was also shown in Figure 4-9 p 94. That was the only case that has this relationship, all the other cases, although they shared the same types of breach name, were not from the same DBI. For example, CDs lost was mentioned by interviewees B11 and F1, however this CDs lost breach was not the same DBI.

¹²⁶ The word *case* was adopted to cover all incident types (security and data breaches) reported by interviewees.



Interviewees that *referenced* difference cases are shown in Figure 4-11 p 95. DBIs that interviewees have *referenced* cases e.g. TalkTalk were marked under *R mentioned* as shown in Figure 4-12 p 96. The types

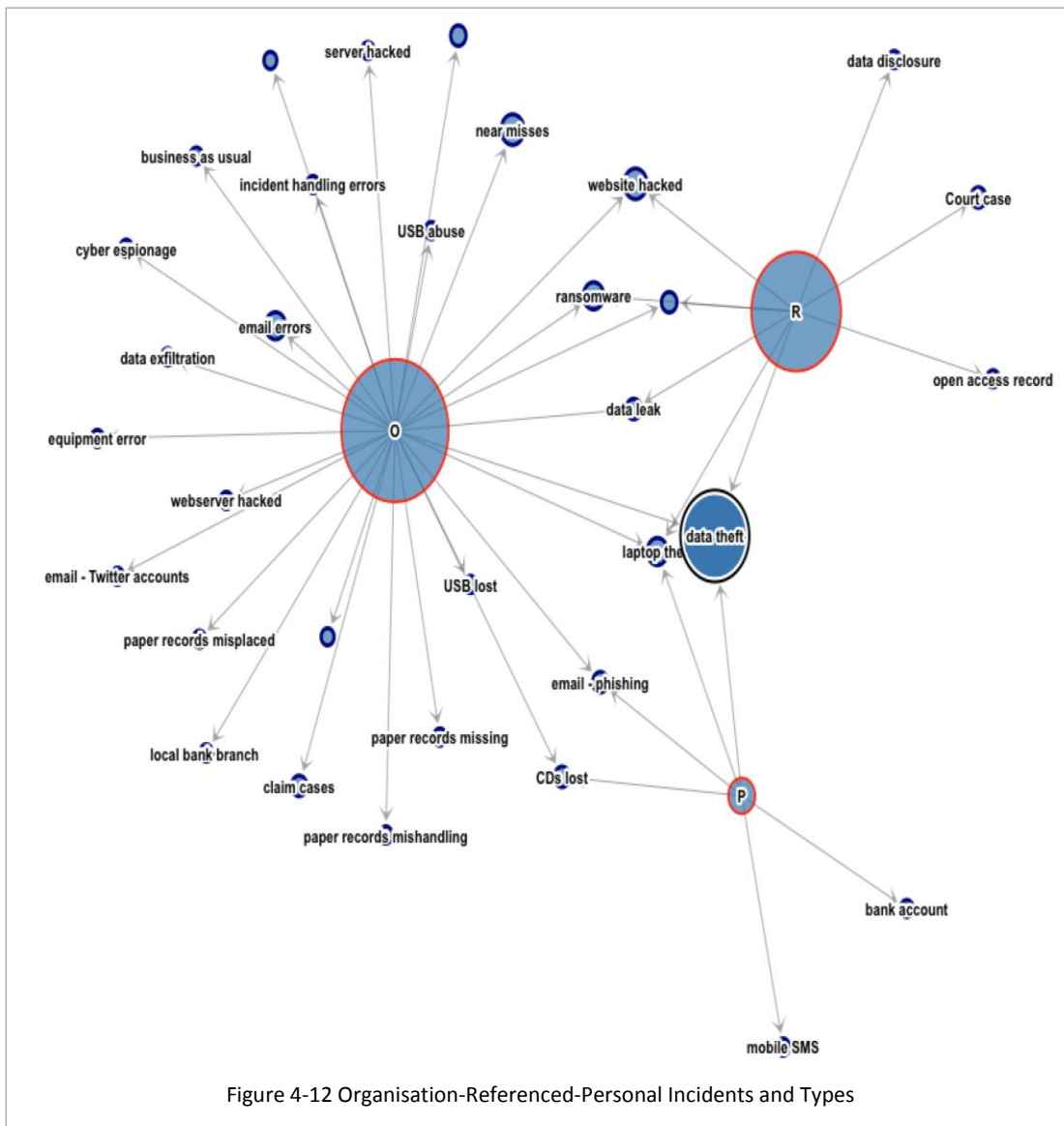
of breaches¹²⁷ or incidents (e.g. email errors, data theft, email phishing) were extracted and analysed from the *recurrent themes* shown in Figure 4-12 p 96. In Figure 4-12 p 96, the circle size indicates the number of cases mentioned. It showed that the majority of incidents mentioned by interviewees were DBIs in their organisation (O mentioned – the largest circle) with 39 mentioned cases, referenced DBIs (R mentioned cases) came up 32, and seven mentioned personal (P cases) DBIs. Data theft (which included TalkTalk) breach types were the most frequently mentioned with 22 counts. *Data theft* was the label for data incidents that were intentional or malicious, involving exfiltration of data that compromised privacy and/or confidentiality. *Email errors* involved emails sent without blind copying (bcc) or *TO* incorrect recipients.

Interviewees e.g. F1, B9, F12 and G15, used the term *cyber* for data theft/crime and internet related incidents. F1 said: ‘One of the problems with cyber, it is always labelled as an IT problem. It’s not, it’s actually people using IT which causes the biggest amount of risk. People complacency’. ‘We used to call it fraud and crime but now we call it cyber-crime because it’s way sexier when it’s cyber-crime’ (B9).



Figure 4-11 Referenced DBI

¹²⁷ There is no definitive list of data breaches or a uniform way to label these. ICO on their website <https://ico.org.uk/action-weve-taken/data-security-incident-trends/> [Accessed 29-December-2018] used *data security incident* and *cyber security incident* for reporting the types of cases or incidents.



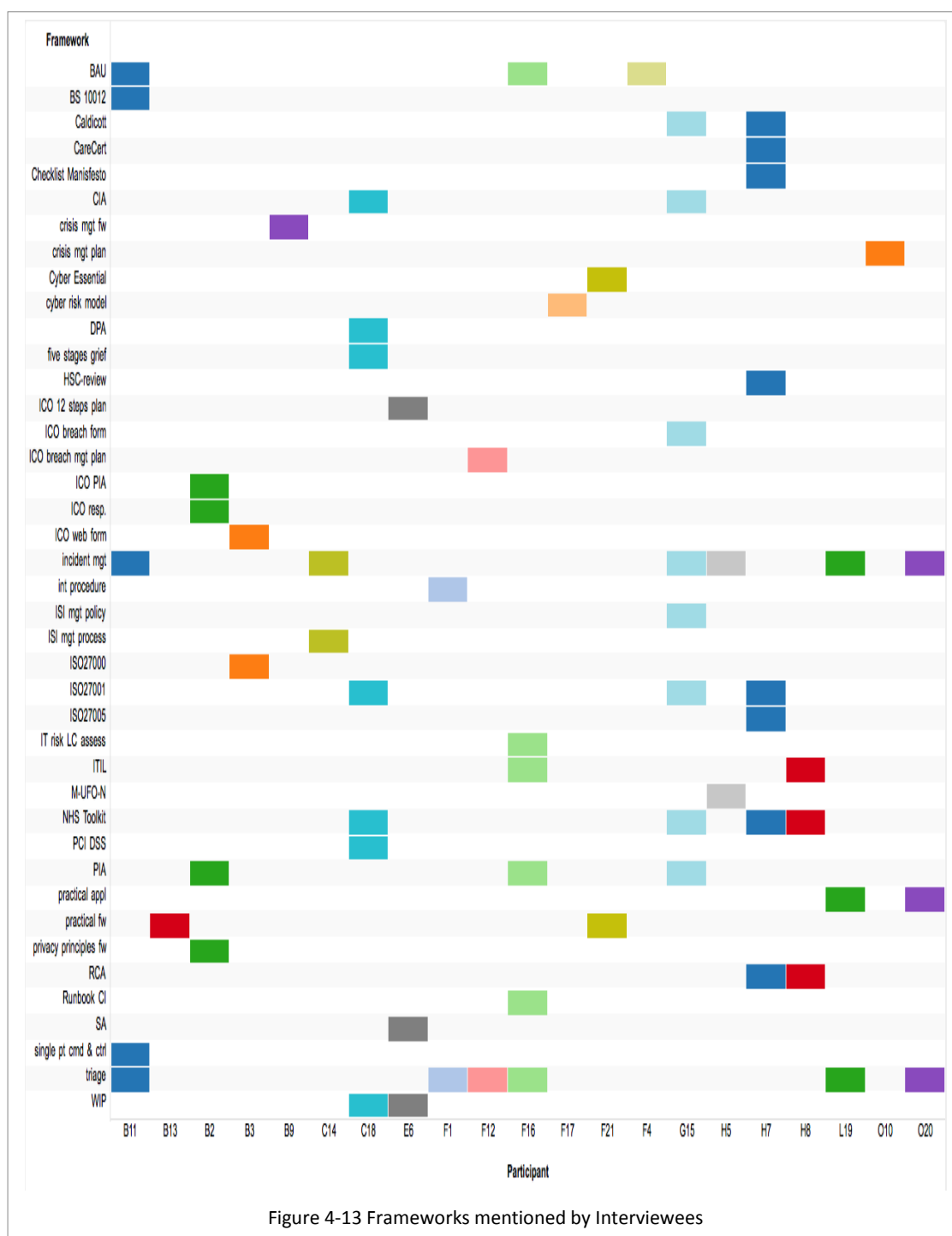
4.5.2 Frameworks mentioned by interviewees

Although there were no dedicated or specialised DBI response frameworks it appeared that there were frameworks to handle security and data related incidents. Such frameworks that were in place or work-in-progress in organisations were informal (ad hoc and not written down) (B11, O10, L19, O20) or formal (customised or standards/industry driven and written down) (F1, E6, H7, H8, B9, B11, F12, C14, G15, F16, C18, F21) types.

Various frameworks are listed in Figure 4-13 p 97. A network view of interviewees and frameworks is shown in Appendix L, Figure L- 5 p 229. These frameworks handled incidents, not just for handling or responding to DBI. **The study revealed that there was currently no dedicated framework for handling just DBI.**

However even when there were incident response frameworks, these were generally not followed or were ignored during a crisis or disaster such as DBIs (H7, C18, B11). During DBIs, which were considered as a crisis or a disaster (F4, H7, B9, B11, O10, F21), people panic or over react, *all over the*

place or were under time pressure to respond (B9, B11, F12, G15). In the case of TalkTalk – which was referenced by many interviewees – F12 said ‘But the problem was they (TalkTalk) got panicked’.



Those that reported they have formal frameworks, also mentioned training, teamwork and responding based on common sense or basic or intuitive or on the spot human approaches (B9, B11, F12, C14, F16, F21). Those without formal frameworks were still able to handle a crisis DBI due to teamwork or common sense and/or leadership skills or through experience (O10, L19, O20). However, even F21 who expressed lack of confidence in any guidelines also said this: ‘If somebody is using a framework as a guideline it's arguably better than nothing but most of the time those are common sense guidelines, I mean there is very little magic formula in them. They are common sense, relatively basic standards’.

It was clear that even without any written down, formal frameworks, when faced with a crisis such as a DBI, organisations have no options but to react to the incident. This was demonstrated by O10, L19, O20 and also interviewees who were in the process of creating their formal DBI frameworks (E6, F16, C18) in preparation for the GDPR.

4.5.3 On standards, plans and tools

Existing standards or industry driven frameworks were seen as expensive (e.g. L19) or mostly for *tick box* exercises (B2, H7, B13, C18, L19, F21), and not taken seriously. In organisations where there were multitude legal requirements, the different sets of standards and principles meant that getting a good working set of standards was difficult (C18). A *cut and paste* exercise of these standards was done which meant that during DBIs, the procedures were not followed (C18). In C18's organisation providing social and/or humanitarian services exposed them to not only DPA but also various regulations, including compliance to PCI-DSS. There was a similar situation with C14 and also in the banking sectors (F1, F16). Hence in F16's organisation they utilised multiple incident response frameworks.

None of the interviewees mentioned the ISO/IEC 27035:2011-IT-Security techniques-information security incident management¹²⁸, although formal information security management process or policy were adopted by C14 and G15 for their organisations.

The ICO breach management plan¹²⁹ was referenced but was not appropriate during DBI response as time is of the essence (F12). G15 stressed that the procedures, the responses and the management of the incident were very important and pointed out that the ICO's Data Protection Breach Notification Form¹³⁰ does not handle a DBI case dealt in the health and social care context which involved vulnerable children. It was considered a good guide but not useful for conducting an investigation (G15).

For the insurance industry, F17's organisation has produced *cyber models* for (probabilistic) modeling of cyber events and threats¹³¹. These initiatives emphasised the *cyber* related incidents which indirectly also placed DBI under a wider radar, and as described by C18 – the mosaic issues of interweaved, interlinked personal data with a host of PII in cyberspace, making DBI response more urgent and critical to address. F17 said '*Cyber is in its infancy. Now, the only thing that really will wake people up is that there's a wide scale event that affects a lot of people. Like a hurricane, and we call this the Hurricane Andrew of cyber. It will happen*'.

Although DBI response frameworks have not been targeted by standard bodies, the British Standard Institute (BSI)¹³² had issued an updated BS 10012:2017 version – driven by the GDPR – for the *Data Protection - Specification for a personal information management system* (B11). Sooner or later, DBI

¹²⁸ This IS Incident Management standard was used by Tøndel et al. (2014), Hove and Tårnes (2013) and ENISA (2012).

¹²⁹ The ICO's guidance on breach management plan that was accessed on 22-January-2017 is no longer online.

¹³⁰ Report a data security breach (DPA): <https://ico.org.uk/for-organisations/report-a-breach/> [Accessed 27-December-2018].

¹³¹ <http://www.air-worldwide.com/Models/Cyber/> [Accessed 27-December-2018].

¹³² BS 10012 specifies the requirements for a personal information management system (PIMS), which provides an infrastructure for, among other things, maintaining and improving compliance with the Data Protection Act (DPA) 1998. British Standard BS 10012: <https://www.bsigroup.com/en-GB/BS-10012-Personal-information-management/> [Accessed 27-December-2018].

response frameworks will appear as seen by a recent update from the US President's Office of Management and Budget on *Preparing for and Responding to a Breach of Personally Identifiable Information*¹³³.

Although there was a tool, Datix, which was widely used for incident response¹³⁴ (H7) in health sectors, H8 stressed that *'incident response mechanisms were not efficient, because of the need for solutions to handle people, process, and technology'*. Even though a mandatory NHS toolkit¹³⁵ existed which included a wide range of mandated reporting standards¹³⁶ (including data breach incidents), cyber response initiatives such as CareCERT¹³⁷ for the health sector were recently introduced and are now in place (H7).

4.5.4 On effectiveness and efficiency

As regards the effectiveness and efficiency of the frameworks, a striking dialogue with C14 revealed the nature of DBI response being a *human response*, and that auditing of frameworks was deemed as difficult.

INT: *Would you say that your current processes and procedures are functioning efficiently and effectively?*

RES: *As far as we know it's very difficult to test. We haven't actually done an audit on people's awareness or knowledge. I sense it in any large organisation, all over country, there will be incidents which are not reported and one of the tensions is that in a way it makes people - they have to say something about themselves that they've done something which could be in breach of our policies or procedures. So, they have to – whistle-blown themselves almost and that's quite difficult.*

Similarly, C18 said *'It's difficult to measure'*, but concurred with F21 that having a framework may be better than nothing.

C18 expressed that an efficient framework is one that has *'sized just-in-time information'*. According to B2, for a framework to be effective, it will need to have an effective regulation in place, it needs a strong Regulator (ICO) that is actually not just doing a tick box exercise. The lack of funds from the government in ICO was identified as an issue by C18 and F21. On the other hand, on effectiveness and efficiency, O10 offered this: *'it's about the team what they have to do and who does what'*.

B13 advised his clients that *'it's much better to be proactive and getting a plan in place before you have the incident, something you could do there'*. He also advocated for a practical framework, whereby such policy framework will need to have traction within the organisation. Testing or piloting or demonstrating or putting such *practical frameworks* or guidelines/plans/policies into practice was considered another factor for such frameworks to be usable or practical (B9, B11, B13, F12, C14, F16, F21).

¹³³ https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf and news report: <https://www.bna.com/us-promotes-riskbased-n73014449642/> [Accessed 27-December-2018].

¹³⁴ Clinical and information incidents, where DBI were viewed as less critical or important.

¹³⁵ IG toolkit (changes in 2019/20): <https://www.igt.hscic.gov.uk/> [Accessed 27-December-2018].

¹³⁶ Shared by H7:

<https://www.igt.hscic.gov.uk/resources/HSCIC%20SIRI%20Reporting%20and%20Checklist%20Guidance.pdf> [Accessed 27-December-2018].

¹³⁷ <https://www.igt.hscic.gov.uk/CyberWhatIs.aspx> [Accessed 27-December-2018].

4.5.5 Practical response activities: checklists and triage

Some interviewees were not directly involved or have little experience with DBI response handling (B2, B3, F4, B13, F17) in organisations. B13 suggested asking practical questions: *‘Are people aware of it? Do they understand its importance? Is it something which is going to be actioned and acted upon if there is an incident?’* Besides B13, other interviewees (B2, H7, B9, B11, C14, C18, O20) also used questions or checklists in their frameworks or during the response. It seems that accountants/auditors have placed privacy and personal information as an agenda to address during incident management and response. B2’s (an auditor) shared notes – privacy principles framework – which consisted of a list of questions (checklists), had a section for incident management and response which asked *‘Do you have an incident response plan that addresses privacy, personal information and/or data quality?’* The checklists are based on the Generally Accepted Privacy Principles adopted by Chartered Accountants in US and Canada.

These checklists or questions will need to address the issues with gathering and assessing information for timely response to individuals. The *gathering and assessing of information* – the triage which circulates between *detection and reporting, assessment, decision* – appeared to be done by interviewees (F1, E6, B9, B11, F12, F16, L19, O10, G15, C18, O20)¹³⁸ who were directly involved with the response activities. The *information* does not relate solely to security or technological information or answers as highlighted by the non-security lead response whereby a governance approach was needed for responding to individuals. Asking relevant questions to ascertain *the nature of the breach* so that appropriate response activities could be conducted required experience and also judgment calls, especially where sensitive personal data and vulnerable individuals were involved.

H7 said his first question to his client (when asked about DBI response activities) was *‘has the source of the breach been identified and has the breach stopped?’* However, to answer these questions will require *circular and iterative* response activities to gather and assess the information – initial triage as outlined by O20. Triage is a circular, iterative activity of gathering and assessing information which happened between detection and reporting (O20).

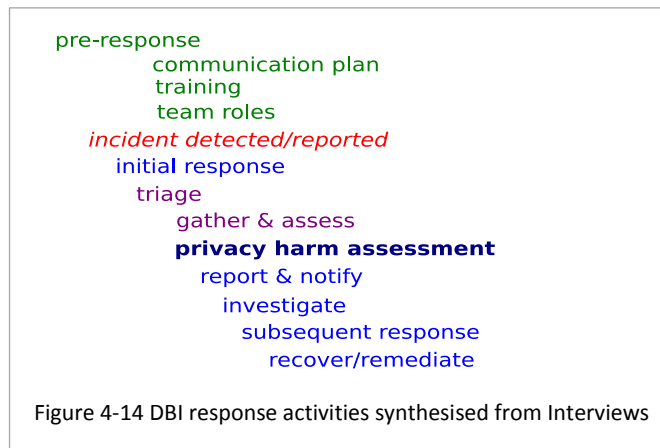
In essence, triage was used during the initial phase namely immediately when a data security incident was detected or reported. Before reporting (to relevant authorities) and notification to affected individuals, information gathering or collection was conducted followed by assessment or investigation (i.e. digital forensics investigation). Assessment involved checklists or questions and/or impact assessment approaches or use of specialist tools. The outcome of the triage was to obtain actionable information for timely response to individuals. F16 used the term *actionable information* in the discussion on prioritisation. Timely response will be driven by the GDPR notification timeframe.

Depending on the response goals i.e. business driven (e.g. concerns for organisation’s reputation) or data privacy driven (e.g. concerns for privacy harm to individuals), the response activities for gathering and assessing the information will be different. However, PHA will be needed to drive the DBI response such that the consequences or damages of the incident to individuals could be assessed. The DBI response

¹³⁸ C18 did not mention triage but did mention investigation (assessment) and questions to ask. There was an assessment or investigation activity following detection of the event.

activities were synthesised and shown in Figure 4-14 p 101. These activities are presented linearly downwards – without any lines/arrows – to show that there is a sequence in the response phases. Instead of a phased response, B11 discussed two levels of response – a short term and a long term response.

The DBI response mechanisms (ad hoc) as described by O20 showed the working of triage and the various response activities (security and non-security). O20 outlined this: *'you have a whole series of decisions about who to tell what and when. So depending upon the nature of the incident (or breach), each or any of those groups may need different kinds of communication and at a different point in the process.* The response activities called *'for technological, communication, people and process response mechanisms whereby the prioritisation of the activities were driven by the nature of the breach'.*



Based on the natures of the breach, experience and judgement calls, the priorities tend to shift between technological response, people and communication response. Where DBI involved personal data or sensitive data, the potential harm to affected individuals was considered a priority which then drove the people and communication response activities.

4.6 Concerns or views on DBI response (EQ2)

Interviewees who were responsible or involved in their organisation's DBI response planning highlighted that they will be reviewing or setting up their response mechanisms (e.g. E6, O10, C14, F12, F16) because of the GDPR. As stressed by B11, organisations should have *'some sort of procedure or process in place that they will follow well before the incident'*. Hence testing and training were seen as crucial pre-response activities for successful execution of the response framework.

As DBI is a business-critical or crisis event, any response mechanisms, including pre-response planning, need to address not only the security aspect but also the non-security aspects of the incident.

Moreover, a DBI response framework will need the capabilities to handle the wide spectrum or nuances of data security related incidents from business as usual (BAU) (e.g. DDoS attacks) to business-critical incidents (e.g. website hacked or personal data compromised). Having one system or framework to include both the security and non-security aspects will need the involvement of relevant subject matter experts, and such frameworks need to allow the capabilities and flexibility to handle the nuances of DBIs.

The issues with incident management systems or frameworks were best summed up by O20: *'I think a lot of the incident management systems are not set up in a manner which allows information to develop and the incident management needs to develop with it and I think because of the nature of*

personal data loss, there may not be a moment at which it happens and a moment at which it has finished happening’.

Although detection and assessment of DBI proves to be challenging, when an incident occurs, work on the basis that it is a breach, and at the very least have a pre-response plan that includes a response communication plan for individuals and the media. Such a pre-response plan should have a DBI response framework that is driven by the assessment of damages or harm to their customers or individuals. These will require organisations to know their stakeholders, data assets or data/record types classification or a data risk matrix, and such pre-response plan and DBI response framework to be put into practice by testing and training. Having a DBI response framework in place as part of pre-response planning and testing will ensure the DBI response activities can be managed or coordinated. Even with well-defined roles/responsibilities for the response team, the lack of coordination or team leadership could potentially make or break the timely response that was needed during a crisis as shown by the response conducted by B9, B11, O10, G15, O20. Moreover, even with actionable information obtained from technological or technical response involving triage, C18 highlighted that as a frontline technical expert, a lot of time is spent explaining and justifying to senior decision makers so that they can understand the situation. She added that the *‘person with the seniority to be able to get stuff done is very rarely the person with the level of technical understanding to appreciate what needs to be done and in what order’*. The subject matter expertise issues can potentially be addressed with appropriate response planning, testing (considered important activity by B9, F12, B13, B11, F16, C18, F21) and coordination as done by B9, O10 and B11.

Although different views/comments were expressed for prioritisation of the DBI response, on the whole, interviewees indicated no objection concerning the notification to affected individuals. In fact, O10 said, *‘it is good practice and it is common sense’* and expressed that there is no need for regulation (GDPR) to tell us this. In the health sector which has the highest reported DBIs (H7), mandatory procedures existed to notify individuals, and H8 commented that *‘it is very important’*. B13, who was a specialist in governance, compliance and risk also said it is very important to notify if you want to retain the trust of your customers. He also said the customers have to be told as soon as you know, and to do the work to make sure you understand the facts. Getting the relevant facts of the nature of the breach within a 72 hour timeframe *‘is an incredibly tight deadline’* and F12 further added that *‘it must have been horrendous situations’* for large organisations like TalkTalk to respond in such a short timeframe. However, in the banking sector, besides stating that *‘it is key to let them know’*, F16 said their target was even stricter (imposed by other regulators); a 24 hour timeframe was the aim. Hence there was now a drive to use tools to automate incident response.

Most organisations viewed their business goals/aims as key priorities (F1, B3, F12, F16, B11) i.e. focusing on their business or company reputation rather than the potential or likely impact of the DBI to their customers or clients. In the health sector, the emphasis was driven by mandatory clinical incident reporting and notification. In the public, social care and voluntary sectors (G15, C14, C18), public interests and political agendas were at play. However, their customers were also a key consideration when it comes to DBI response.

Moreover, the triage activities were mentioned by interviewees with technical or IT security backgrounds or DBI response professionals/consultants and were driven primarily by IT security impact assessment (F1, B11, F12, F16, O20) and/or by business impact assessment (F1, B9, B11, F16) (i.e. business goals). Those that were driven by data types or the nature of the breach or concerns for the individuals whose data was comprised followed a (human-driven) governance or non-security lead response (B9, O10, C14, G15, C18, O20). For this response, social care risk assessment (G15) or stakeholder impact assessment (B9) or data privacy concerns (O10, C14, O20) or breach of confidentiality (C18, G15) underpinned and drove the response mechanisms. Both these response activities (security and non-security led) need to be coordinated or managed to ensure that accurate information (technical and non-technical) was gathered and assessed for timely response to individuals.

4.7 Concerns or views on privacy harm to individuals (EQ3)

Given that *distress* was a recognised non-pecuniary damage – when organisations breached the GDPR, besides the hefty fines imposed in the GDPR (highlighted by B11, G15, F17 and C18), and the associated response notification and monitoring costs, there will also be the potential liabilities from affected individuals (F12, F21) who have the right to sue for distress and claim for compensation. Although cyber insurance policies may not cover damages of the end users (F12), F17 highlighted the use of the term *silent cyber* whereby a lot of insurance policies were paid out, which involved data related incidents, without the use of the term cyber.

There were different concerns and views on privacy harm, and although privacy harm was considered as *tricky to measure*, various suggestions were made on how to assess privacy harms, which indicated that there was *value* attached to (personal) data. The *value* attached to one's personal data has financial (pecuniary) and non-financial (non-pecuniary) costs to the organisations. Instead of *value* C18 used this term *human costs*. Knowing how these costs could be translated into privacy harm costs as a consequence of an organisation breaching the GDPR or the data privacy principles, would require ways to assess privacy harm. Assessing such harm will be challenging as expressed by C18: *'because you can't trace the consequence to a single or even a set of events because data is data and it's all over the place. The effect on society as a whole where the commoditisation of data abuse has led to a race to the bottom - to abuse the most data for the most money'*.

As pointed out by B11: *'It is a new way of thinking because most organisations are focused on the organisation itself. They are not focused on the individual, they are there to make money, they are there to achieve their business goals. The risk to the individual - it will become better'*. It will become better, with appropriate impact assessment of privacy harm to individuals. B11 reasoned that under the GDPR, the emphasis on privacy by design, PIA and the introduction of privacy officers (Data Protection Officer) will put more burden on organisations to reassess the way they view or handle personal data. C18 also raised the role of the GDPR in that *'it takes the good practice and makes it the bare minimum'*. The good practice was enshrined under the *unfairly and unlawfully processing personal data and has, caused you harm*. As to whether this harm is important, O10 expressed that *one should not bear the pain if one has suffered a loss*.

Furthermore, C18 viewed that the role of the organisation in society should be to do good, to bring net good to humanity, and with the GDPR, it should be easier to make the case to people that in order to do good, you have *got to do right*. As pointed out by O10 on ethics: *'It's about doing the right thing'*.

An assessment approach – for prioritisation as well – was shared by F17, who pointed out that there was a relationship between the type of industry sector and the type of *value* attached to the lost or compromised data as perceived by the affected organisation. He revealed that in healthcare it will be about making sure your patients are not affected i.e. a humanitarian aspect. On the retail side, it will be about making sure that the retailer does not have to pay a lot of money to customers whose accounts are affected i.e. a fiscal aspect. In the education sector, it will be about reputation loss if academic work and research work were compromised (lost or destroyed) i.e. an emotional aspect. In comparing the liability risks associated with the humanitarian, fiscal and emotional aspects, the liability risks for health data far exceed the financial data loss and the reputation loss. F12 also expressed that health data carried huge liability risks. For F21, health data is personal data and financial data may or may not be personal data *but certainly a personal harm or threat to an individual if financial data relevant to the individual is lost, stolen, infiltrated or damaged*.

4.8 What did the interviews expose? (RO2)

4.8.1 Organisations and DBI response

How an organisation handles or responds to a DBI will depend on the nature of the organisation and how it interacts with the public. Although there were incident frameworks or procedures ranging from standards to best practice guidelines from various institutions, the findings from the interviews indicated that organisations across the sectors do not use a specific framework for responding to DBIs. There were numerous incident frameworks used in practice in organisations. None of the incident frameworks referenced or applied the incident management standard (ISO/IEC 27035:2011), the privacy framework standard (ISO/IEC 29100:2011¹³⁹) or followed ENISA's holistic *personal data breach handling procedure* (Appendix G, G- 1 p 216). Even where ISO 27001 and Cyber Essentials were mentioned, in general such standards/schemes were viewed as tick-box exercises with little practical relevance. However, in the health sectors where a mandatory information governance (IG) toolkit existed for clinical type responses, DBI was viewed as secondary or sometimes ignored due to the reliance on tools (e.g. the use of Datix). It was clear that existing standards, including the mandated IG toolkit, do not have the capabilities for handling DBIs. The introduction of *cyber response* initiatives such as CareCERT¹⁴⁰ and also Caldicott¹⁴¹ version 2 further amplified the issues around the handling of DBIs in health and social care sectors.

The ICO's notification guide (ICO, 2012b) was mentioned as a guide for reporting to ICO, but the breach guidance management plan (ICO, 2012a) was found to be not suitable for investigation where *time*

¹³⁹ The standard for Information technology – Security techniques – Privacy framework covering privacy controls and PII.

¹⁴⁰ <https://www.igt.hscic.gov.uk/CyberWhatIs.aspx> [Accessed 29-December-2018].

¹⁴¹ <https://www.igt.hscic.gov.uk/Caldicott2Principles.aspx> [Accessed 29-December-2018].

is of the essence. Information security management processes or policies that have been adopted do not document or specify the incident response processes or activities. Also, the incident phases and processes lifecycle as shown in the IMP diagram Appendix E, Figure E- 1 p 214, did not reflect what happens in organisations or how the interviewees respond when faced with security or DBI incidents. Instead, interviewees have used other best practice approaches (e.g. the OODA loop) or ad hoc (not formally written procedures) but systematic approaches, including checklists for handling and responding to DBIs.

One notable finding was that interviewees regarded incident frameworks and/or the response handling as *common sense or basic or intuitive or on the spot human approaches*. However, there was a general consensus that having a formal written, tested and practical *pre-response* procedure/plan that included communication plans and response team roles/responsibilities was essential, especially in view of the impending GDPR. Relevant subject matter experts and a coordinator/leader were key aspects for ensuring that the DBI responses are handled in a timely manner, especially for communicating with affected individuals. Pre-response plans and testing or trial runs were crucial, as during an incident – *viewed as a crisis or a critical business event* – any written formal plans/procedures tend to be ignored or not followed. Moreover, current security incident frameworks or crisis frameworks were not designed for responding to DBI, especially for data privacy harm assessment (PHA). Various impact assessment related approaches such as business impact assessment, IT security assessment, situation assessment and social care risk assessment were used by interviewees. Although PIA was also mentioned, this was not used explicitly for PHA.

Also, views were expressed as to the relevance of having DBI response frameworks, especially one that could address all of the nuances or spectra of DBIs. One approach identified was to view DBIs as business-critical events and hence handle them using a single crisis framework or embed the DBI responses in the business continuity plan. Such an approach then should also embed PHA, which will require *new thinking* in organisations. As stressed by interviewees working in organisations where making profits and/or maintaining their reputation were their primary business goals, *DBI responses focusing on the likely consequences of the personal data breach to data subjects will require new ways of thinking*. This was also reflected in their DBI response posture in terms of prioritisation: *whether to or not to disclose DBIs*. The commercial or reputational aspects were top priority and DBI disclosure and hence response handling was driven by business goals. In non-profit/commercial organisations such as in health, social care, public or voluntary sectors, serving the public or their organisation's social or other humanitarian causes dictated these organisations' goals. This has been referred to as the *culture* of the organisation - the dynamic interplay of public interests and the interests of their clients or customers. Hence in these organisations, breach of confidentiality or reputation harm to their clients was their main concern. These aspects were also reflected in their DBI response posture. Thus, the response could be of three semiotic types: 1) legal (e.g. GDPR), 2) moral or 3) cultural.

However, all organisations who serve or have customers will in general involve confidentiality agreements to protect their customers' interests and these involved personal details. In our interconnected digital world, enforcing confidentiality or protecting the processing of personal data has driven policy makers to introduce stringent data privacy related laws such as the GDPR. Besides hefty breach fines, the GDPR requires the adoption of DPIA or, more appropriate for this research, PIA. PIA

connotes that there is a relationship or link between privacy and personal data (as implied in the term, PII), and as noted by Wright et al. (2011), a breach or loss of personal data is a *distinct risk* for any organisation. As regards risk management and *business impact assessments*, these form the basis for *determining the priority of resource protection and response activities* (Johnson, 2014, p 66). Extending this risk concept to PHA, the emphasis though is on determining the response activities such that the priority is to *limit or minimise privacy harm* to data subjects or individuals whose personal data has been compromised in the DBI.

A challenge then is to construct a PHA approach for use in DBI responses such that breach notification can be prioritised within a short time frame i.e. 72 hours from breach awareness. Although there are numerous available risk assessment methodologies, there is no universal PIA framework which could be used for referencing or comparative privacy risk analysis. Even in the established information security risk domains, there is a lack in agreed reference benchmarking, as well as in the comparative framework for evaluating information security risk methods and information security risk (Shamala et al., 2013). This research steered away from conventional risk assessment approaches or methodologies, and instead adopted Peirce semiotics-ternary. This is the gap in current research on approaches for DBI response handling and privacy harm assessment. One identified DBI response handling method is the use of triage and checklists during the initial response phases. This is discussed next.

4.8.2 Triage for DBI response

As clearly identified by Casey (2013), one of the more complex issues related to triage in digital forensics is the legal perspective on privacy. In practice though, triage has surfaced in the discussion on DBI response. Despite the fact that organisations do not use any formal DBI framework or a dedicated incident response handling procedure for DBI, triage appeared to be in use in practice during the incident response and in the initial phases of incident handling. In particular, triage has been used by organisations to identify or assess the severity of the data breach or in terms of its pragmatic aim – to obtain *actionable information*.

What emerged was that although interviewees did not clearly identify or mention the DBI response activities or use the term triage, it was clear that once an incident was reported/detected, immediate action was taken in a central point/location or on-site. Triage in the context of a DBI is the immediate, initial response action focused on coordinating and/or informing the assigned response team (done during the pre-response) to take specific actions, and communicating the DBI to individuals, which was viewed as a key priority. The challenges raised centred on getting *accurate and timely messages* to individuals. The initial response was followed by subsequent responses, whereby individuals were informed of the actions (remedial and preventative measures) taken by the organisations, and similar measures that individuals should be aware of to protect or reduce likely damages or harm to themselves. Above all, communication channels for individuals to contact the organisation were critical.

Moreover, during the initial response IT personnel or security subject matter experts were called to do the investigation. This is triage in security incident response (or more formally digital forensics investigation). Although triage was not mentioned by non-security or non-technical interviewees,

inherent in the described initial response activities was the gathering of information to assess the nature of the breach. There was an *assessment* or *investigation* activity following detection of the event.

Currently the ICO notification form¹⁴² dictates to a certain extent the information that organisations need to gather and report. Due to the fact *time is of the essence* for notification to data subjects and the need to provide accurate and timely information on the *likely consequences of the personal data breach to data subjects*, the use of triage and PHA could support organisations to meet these compliance requirements. Having a PHA in place may in itself show or demonstrate compliance of the GDPR and is worthy of further consideration.

In triage there is a sequence of gathering and assessing of information that circulates between *detection and reporting, assessment, decision* (i.e. the cycle of phases in the IMP diagram). Based on the findings, triage is an important activity in the initial phase as it is a key initial decision point before any reporting/notification. Due to the fact *time is of the essence* for notification to data subjects and ICO, triage needs to be done speedily or quickly as in a crisis response. The prioritisation of resources for DBI response then is driven by the need to gather and assess information as quickly as possible to notify *without undue delay* as required by the GDPR. Irrespective of the GDPR or other data privacy laws, notifying affected individuals was seen as the *right thing to do*.

The outcome of triage is to obtain actionable information. Hence the first assessment question – *it is a personal data breach?* as indicated in ENISA’s flowchart in Appendix G, Figure G- 1 p 216 – was best answered as *assumed you’re breached* and *err on the side of your customers*. The initial action: to work towards an *actionable - proportionate and ethical - response communication approach* that limits or reduces or minimises the consequences of the breach to your customers and other stakeholders. In particular avoid the response messages and approaches as done in the TalkTalk DBI. As stressed by B11: *communicating the right things to the right stakeholder is going to be one of your key duties*.

Although triage is viewed as *intuitive* and based on experience, it does have systematic steps i.e. gathering and assessing information and moreover there appeared to be breach assessment indicators such as industry sector types and/or data or record types thresholds that trigger and/or direct the types of response. To obtain actionable information that could direct the types of response – be it a security and/or non-security led response, breach assessment, namely PHA, will need to be incorporated into the triage. Although triage was not mentioned in a crisis framework used by an interviewee, and an ad hoc DBI response by another interviewee resulted in this remark from a victim of the DBI¹⁴³: *‘very good response, very, very quick and then they kept me informed of what actually had happened’*, response handling in both cases centred on, and was driven around, the *concerns for and of their customers*.

The synthesised pre-response and initial response handling activities, including triage sequences (gather and access) which were circular (not shown in the diagram, Figure 4-14 p 101) in that the decision

¹⁴² The ICO guidelines for notification and the breach notification form:

https://ico.org.uk/media/1536/breach_reporting.pdf [Accessed 12-February-2017]. This has been replaced by a new form (GDPR era): <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/> [Accessed 31-October-2018].

¹⁴³ The DBI response by O10 and the victim was B3.

to notify and decide what further steps or actionable information is needed, relied to a certain extent on intuition and experience.

One notable surprising finding was the use of questions resembling a checklist of steps during the DBI response and especially during triage. Interviewees used such checklists/questions intuitively, hence the interviewees' triage activities were not formally written down. Moreover, each DBI, depending on the nature of the breach, would change the types of questions which then led to actionable information. In essence the questions/checklists approach was used to conduct *breach impact assessment*, as the aim was to gather information and assess the *nature of the breach*.

On formal incident frameworks, impact assessment on stakeholders was noted in a crisis framework (B9) which was used for all types of incidents. Even in the ad hoc DBI response by O10, the initial step was: *'The first thing you do is call everybody together and you get as much information as you can on the nature of the breach'*. In essence the outcome from the initial triage was to have a handle on the nature of the breach such that affected individuals were alerted to the problem i.e. *'tell the customers and to do anything we could about it'* (C18). The concerns for their customers (not the organisation) drove the initial triage.

4.8.3 Information Governance (IG) and human costs

From the perspectives of DBI victims, response handling by organisations seems to lag or not be quick in certain cases, so that the whole response episode when reported to relevant authorities can fall on deaf ears. Interviewees who were victims have described the consequences of the DBI. Typical words such as *upset, anger, distress, angry, nuisance, annoyance, furious, discomfort and cross* were expressed. Such words can depict the immense disruption to a victim's personal and professional life e.g. as endured by F4.

Although the lack of detection capability has been cited as a contributing factor for the low level of maturity for incident response, this factor alone will not resolve the issues around DBI responses. Even in large banks where detection tools and various incident procedures were used, it was recognised that information (including IT) *governance* related approaches were also needed besides the technical or security led response measures. However, IT governance as discussed in Section 2.2.4 proved to be challenging especially in DBI where the *mosaic of linked/chained breaches* extends beyond an organisation's boundary and hence accountability or who is responsible will be difficult to locate or trace. This concern was raised by C18 which reinforced the *human interactions and interpersonal relationships* issues as described in Section 2.2.5.2. The personal data linked/chained the DBI creating the mosaic of linked/chained breaches. In the wild – cyberspace for example – assessing the *human costs* or privacy harm in the interwoven mosaics of breaches will be very challenging for researchers. Quoting C18 who used the terms *mosaic* and *human costs*: *'there's a lot of harm that's going under the radar and there's a lot of harm that is – cannot be – attributed to a particular incident because there are just so many'* (C18). An insight was revealed by F21 who pointed out *why have a framework if you know you can't do the first step – value the piece of data?* This sets the tone for future research on privacy harm.

4.8.4 Privacy harm

The different views and suggestions from interviewees indicated that there was *value* or *human costs* attached to personal data. The *human costs* attached to one's personal data have financial (pecuniary) and non-financial (non-pecuniary) costs to the organisations. Although valuing or measuring privacy was difficult (Littman et al., 2014), and privacy harm is *tricky to measure* (G15), *distress – a form of harm – is* a non-pecuniary damage. This potentially translates to pecuniary costs for organisations in breach of the law. When faced with DBI, there will be disruptions to the business and the associated reputation costs, which do not require new ways of thinking by organisations as these are the *costs of doing business*. Such costs and the associated costs for breach notification can be managed by the use of appropriate insurance as highlighted by an interviewee from the insurance sector. Similarly, the breach fines imposed by the GDPR are quantifiable i.e. 4% or 2% of global turnover (GDPR Article 83). The *human costs* (e.g. potential litigations and compensation claims)¹⁴⁴ from affected individuals that are associated with the privacy harm to affected individuals, are not readily quantifiable as privacy harm has not been researched in the context of DBI. There were numerous types of personal data as shown in Appendix L, Figure L- 6 p 230. However, interviewees have revealed that there were indicators of privacy harm and there were ways of categorising based on industry sectors and/or the data or record types. There were *types of data that are going to be more harmful than others* e.g. health data (B11). Although distress is legally recognised as non-pecuniary damage, O10 commented that distress is a *very vague, subjective term*. In general, though interviewees viewed privacy harm to affected individuals as an important topic.

If an organisation is not prepared to address DBI response such that the *human costs* are factored into their response plan, the overall costs of DBI could potentially severely damage the organisation. DBI affects all organisations irrespective of sizes and industry sectors as seen by the reported cases (Appendix L, Figure L- 4 p 228). Even in the health sector where a mandatory Information Governance (IG) toolkit and various cyber-related initiatives have appeared, DBI have not ceased.

¹⁴⁴ GDPR Article 82 provision for right to compensation and liability.

Chapter 5 Prototype Dashboard Design and Build (D&B)

This chapter describes the *doing aspect* of the method and theory described in Chapter 3. In particular the focus is on the Solution Design as shown in Figure 3-8 p 75. Hence this chapter provides the unfolding of the DSR processes and outputs from the SSM literature review and interview study which led to the proposal of a triage playbook and the design and build (D&B) of two versions of a prototype dashboard (dashboard). As discussed in Chapter 3, the RITE Process, i.e. Figure 3-12 p 80, shows the two iterations of D&B and each iteration delivered a dashboard, which was then used in the UES (Chapter 6). The outcome of the D&B was to deliver an artefact, i.e. the dashboard that meets the identified needs and requirements (Section 5.2).

The initial unfolding started with the motivation and an awareness of a problem (Chapter 2) which led to the interview study (Chapter 4). The interview study revealed problems faced by organisations and also suggestions that guided the identification of a research problem and a solution. A triage playbook solution was proposed. The research objectives/sub-objectives RO3 and RO3-1 were formulated as shown in Figure 5-1 p 110. These objectives form the overarching aim of this chapter.

Research Objective/Sub-Objective	Methods
(RO3) To develop a triage playbook for organisations in the UK to assess privacy harm for breach notification support during initial DBI response.	Rapid Iterative Testing & Evaluation (RITE) approach; Prototyping Design & Build (D&B) with developers i.e. Developer1 and Developer2; Build two versions of the Dashboard i.e. DashboardV1 and DashboardV2.
(RO3-1) To iteratively design and build the prototype dashboard (Dashboard) to address the initial breach notification question: <i>to notify or not affected individuals and/or the ICO?</i>	

Figure 5-1 Design & Build (D&B) objective/sub-objective

To achieve (RO3), a prototype dashboard (RO3-1) was suggested for proof-of-concept and proof-of use of the triage playbook. An initial conceptual model of the triage playbook (Figure 5-3 p 113) was created to show how the dashboard implemented the triage playbook.

Before the D&B, a set of requirements was created. As pointed out by Hevner (2007): *DSR projects typically start by providing requirements for research (e.g. what is the problem to be addressed with technology), and then proceeds to design, construct, and evaluate suitable technological solutions.* DSR is research using *design, analysis, reflection, and abstraction* to create artefacts that satisfy given sets of *functional requirements* (Vaishnavi et al., 2017). In terms of activities, the functional requirements¹⁴⁵ were explicated from the identified problems which were transformed into a set of *requirements* and were used for guiding the D&B of the artefact (Johannesson and Perjons, 2014, p 103-104). Johannesson and Perjons (2014, p 104) highlighted that research objectives are also requirements e.g. *goals on the effects of using an artefact*. Their guidelines on requirements were adapted for the formulation of the set of requirements as discussed in Section 5.2. What is not explicit in their guidelines is that the requirements

¹⁴⁵ Functional requirements are requirements that concern the functions of the artefacts (i.e. stakeholders' needs/wants framed as problems to be addressed) unlike non-functional requirements that pertain to structural (i.e. design aspects) and environmental (i.e. technical or architectural) requirements (Johannesson and Perjons, 2014, p 103).

are dynamic due to the iterative nature of the D&B. Requirements were updated during the iterative D&B with the developer as insights or needs from the UES with users were captured. Such needs have to be *realistic* (Johannesson and Perjons, 2014, p 108) and were validated against the research aim and objectives.

The prototyping of the dashboard as done with the iteration of D&B *has potentially powerful effects on the quality of information systems analysis and design* (Privitera, 2016). These effects were realised during the D&B with two developers (i.e. Developer1 and Developer2) and in the form of their dashboards. For example, the first delivery from Developer1 was rejected as it failed to meet the expected quality and requirements. Such *prototype serves as a design tool and its representation acts as reminders and paradigm cases for contemplation of future systems and their use for evaluation* (Baskerville and Stage, 1996).

Furthermore, although Baskerville and Vaishnavi (2016) suggest a pre-theory design framework they did not explicitly describe how to articulate the design elements/constructs (artefacts), and/or how to organise the design artefacts into a collection (a framework). Instead they mentioned the various conceptual models and how they merged these for their theoretical model i.e. their pre-theory framework. Also, Swan and Brunswicker (2018) referenced Baskerville and Vaishnavi (2016) but they did not describe or show how they have used the pre-theory framework. To ensure rigor, the pre-theorising steps for theorising of the triage playbook – based on Peirce semiotics-ternary – were also applied for rationalising and depicting the problem space and the solution design space as described in the following sections. This completes the unfolding of the overall DSR pre-theorising design approach for the triage playbook (Figure 3-11 p 77).

5.1 Identified problem and suggestion

As outlined in Section 1.3, the identified problem is: organisations will need to conduct data privacy harm assessment (PHA) during initial DBI response to meet the GDPR breach notification requirements. In particular, the PHA will need to address the breach notification prioritisation question: *whether to notify or not affected individuals and/or the ICO during initial DBI response?*

The summarised organisations' needs from the interview results and SSM are:

- (a) The need to be sensitive to the diverse views on data privacy and data harm;
- (b) The need to gather information, assess the nature of the breach for data harm to affected individuals;
- (c) The need to address the lack of complete or reliable data breach information during initial stages of DBI;
- (d) The need to notify relevant authorities¹⁴⁶ and the affected individuals within specified timeframe as required under the GDPR.

In outline the main questions and challenges during initial DBI response are:

- (a) Is the data protected/secured (encrypted or appropriate technical and organisational measures?) (information available or obtainable: a yes or no answer);

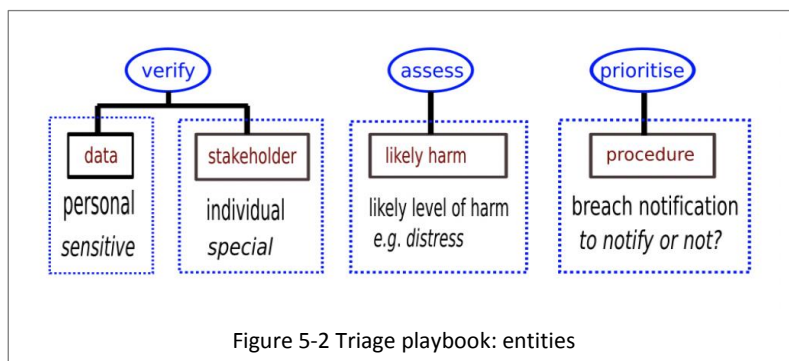
¹⁴⁶ Although the ICO is the data authority for breach of the GDPR, there are potentially other authorities, e.g. Action Fraud, who may also need to be informed.

- (b) *Is the data personal data?* (information available or obtainable: a spectrum of data types);
- (c) *Is there a risk or high risk to the rights and freedoms of natural persons?* (criteria not clear: data privacy impact (e.g. distress) on affected individuals);
- (d) The individuals affected need to be identified (information available or obtainable: category of individuals).

As there is little research on privacy harm to individuals as a consequence of DBIs and on triage for initial DBI response, this research suggested a triage playbook as outlined in Section 5.1.1. Also, this research proposed the use of Peirce semiotics-ternary (Chapter 3) for formalising and rationalising the triage sequence of steps i.e. verify, assess and prioritise. These triage sequence of steps were synthesised from the literature review (Chapter 2). Similarly, Peirce semiotics-ternary was used for rationalising and depicting the design elements/constructs that constituted the triage playbook. To visualise the transition from the *problem-situation* i.e. problem space to the design and solution space, Figure 5-4 p 121 and Figure 5-5 p 122 were created.

5.1.1 A triage playbook solution

From the synthesised findings from the SSM study (Figure 2-11 p 61) and interview study, the explicated entities for the triage playbook are shown in Figure 5-2 p 112.



The triage playbook components:

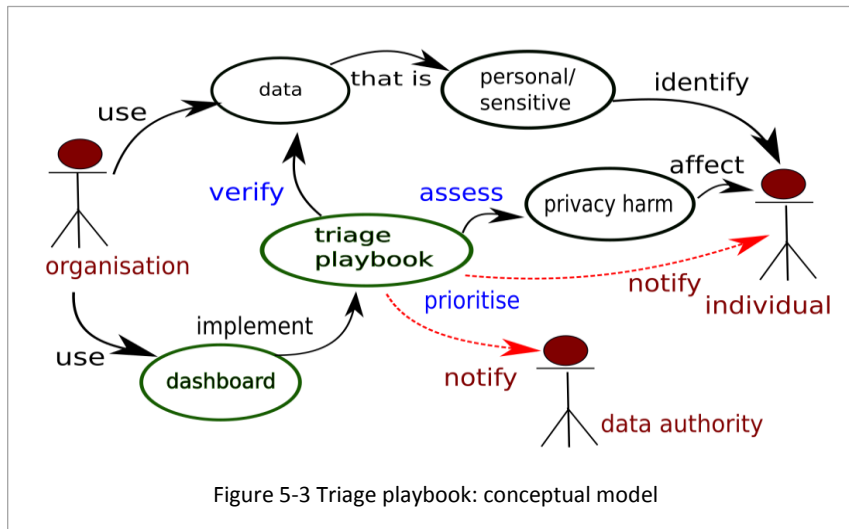
- (1) Triage for initial DBI response (triage sequence of steps).
- (2) Checklists for data privacy assessment (checklists).
- (3) Data harm matrix with pre-set entities and scores (data matrix).

The triage sequence of steps (i.e. verify-assess-prioritise) (discussed in Chapter 2) with the checklists are shown in Appendix N p 233. Checklists i.e. a set of questions and answers were used to direct the focus on the nature of the incident or breach. The sequence of steps drove the checklists which captured the user's DBI scenarios and breach information. The captured breach information was used with the data matrix (shown in Appendix O p 236), to derive the level of data impact and impact on individuals.

The triage playbook conceptual model in Figure 5-3 p 113 provided the context for the D&B. The simple DSR notations from Johannesson and Perjons (2014, p 4) were used for the relationship of the artefacts (represented by ellipse) and the environment i.e. the organisations and people (stakeholders). The data authority is the ICO (UK).

The GDPR (2018) and the associated ENISA (e.g. ENISA, 2012) and ICO reports/publications i.e. (ICO, 2012; 2018) were the main sources for identifying the regulatory breach notification requirements

and the entities as specified in the data matrix. The following sections outline the requirements for the dashboard and their formulations.



5.2 Dashboard requirements

In Johannesson and Perjons (2014, p 108), their DSR method framework also included *guidelines for defining requirements* which were adapted to elicit the dashboard requirements. The extracted guidelines are:

- Specify what artefact to build. Specify the type of the artefact (construct, model, method, instantiation) and its general characteristics.
- Formulate each requirement clearly. Describe each requirement in a precise, concise and easily understandable way.
- Justify each requirement. For each requirement, explain why it is needed and relate it to the problem.
- Be realistic but also original. Ensure that it is realistic to develop an artefact that fulfils the requirements, but also try to be original.
- Specify the sources of the requirements. Describe the literature and the stakeholders that have contributed to defining the requirements.
- Describe how the requirements have been defined. Explain what has been done to define the requirements, in particular, how the stakeholders have been involved and how the research literature has been reviewed.

The following sections were guided by (c), (e) and (f).

5.2.1 High-level requirements and assumptions

The high-level requirements are:

- (1) *PHA information*: Provide PHA to affected individuals in the response steps.

- (2) *Incident information and PHA information*: The response steps, including PHA can be conducted speedily without undue delay or within 72 hours of being aware of the incident. This is to enable breach notifications (notification) to comply with the GDPR breach notification requirements.
- (3) *User event and incident information*: The response steps need to support the gathering of incident information in phases.
- (4) *Incident information*: Enable the user to capture, track, record and manage the response steps from logging of the incident to closing of the incident.
- (5) *PHA information*: Provide actionable information with breach indicators and alerts to support breach notification prioritisation to affected individuals and to the ICO.

The supporting *other requirements* (non-functional) are also shown with the list of high-level requirements in Appendix M p 231.

The assumptions/constraints are:

- (a) *Initial* refers to the early or first response steps/activities following the awareness of the data incident i.e. initial DBI response steps.
- (b) PHA is a separate response step and is not done under or as part of digital forensics investigation.
- (c) The end-users profile: with DPO status/title or data record management responsibility or compliance/governance role/title or a senior data/security incident manager or senior manager or consultant with the relevant experience/knowledge/expertise.
- (d) The intended dashboard is for end-users responding to DBIs in the UK and driven by the GDPR breach notification requirements.

5.2.2 Formulation of the checklists

This researcher was inspired by Gawande's (2011) *Checklist Manifesto*, which was also mentioned by an interviewee (H7). Although there are no formal or widely accepted steps or procedures or frameworks for conducting triage and the DBI response activities, questions resembling a form of a checklist were used by interviewees. For example, some questions: *How serious is it? How do I prioritise this? What's the severity? How much is the individual hurt?* Similarly, ICO (2012a) also identified questions for assessing the *nature of the breach*. These questions are: *What type of data is involved? How sensitive is it? If data has been lost or stolen, are there any protections in place such as encryption? What has happened to the data? How many individuals' personal data are affected by the breach? What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?* From these examples, checklists were formulated as shown in Appendix N, Figure N- 1 p 233, N- 2 p 234 and N- 3 p 235.

5.2.3 On checklists: background and justification

Checklists have been used in triage in the medical fields as early as 1981 with the research by Wilson et al. (1981) on the computerisation of paediatric checklist and triage system. Wilson et al. (1981) further advocated research by Looney et al. (1980) that software (algorithms for emergency medicine problems) requires *specific concepts and sequential diagrams to discern, maintain, and express thought*. These were the triage principles (*specific concepts*) and the *sequential diagrams* were the sequence of steps for operationalising the checklists. The checklists were used to enable prompt identification of the

nature of the breach for decision support in prioritising breach notifications. Kane (1985) designed a triage instrument using simple checklists for determining which patients ought to be treated at trauma centres, and highlighted that *simple checklists performed approximately as well as weighted scales*. The simple checklists *do work* not only in complex and dangerous work such as in medical, construction, flight cockpits but also in factories and have been used for checking decision making in investment (Gawande, 2011).

Currently, the use of electronic checklists during triage has not appeared as research interests or topics under DBI response domains. As regards cyber resilience, Ahmad (2016) used the World Economic Forum's (2012) checklist tool – *C-Suite Executive Checklist* – for executives to identify specific cyber resilience strengths and weaknesses in their organisations and help *inform their actions*.

Krüger et al. (2012) were motivated by Gawande's 2011 '*No matter how expert you may be, well-designed checklists can improve outcomes*'. They used checklists for their prototype checklist client to show the relevance of their checklist approach in a mass casualty incident domain. In examining the checklist paradigm, they exposed that among experts of rescue organisations, checklists are a highly discussed and controversial topic; opinions differ about *what checklists exactly are and how and where to use them*.

Researchers in the disaster recovery and business continuity domains have discussed checklists for planning and noted that checklists can be *easily referenced* during emergency response and recovery operations (Snedaker and Rima, 2014). Checklists have appeared in security incident literature, for example Hafkamp's (2006) finding: *Using checklists, procedures and dedicated response capabilities, IT organisations are able to faster detect and respond to incidents*. Kane and Koppel (2013, p 65–72) offer a *Risk Assessment and Compliance Checklist* in an Information Security Playbook. In referencing Gawande (2011), Wright and Zia (2011) conducted an experiment involving the analysis of incident response personnel as they reacted to incidents. They examined the response times with and without a checklist, whereby the responders used their own processes and steps to create their checklists. Their research demonstrated how the use of a basic checklist – an effective low-cost solution – reduces the number of false positives. From their finding they concluded that using a checklist is beneficial in an (security) incident response. Using a checklist allowed them *to determine the processes that function better and to integrate these into the system improving practice over time*. Moreover, Wright and Zia (2011) in expressing that there are a wide range of security papers calling for the use of checklists, also quoted Bishop and Frincke's (2005): *security checklists cause both alarm (because they can replace thinking with conformance to irrelevant guidelines) and delight (because they serve as aids in checking that security considerations were properly taken into account)*. They also raised the remark by Bellovin (2008) that a poorly structured checklist *especially if followed slavishly or enforced without thought—can make matters worse*.

5.2.4 Checklists as artefact and conceptual model for decision support during DBI response

A checklist, besides acting as a communication tool (Gawande, 2011, p 70), is an important decision-making support tool at helping in risk identification and assessment (Zhou et al., 2008). Hence a

checklist approach has been used to propose a risk identification ontology (Stufflebeam, 2000; Zhou et al., 2008).

During the UES (Iteration 1), a user suggested adding to the checklist questions on user's levels of confidence for the identified breach information (ReqID 3.3 & 3.4 in Appendix M p 231). Gathering confidence level is a form of obtaining assurance on the validity of the results. Confidence values¹⁴⁷ are captured in well-known Structured Threat Information Expression (STIX) incident structure (de Fuentes et al., 2017). The checklist then acts as a decision-support and assessment tool. In this research, risk is an event e.g. the DBI that may or may not happen. Impact is what will happen (the outcome or consequence) if or when the event occurs. DBI response is conducted when the DBI has occurred or has been reported or logged or detected. So, the focus of the requirements was not on risk assessments. However, the use of a checklist to ask users' confidence or assurance on their answers to the key breach events of interest, e.g. distress suffered by individuals, was to enhance decision-support for breach notification during triage. In a comparative study on using confidence level and *feeling of knowing* in question answering, it was shown that the *level of confidence in the correctness of a recalled answer is a reliable measure* (Costermans et al., 1992).

Moreover, checklists are a type of informational artefact that conceptualise *activities and decisions in work routines* (Reijers et al., 2017). The nature of checklists is that they are a type of conceptual model *that provide a purposeful and relevant representation of a particular real-world domain* (Reijers et al., 2017). This abstraction aspect aligned with the requirements for digital forensics frameworks (DFRWS, 2001; Beebe and Clark, 2005).

5.2.5 On breach assessment for notification

As expressed by the user (f1) who suggested the use of confidence level: '*we would play with the law to a degree to not notify until our confidence factor has got to a certain level*'. Hence the decision to notify individuals and/or the ICO was not *obvious* unlike the Article 29 Working Party (2018) guidelines on breach notification (the Guidelines): *It will be obvious in some cases that, due to the nature of the breach and the severity of the risk, the controller will need to notify the affected individuals without delay*. What is risk or high risk when it comes to breach notification under the GDPR remained unclear. Furthermore, the Guidelines noted that risk assessment in a DPIA is for a *hypothetical* incident and as such has a *different risk focus for assessing the damage or harm to the data subject*. The Guidelines included a list of breach assessment criteria and mentioned risk parameters/consequences e.g. severity risk, but there is little guideline on what are the thresholds for assessing or quantifying the severity of the breach, hence the risk and high-risk issues. The Guidelines for breach assessment criteria are: ***The type of breach; The nature, sensitivity, and volume of personal data; Ease of identification of individuals; Severity of consequences for individuals; Special characteristics of the individual; Special characteristics of the data controller; The number of affected individuals; General points.***

The triage playbook was conceived in the summer of 2017 well before the Guidelines were revised/published in February 2018 and hence the Guidelines have little influence for this research in

¹⁴⁷ The confidence that the reported incident information was encrypted.

terms of the formulation of the triage components and breach notification requirements. However, some of the criteria (those highlighted in **bold**) in the Guidelines have been implemented in the triage playbook. These showed the relevance of the breach indicators, harm entities and parameters as used in the data matrix. It is interesting to see this remark under **General points**: *If in doubt, the controller should err on the side of caution and notify*. On the dashboard, a similar message is displayed on the final prioritisation screen (i.e. Appendix Z, Figure Z- 15 p 276): *Do please notify the individuals as a matter of good business practice. Minimising distress to the affected individuals must be your first priority*.

During a DBI response, the damage or harm was already done i.e. the genie was out of the bottle. The focus of the response then was to minimise further harm by ensuring affected individuals were informed so that appropriate steps could be taken by the individuals. However, there is the issue with breach notification fatigue (Chapter 2) and also the GDPR breach notification requirements. As noted by Callahan (2017) the two-tier EU approach i.e. notification driven by high risk or risk of harm *will likely create confusion* as it *will also likely encourage over-notification to avoid the daunting GDPR fines*. The conflicting requirements raised this prioritising question: *to notify or not?* Hence the *to notify or not* question in the research objective (RO3-1).

Furthermore, in a crisis response (e.g. Chen et al., 2007) such as initial DBI response, where time is of the essence, reliable information is usually not available, and a decision needs to be made under conditions of uncertainty, these constraints were addressed by adopting the principles of triage.

5.2.6 On the breach indicators and data sensitivity

The identification and the quantification of the affected individuals is information that is ascertainable or obtainable (after thorough investigation) as seen by the various reports on data breach revealing the number of customer records compromised e.g. the TalkTalk October 2015 data breach affected 156,959 customers (ICO, 2017). However, the notion of *special* (e.g. GDPR Article 9 and Recital 53) and *sensitive* in the realms of assessing data harm are contextual and not readily quantifiable. Sensitivity of data has been debated and researched (Turn, 1976; Al-Fedaghi, 2007; McCullagh, 2007; Wang and Jiang, 2017) but little is known about what *special* means as in *special categories* of individuals. Al-Fedaghi (2007) points out: *sensitivity is a notion that is hard to pin down as it seems to depend on the context, and this cannot always be captured in a linguistic analysis*. A corollary from this is that the notion of *special* is also hard to pin down. However, it seems perhaps from prior knowledge or experience or intuition or common sense, there are *special* individuals (e.g. children, patients, criminals) who may suffer high harm compared to others or non-special individuals. Take for example, distress - a type of privacy harm, *can we rationalise that a DBI victim who is not a child or a patient will not suffer high distress?* Perhaps this is one explanation for why the UK Courts have recognised distress, without the need to quantify how much distress.

In an empirical study on privacy harm and protecting consumers' privacy online, *users see data security failures as a significant harm* (Reidenberg et al., 2015). Also, the GDPR (Article 32(1)) places the responsibility on the controller and the processor (organisations) to implement appropriate technical and organisational measures to secure personal data. The security measures/protections indicator was reflected in the checklists and in the data matrix for scoring the sensitivity of the data. Only encrypted

digital data was treated as *protected*. Other protection or organisational measures (e.g. privacy policies and/or data or record handling policies or physical locks) for non-digital data must be in place or have been implemented to be considered as protected.

5.2.7 Data matrix

The data matrix is shown in Appendix O p 236. The *entities* are the A and Q columns in the data matrix. The term *entity* is used instead of *indicator* to reflect the nature of the data matrix i.e. it is not a security risk or vulnerability matrix. The term *breach indicator* is used in the context of data breach but not for referring to data harm. As pointed out by Savage (2017) harms have both a risk and an outcome. Hence the data matrix uses data harm entities to derive the risk scores and the outcomes in terms of data impact and impact on individuals. The derived values are shown along E-G and N-P in the data matrix. The PHA approach centered around the concept of data causing harm (e.g. distress) to the individuals as a result of a DBI. The data harming entities are *personal data* (types) and *individuals* (categories) and the *data impact* and *breach impact values* reflect the likely level of distress e.g. high level of data impact signifies or points to the occurrence of distress. The data *sensitivity* and *security* and the *breach* (for individuals) parameters have pre-set values, which were used to score and derive the *data impact* and *breach impact* values. Data impact levels were derived from data sensitivity, volume and security protections/measures. Examples of the scoring levels from Figure O-1, p 236 are shown below (=> means *implied*):

Sensitive => high impact (red/high 'data impact' for high value in 'score').

Not sensitive + low volume + not protected => medium impact (yellow/medium 'data impact' for medium value in 'score').

Not sensitive + high volume + protected => medium impact (yellow/medium 'data impact' for medium value in 'score').

Not sensitive + high volume + not protected => medium impact (yellow/medium 'data impact' for medium value in 'score').

Not sensitive + low volume + protected => low impact (green/low 'data impact' for low value in 'score').

Individual impact levels were derived based on the special category of individual records and the number of records as shown by the examples below:

Special record => high impact (red/high 'breach impact' for high value in 'breach').

Not special record + high number => medium impact (yellow/medium 'breach impact' for medium value in 'breach').

Not special record + low number => low impact (green/low 'breach impact' for low value in 'breach').

ENISA (2012) use similar scoring methods but with extensive lists of indicators primarily for security threats and not focusing on privacy harm to individuals. Best et al. (2017) use information (data) types e.g. credit card, date of birth, diseases, defined at lower level of granularity (or fine-grained) for scoring their privacy risk¹⁴⁸. Another paper uses a scoring method on the sensitivity of the misused/leaked data and the harm to the organisation due to the leaked data (Harel et al., 2010).

¹⁴⁸ Their focus was on *data likely to be found in incident records that cyber subject matter experts reported to be concerning*.

A well-cited privacy scoring method from Liu and Terzi (2010) shows that a user's potential privacy risk due to his or her online information sharing behaviour *can be estimated*. They base their privacy scoring method on two *intuitive* properties or factors from which they formulated the mathematical scoring calculation. They claim that such a scoring system can *estimate the inherent attitude of each individual i.e. a form of psychometric measure*. Their contribution in providing an intuitively and technically driven definition of privacy score is relevant for this privacy harm research. In particular, as regards the *sensitivity of the information being revealed*. In their definition of privacy score, *it needs to satisfy the following intuitive properties: The score increases with (i) the sensitivity of the information being revealed and (ii) the visibility of the revealed information within the network*. In following their claim, the notion of *sensitivity of data being revealed (i.e. unprotected) increases the data harm score* and hence the likely harm to individuals can be estimated and computed.

O'Keefe et al. (2017) in pointing out that *harm might also occur at the individual, organisation or societal level* also recognised that *sensitivity is a key concept which tends to be connected with the potential harm of any privacy breach*.

The data matrix for scoring data harm has the notion of sensitivity of data and the impact of data harm. Based on the sensitivity of the data and the amount of exposed or revealed information i.e. dependent on data volume and security and also information about the individual, the level of data harm and individual impact were scored or derived. These derived data harm values are estimates based on simple intuitive scoring as shown in the data matrix (Figure O- 1 p 236). To align with GDPR Article 33 and 34, the simple *high, medium, low* labels were used to show the likely level of data and individual impact (e.g. in Appendix Z, Figure Z- 15 p 276). These values then enabled decision support in terms of the prioritisation question, *why notify?* as shown against the GDPR requirements (Appendix Z, Figures Z- 16 p 276, Z- 17 p 277).

5.2.7.1 On the data harm entities

The concept of using individual types or records for assessing privacy harm has not appeared in the reviewed literature. However, the ICO has published an Excel template (ICO, 2018a) aimed at organisations for GDPR (CMS LawNow, 2018). In the Excel template it has a column for *Categories of individuals* (e.g. employees) and a column for *Categories of personal data*. Also, organisations process personal data to identify an individual – this is shown in the conceptual model, Figure 5-3 p 113. To identify the individuals, individual types/records or the categories for individuals need to be defined. It is common practise in organisations to hold *employee* records and other individual-related records. For this research, the individual-related records were created at a high-level of granularity. There is little research on individual types in the context of privacy harm unlike research on personal data (Chapter 2).

As regards the use of high, medium and low (e.g. high for more than 100 individual types) for labelling the levels of measurements for the entities, these crude labels have also been used by other researchers (Chen et al., 2007; Oetzel and Spiekermann, 2012; Savage, 2017; Williams et al., 2017). For example, Oetzel and Spiekermann (2012) use low, medium and high to systematically evaluate the degree of protection demand for a privacy target. In terms of data harm as a consequence of a DBI, DBIs are nuanced and potentially with hundreds of victims. However as indicated by the interview study, one DBI victim (F4) suffered emotional distress over a long period of time which affected her quality of life. Hence

in terms of harm to individuals: *how to set a value or scoring for distress?* There is no benchmark data for privacy harm to individuals as a consequence of a DBI. The approach adopted in the data matrix was a heuristically set value of 100 for determining the high or low of affected individuals i.e. beyond 100 was considered as high. Even in the GDPR, *high* to denote a risk level for rights and freedoms of individuals is undefined. ENISA (2013) made *more precise the levels of severity of a data breach* that was originally in ENISA (2012) and introduced two *flags* for the final scoring taking into *account the impact to the individuals*, **it did not consider the categories or types of individuals**. However, one of the flags is for the *number of individuals breached exceeding 100* with this description: *Data of an individual, breached in the context of a bigger incident, can potentially be more easily disclosed, whereas at the same time a high number of affected individuals influences the overall scale of the breach.*

The interview study findings provided the insights to use checklists and to examine data types for privacy harm. Also, interviewees revealed the diverse DBI scenarios (Figures 4-9 p 94; 4-12 p 96) and a multitude of incident frameworks (Figure 4-13 p 97) which gave a rich set of information that underlies the overall design and specification of the data matrix and also the overall specification of the triage playbook. There are no formal descriptions or definitions for data harm i.e. data likely to harm individuals as a consequence of a DBI, unlike indicators of threat or threat indicators or *indicators of compromise* (IOC) (Rowell, 2017). Although there are privacy harm topologies and types of privacy harm (Chapter 2), these are theoretical concepts with little research on operationalising privacy harm in organisational contexts. However, any PHA needs to examine or address the diverse DBI scenarios and the views of the users or organisations on privacy harm, hence the UES with users (RO4).

5.2.7.2 On data privacy harm assessments (PHA)

Following the call by Pollitt (2013) i.e. to seek better sociology paradigms *instead of focusing on the geology and archaeology of computers and on the extraction and interpretation of data in a historical context in the current computing environment*, the concept of data harm assessment was introduced into DBI response for prioritising breach notification.

As discussed in Chapter 2, existing PIAs and DPIAs are not suitable for addressing privacy harm in the context of breach notification during DBI response. Wright et al. (2013) revealed that not all PIAs incorporate *identify risks to individuals*, instead most of the PIAs stressed *identify risks to the organisation*. Moreover, their findings indicated that *PIAs are sometimes not simply the best for risk management*. Instead practitioners have used *data compliance checklist list* and emphasised that the PIA process needs to be *workable* and suggested that an ideal PIA should be a *two-p PIA in the form of an easy and fast checklist*. This recommendation was suggested as the PIA checklist in the ICO PIA Handbook¹⁴⁹ was deemed to be complex with too many initial pre-assessment questions. Also, Wang and Nepali (2015) acknowledged that most approaches for PIA are based on checklists and audits.

Furthermore, vulnerability¹⁵⁰ assessments in security or cybersecurity domains generally covered harm to data (Clarke, 2013), on devices or networks (Williams et al., 2017). Even the privacy

¹⁴⁹ The 2007 PIA Handbook was revised in 2009 and 2014: <https://ico.org.uk/media/about-the-ico/consultations/2047/pia-executive-summary.pdf> [Accessed 20-December-2018].

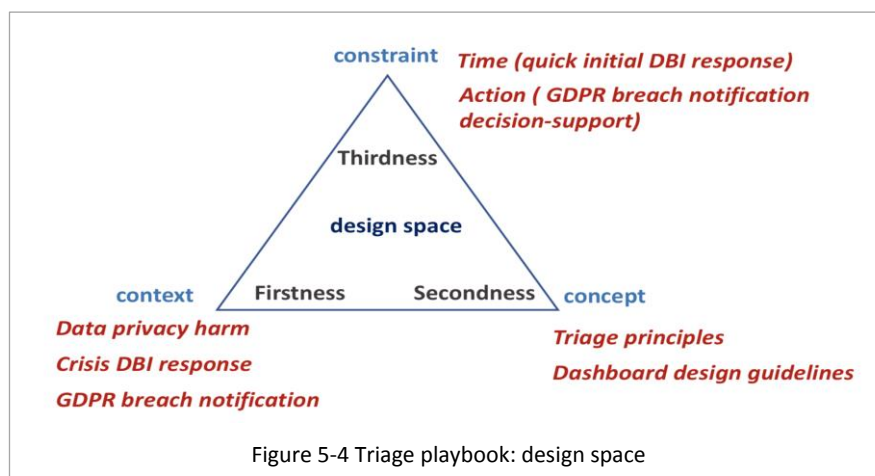
¹⁵⁰ Search on (vulnerability and “privacy harm”) retrieved zero papers on IEEE.org, and 2 papers on Scopus.com [Accessed 9-September-2018].

taxonomies by Massey and Antón (2008) are on vulnerabilities in web-based information systems. Even though the Common Vulnerability Scoring System (CVSS), a public initiative framework, uses contextual scoring with the view to help organisations to prioritise remediation efforts, the vulnerability indicators and assessments are for assessing and quantifying the *impact of software vulnerabilities* (Mell et al., 2006). The PHA approach as specified using the data matrix is different from security or software vulnerability assessments as the focus was for DBI response and data harm to affected individuals.

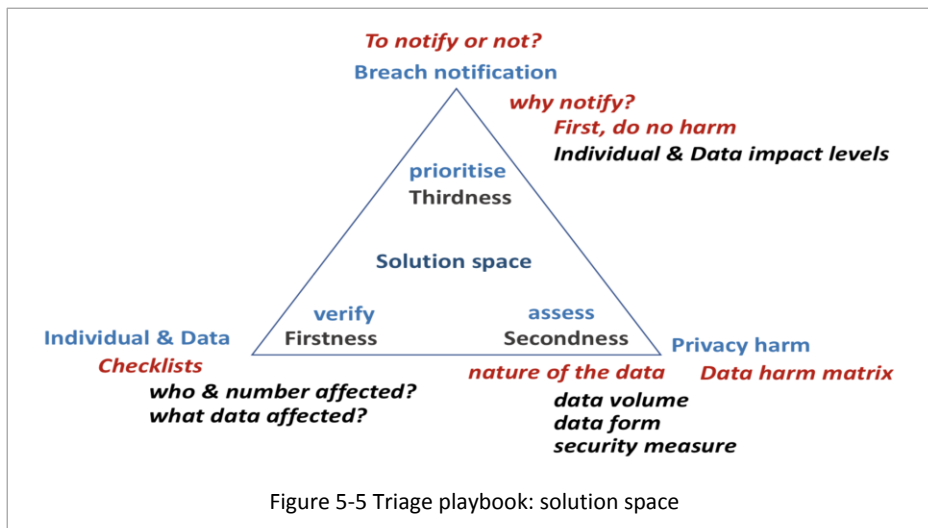
The term *vulnerability* itself has complex interpretation and usage (Hinkel, 2011; Giupponi and Biscaro, 2015) and the use of *indicator* in the context of *vulnerability* also poses challenges (Hinkel, 2011; Doorn, 2017). In referencing others, Doorn (2017) noted that *indicators* have been criticised for *their narrow focus on quantifiable effects*. Hinkel (2011) uses the terms, *entity* and *variable* in the discussion on *measurement and indicators*, and the need to distinguish *harm indicators* and *vulnerability indicators*. Hinkel (2011) provides this: *Harm indicators are indicators that evaluate a state of an entity based on normative judgements of what constitutes a good or bad state. These indicators do not include the forward-looking aspect. Vulnerability indicators are indicators of possible future harm. These indicators include both the forward-looking aspect as well as the normative aspect of defining harm*. Hence existing DPIAs, PIAs or security risks assessment methods that are driven by vulnerability indicators are not suitable for assessing the damage or harm to the data subject as raised by Article 29 Working Party (2018). Based on Hinkel's (2011) indicators¹⁵¹, the data matrix provides a set of data harm entities for assessing privacy harm in a specific context i.e. during DBI response.

5.3 Dashboard design

The design and solution space are visually illustrated using Peirce semiotics-ternary as shown in Figure 5-4 p 121 and Figure 5-5 p 122. From the conceptual triage model and the identified needs and requirements from the SSM and interview study, a rough tentative conceptual design was produced as shown in Appendix P, Figure P- 1 p 237. To implement some of the design concepts, Dr Ludi Price kindly produced individual icons from the tentative icons as shown in Figure P- 2 p 238. This researcher then consolidated the individual icons into two designs as shown in Figure P- 3 p 239. Developer2 implemented the design into the dashboard.



¹⁵¹ The author also states the deductive, inductive, normative substantive arguments for developing vulnerability indicators.



5.3.1 Why a visual dashboard?

The idea of using a visual dashboard was inspired by the appearance of *dashboard* as pragmatic tools under business intelligence, decision-support and various performance analysis and monitoring systems. Furthermore, at the *InfoSec2017* in London¹⁵², dashboards were used for security monitoring and also for GDPR related applications.

Researchers have used dashboard for triage in mass casualty disaster (Vassell et al., 2016) and in security incident domains (Bharosa et al., 2010; Haim et al., 2017). In the privacy design space, although not related to privacy harm or DBI response, Karunakaran et al. (2017) designed a *Privacy-Dashboard* for consumers to control their privacy settings and revealed the need to *design theoretically based IS artifacts that can be used for privacy protection*. Their design is based on the privacy scoring methods by Liu and Terzi (2010). Karunakaran et al. (2017) did not provide a visual diagram or a detailed description of their design approach, but they reported that when shown in the dashboard format and offered in a collated form, *all the participants expressed interest to read privacy policy and would use the controls to protect their privacy*.

Few (2006, p 34) describes: *A dashboard is a visual display of the most important information needed to achieve one or more objectives, consolidated and arranged on a single screen so the information can be monitored at a glance*. Yigitbasioglu and Velcu (2012) describe a dashboard as: *A graphical user interface that contains measures of business performance to enable managerial decision-making*. Yigitbasioglu and Velcu (2012) also reported that there is no standard definition of dashboards in the available literature. They pointed out that there is no agreement over how exactly a dashboard should look and what it should do.

Despite the availability of extant literature regarding benefits, design and implementation of performance dashboards, little is known about the extent to which these can enhance the visibility of information to different users and across managerial levels. In addition, most of the literature is fragmented as it reports the use of different types of dashboards, namely strategic, tactical and operational, as separate tools (Pace and Buttigieg, 2017).

¹⁵² <http://www.infosecurityeurope.com/Conference/> [Accessed 29-December-2018].

5.3.2 Dashboard design aim

Although the design aim was not to address users' interaction behaviour but to construct a visual dashboard to meet the dashboard requirements, visual design principles and dashboard best practices/guidelines were explored and are discussed in Section 5.3.3. The interview study informed the overall design of the dashboard in that: triage is used for actionable outcomes; checklists are used for gathering of breach information to assess the nature of the breach; data types are suggested as indicators of harm to affected individuals, and DBI response requires a crisis response i.e. speedy response with minimal information.

5.3.2.1 Functional design level

At the functional design level, the dashboard implemented the triage sequence of steps to verify, assess, prioritise using the checklists of questions and answers and the data matrix to systematically, accurately and quickly perform the response steps and derive the data impact and individual impact levels. Here the checklist is a *Do-Confirm* type whereby users *DO their jobs from memory and experience, often separately. They stop and pause to run the checklist and Confirm that everything that was supposed to be done was done* (Gawande, 2011, p 123). Another type is a *Read-Do* checklist where tasks are done and checked off (like a recipe) (Gawande, 2011, p 123). Reijers et al. (2017) conducted a comprehensive literature review on checklists and adopted the description for checklist by Hales and Pronovost (2006): *A checklist is typically a list of action items or criteria arranged in a systematic manner, allowing the user to record the presence/absence of the individual items listed to ensure that all are considered or completed.* This checklist description closely describes the nature of checklists used in the triage dashboard.

5.3.2.2 Operational design features

The dashboard operational features provided incident capture/recording, auditing/checking and tracking/monitoring tools. The overall aim of these operational features was to ensure notification to affected individuals can be assessed in a speedy manner, and to be compliant with the GDPR notification requirements. In essence the dashboard steered the organisations towards addressing privacy harm to affected individuals and breach notification during DBI response. As described by Pace and Buttigieg (2017), dashboard features give *users greater visibility and integration of information regarding the performance of the organisation, by collecting relevant data in a timely fashion. In the same manner that a pilot uses the display of indicators in the cockpit to monitor and navigate a plane, dashboards provide relevant information to users to steer an organisation.* These features need to be implemented such that users can intuitively access the information easily. The information needs to be simplified and readily available for users to act proactively (Pace and Buttigieg, 2017, Tan et al., 2017). In term of dashboard types i.e. the features, aim and use, the triage dashboard falls under operational and strategic categories as described in Rasmussen et al. (2009).

5.3.3 Dashboard design guidelines

Some features emerged as *universal visual* design features i.e. visual perception principles that need to be in place in any case unlike functional design features of the dashboard. These are dependent on the (i) purpose of the dashboard, (ii) tasks, (iii) knowledge, and (iv) personality of the user (Yigitbasioglu

and Velcu, 2012). The visual perception principles concern four aspects of dashboard design: colour, form, spatial position and motion (Ware, 2012; Yigitbasioglu and Velcu, 2012).

In terms of highlighting of exceptions, Ware (2012) and Santiago Rivera and Shanks (2015) suggest the use of different display types, better use of icons and colour to improve recognition of the exceptions. Although the dashboards should be concise, simple, and intuitive to use, the features need to be in line with their purpose(s) so that functional fit is attained (Yigitbasioglu and Velcu, 2012). According to Ines et al. (2017) presenting a wrong visual graphic or providing a sophisticated type of visualisation to a beginner viewer, for example, may lead to wrong data interpretation. Hence the choice of a visual form – using familiar visual components – those that are easily understood by users and should represent information in a meaningful way.

The triage design principles (i.e. primarily ethics driven) and concepts for response crisis as indicated by interviewees (i.e. speedy response with minimal information) influenced the overall design of the dashboard. In particular, the *intuitive* aspects of triage and DBI response as described by interviewees (Sections 4.5.2, 4.8.1, 4.8.2) provided the overall underlying design aim of the dashboard. To address the triage principles in terms of the use of appropriate symbols/signs, the triage colours i.e. red for high, yellow for medium and green for low impact are based on the triage categories outlined by Kennedy et al. (1996). The triage colours and their significance are: *red indicates priority one (i.e. the need for immediate care); yellow indicates priority two (i.e. may be delayed for a limited period of time without significant mortality); green indicates priority three (i.e. may be delayed until the patients in the other categories have been dealt with)* (Kennedy et al., 1996).

From the reviewed literature, there was no convincing specific, simple and practical guideline or approaches to design a simple, functional visual dashboard (i.e. low-fidelity) for the triage playbook. This led to the adoption of a combination of practical design guidelines. In particular a good practice on *What makes an effective dashboard?* (Sisense, 2017) was extracted, shown in Figure P- 4 p 239. The recommended guidelines by Ines et al. (2017) on the overall layout for dashboards are shown in Appendix Q p 240. Their research introduced a conceptual model for a dashboard generator process and proposed key components (user, data and visualisation) as shown in Figure Q- 1 p 240. Their dashboard structure, as shown in Figure Q- 2 p 240, was extracted for D&B discussion with Developer1. In terms of data analytics, Humphries (2015) summarised these basic dashboard features/advantages: *The ability to display multiple data sources on the same dashboard, whereas Excel can pull from only one at a time; Alerting capabilities that allow end users to receive texts and/or emails when certain thresholds are met; Real-time connectivity to data sources, so information is pulled much faster and is more accurate; The capacity to allow multiple charts and graphs, including maps and even facility floor plans, to be incorporated into a specific dashboard.* However, the eventual design and *look and feel* of the final delivered dashboard was driven by the D&B with developers¹⁵³ as discussed next.

¹⁵³ It was truly a rapid D&B with Developer2 due to the slipped schedules with Developer1 which affected the overall intended aim of the design of the dashboard. However, the functional aspects were designed into the dashboard.

5.4 Design and Build (D&B) with developers

The developers (i.e. Developer1 and Developer2) were instructed to build a standalone (i.e. client/desktop based) dashboard using free or open-source tools/software and for MacBook environment. The D&B started off with a developer (Developer1) from a company, this stopped after the first delivery of a dashboard. The dashboard did not meet the requirements. The initial discussion with Developer1 is shown in Appendix S, Figure S- 1 p 242. The mockups as shown in Appendix R p 241, were done with Developer1 and then used with another developer (Developer2) from upwork.com to deliver two dashboards for the UES. Appendix S, Figure S- 2 p 243 shows the job specifications and the job details posted on upwork.com. The initial email with Developer2 is in Figure S- 3 p 244.

As shown in Figure 3-13 p 80 the prototyping activities were separated to show those that were done by this researcher (Researcher) and those that involved the developers (Developer). The initial screen mockups (Modeling and quick design) were done with Developer1. The Researcher aimed for regular communication (Feedback) with the Developer. This was a challenge in terms of available resources and commitments from the Developer. For example, communications and interactions with Developer1 were limited to once a fortnight due to his work commitments. Also, Developer1 was unable to commit to further work after the first delivery. Hence another developer i.e. Developer2 was sourced to continue with the D&B. With Developer2, communications were more frequent, driven by the fixed priced and timescales to complete the job. The biggest challenge with Developer2 was having to describe every requirement to him (not heard of GDPR and not in the security domain) and we spent a lot of time discussing the data matrix and how to code and test the logic and also the 72 hours counting down for the notification alert. This researcher's background in software analysis and development provided the necessary skills and experience to successfully work with Developer2.

A summary of the iterations with Developer2 are listed in the following sections.

5.4.1 Iteration 1: DashboardV1

In summary, the activities were:

- (1) DashboardV1 build completed and tested by Researcher and a PhD student;
- (2) Conducted a pilot with a user (a practitioner with the relevant background);
- (3) Rapid analysis of the pilot results (Researcher);
- (4) Communicated feedback to Developer2 for changes;
- (5) Verified the revised DashboardV1 before start of iteration 1 with Group1 users (Researcher);
- (6) UES with Group1 users.

Snapshots of DashboardV1 screenshots are shown in Appendix T p 245.

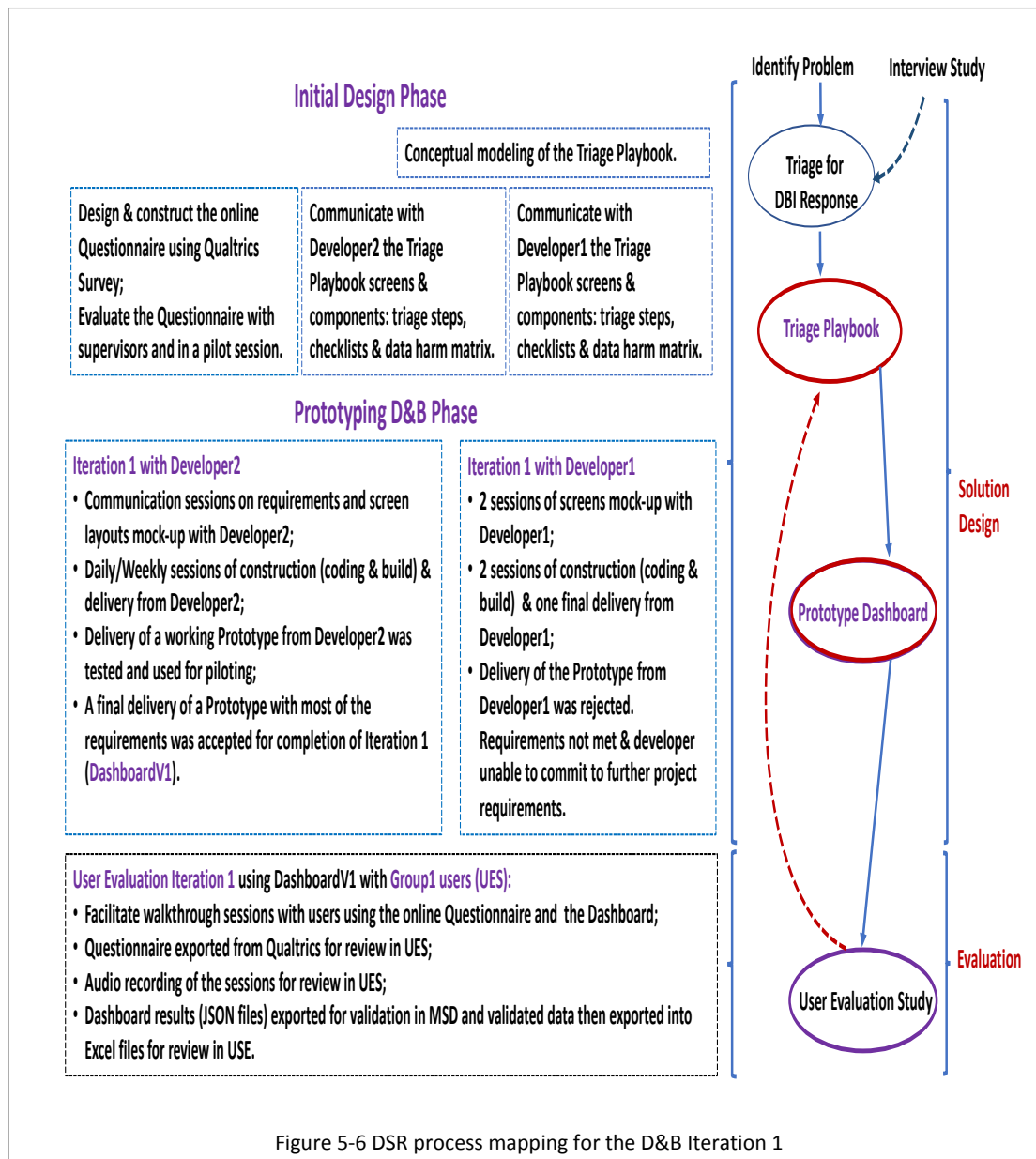
5.4.2 Iteration 2: DashboardV2

In summary, the activities were:

- (1) Rapid analysis of the iteration1 results (DashboardV1 with Group1 users);
- (2) Communicated feedback to Developer2 for the required changes;
- (3) DashboardV2 build completed and tested by Researcher;
- (4) UES with Group2 users.

Snapshots of DashboardV2 screenshots are shown in Appendix U p 254.

Details of the iterations and the D&B activities with the Developer (Developer1 and Developer2) were mapped into the DSR processes (Figure 3-8 p 75) and shown in Figure 5-6 p 126 and Figure 5-7 p 127.



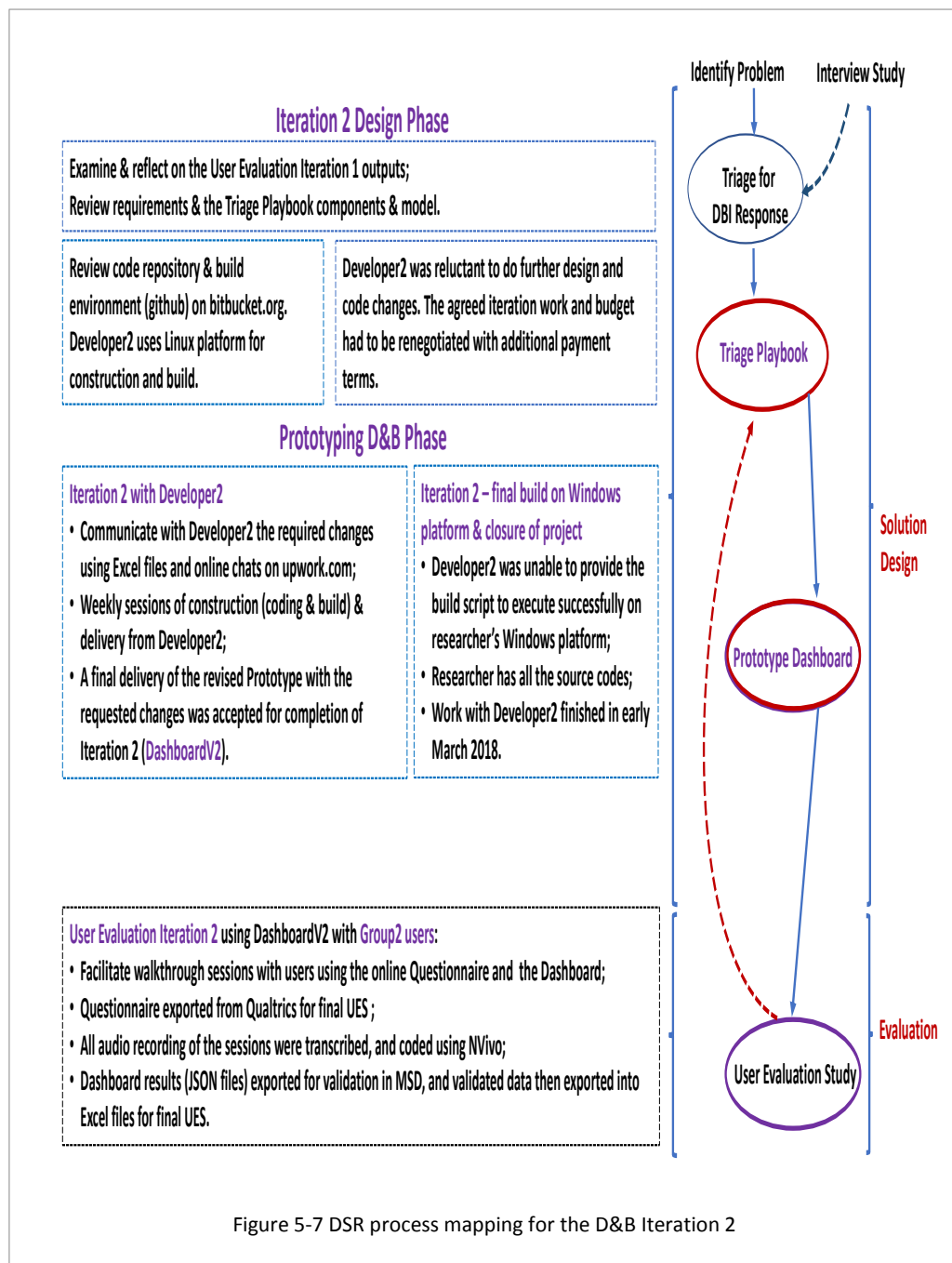


Figure 5-7 DSR process mapping for the D&B Iteration 2

Chapter 6 User Evaluation Study (UES)

This chapter describes the evaluation with industry practitioners (**Users**) of the two prototype dashboards i.e. DashboardV1 and DashboardV2 (**Dashboard**) that were designed, built and tested/validated (Chapter 5). As shown in Figure 3-12 p 80, there were two user evaluation studies (**UES**) i.e. DashboardV1 with Group1 Users and DashboardV2 with Group2 Users (**Users**). The UES objective and questions (Figure 6-1 p 129)¹⁵⁴ were framed to address the research aim and research question.

As discussed in Chapter 3, evaluation is a key activity in DSR and iterative evaluation with users (*action-practical-feedback* in Section 3.4) was conducted to ensure rigor and relevance (Section 3.3.1) of the triage playbook. Evaluation is considered a defining feature in DSR (McLaren and Buijs, 2011) and is a central and essential activity in conducting rigorous DSR (Venable et al., 2012). Venable et al. (2012) state that a key purpose of DSR evaluation is to *determine whether or how well the developed artefact being evaluated achieves its purpose*. Furthermore, McLaren and Buijs (2011), Gonzalez (2009) and Johannesson and Perjons (2014) in concord with Hevner et al. (2004) stressed that evaluation of a new IS artefact (or instrument) should not merely capture how valid or reliable it is. Instead they argue that emphasis is needed on the practical utility of an instrument to produce more actionable research outputs that can be readily corroborated, thus improving the quality and usefulness of the research findings. This is achieved by use of multi-method user evaluation study (UES). It was multi-method as the UES involved multiple methods for data collection and data analysis. The data collection was a face-to-face, audio recorded and facilitated walkthrough with the Users (**Walkthrough**). During the Walkthrough, an online questionnaire designed using Qualtrics (**Questionnaire**) was used alongside the Dashboard. Data preparation and synthesis were done during data analysis (Section 6.4) which created the UES datasets (Figure 6-4 p 138). The UES datasets were examined and the findings are discussed in Sections 6.5 to 6.9. Besides reporting the mostly structured qualitative Questionnaire results, a storytelling approach was used to examine and describe the DBI scenarios captured during the Walkthrough.

6.1 UES objective and questions

To meet the UES objective (RO4) and to address the RA, the Dashboard needs to *show how it is able to support the solution to the problem* (Shukor et al., 2017). This calls for the use of multi-method evaluation to answer the UES questions as listed in Figure 6-1 p 129.

According to Cleven et al. (2009) the term evaluation is complex, used in variety of application areas and it is difficult to clearly delineate the term. Hence the term validation is used in RO4 to include the evaluation¹⁵⁵ with Users and also the micro-evaluation during the D&B iterations with Developer1.

¹⁵⁴ The Q stands for the question number in the Questionnaire.

¹⁵⁵ The term *demonstrated* is also used by DSR researchers in the discussion on DSR evaluation. For example, Venable et al. (2012) in referencing others: *demonstration is like a light-weight evaluation to demonstrate that the artifact feasibly works to solve one or more instances of the problem, i.e. to achieve its purpose in at least one context*. Validation to include demonstration.

UES Objective
(RO4) To validate the triage playbook using a prototype dashboard (Dashboard).
Questions
(RO4-a) How useful is the triage sequence of steps for initial DBI response? (Q19, Q20) (RO4-b) How useful is the triage sequence of steps for PHA? (Q21) (RO4-c) How useful are the checklists for PHA? (Q22, Q23, Q24, Q25) (RO4-d) How useful is the Dashboard for PHA? (Q26) (RO4-e) How useful is the Dashboard for prioritising breach notification during initial DBI response? (Q27, Q29) (RO4-f) How useful are the notification alerts? (Q28) (RO4-g) What are users' views on the impact of the Dashboard on their initial DBI response? (Q30) - Gathering of information (Q30a) - Internal communication during the response (Q30b) - Recording the incident response actions (Q30c) (RO4-h) What are users' views/suggestions for improvement? (Q31) (RO4-i) What are users' viewpoints during the closing of the user evaluation study? (Q32) What did the UES reveal?

Figure 6-1 UES objective and questions

6.2 Justification for the multi-method UES approach

The guided DSR, multi-method UES approach involved facilitated, walkthrough face-to-face interactions with users, the use of questionnaire, prototype dashboard and audio recording. Figure 6-2 p 131 and Figure 6-4 p 138 show the various data capture methods and tools.

6.2.1 On multi-method evaluation

McLaren and Buijs (2011) and Shukor et al. (2017) promote multi-method evaluation. According to McLaren and Buijs (2011) a multi-method evaluation approach is needed in order to produce valid and useful evaluation results. They also adopted DSR and used iterative development and multi-method evaluation – involving questionnaire and prototyping but not a dashboard – of their intelligent products system. Multi-method evaluation approaches in DSR, involving walkthrough of the questionnaire and dashboard prototyping for proof-of-concept or proof-of-use (usability or utility) of data harm assessment for breach notification during DBI response, appear to represent a novel research approach. For example, Sandner et al. (2010), Hoyer et al. (2012), and Baur (2017), discussed prototype dashboard and used DSR but these are not on privacy, breach notification or DBI response related studies.

6.2.2 Dashboard for prototyping and walkthrough with users

Prototyping was used as a proof-of-concept or proof-of-use to demonstrate feasibility, utility or practicality and to illustrate the significant triage playbook components as implemented in the Dashboard. A prototype dashboard is a tangible system for which users can experience and critique, and the system builder/designer gets users' responses based upon that experience (Naumann and Jenkins 1982). This is often the only really effective method for gathering feedback from users about *what is good and what is bad about an idea* (Omar, 2014). Furthermore, for prototyping to be effective, it requires interactions between the user, builder, and system (Naumann and Jenkins, 1982). Hence face-to-face walkthrough with users was used and the RITE approach which espouses iterative gathering of feedback (Chapter 3), further enhanced the overall effectiveness of the prototyping.

Prototyping evaluation approaches have been discussed by DSR researchers e.g. for proof-of-concept to show feasibility or utility (Nunamaker et al., 1990; Peffers et al., 2012; Yigitbasioglu and Velcu, 2012; Gregor and Hevner, 2013) and to demonstrate design principles (Santiago Rivera and Shanks, 2015; livari et al., 2018). Numerous non-DSR works have used prototyping using dashboard for privacy/security related – but not DBI response or breach notification – studies (e.g. Pearson and Allison, 2009; Parkin and Epili, 2015; Monika et al., 2017). Bharosa et al. (2010) highlighted that there is a dearth of research on the development and use of dashboards for disaster preparation and they then used an action research approach for designing their prototype dashboard.

The UES evaluation was naturalistic as it was conducted in real settings using a real, i.e. working, concrete prototype system with multiple stakeholders to solve real problems (Johannesson and Perjons, 2014, p 138-139). They pointed out that naturalistic evaluations are suited for investigating effectiveness of the artefact and for studying the impacts of the use of the artefact. As the research phenomena touches on sensitive topics i.e. DBI and breach notification, such data are not publicly available and little research in these topics, hence a naturalistic UES provided the means to gather diverse users' views and data. A naturalistic evaluation has high external validity unlike an artificial¹⁵⁶ evaluation, but internal validity may be compromised in a naturalistic setting (Johannesson and Perjons, 2014).

6.2.3 Questionnaire design and use

The overall goal of the questionnaire was to achieve the UES objective and RA. The UES objective provided the basis for the designing of the questionnaire (Lavrakas, 2008). The use of questionnaires: *ensures the meaning of the questions is shared by the respondents; the respondents understand the objectives under investigation in roughly the same way; and provide comparisons of the responses* (Lepmets et al., 2014).

The Questionnaire was online and consisted of two parts i.e. pre-Dashboard and post-Dashboard as shown in Appendix V p 260. The Questionnaire was designed such that it can be paused or stopped during the Walkthrough. This allowed the user to pause and use the dashboard before continuing with the post-Dashboard questions in the Questionnaire. The evaluation of the Dashboard starts after Q18 and after completion of the Dashboard. To capture the description and the nature or type of DBI, Q11 provides 3 types of DBI response scenarios for Users to choose one scenario and the description captured in Q12. Users were briefed at this point that their selected scenario was then used for the rest of the Questionnaire and also for use in the Dashboard. In the Dashboard, Users were also required to input a short description of the scenario. Some questions e.g. Q15 and Q17 automatically skip or direct the user to the next question depending on the user's input (i.e. contingency or filter type questions). Likert-style scales, i.e. the traditional 5-point scales, were used for the factual and/or closed questions. Although not in the same IS research field, Garratt et al. (2011) revealed that there is preference for the use of 5-point scales to longer scales. This view was also expressed by a user¹⁵⁷ during the Walkthrough.

¹⁵⁶ An artificial evaluation means that the artefact is evaluated in a contrived and artificial setting, e.g. in a laboratory (Johannesson and Perjons, 2014).

¹⁵⁷ f1 preferred 4 points instead of the 5 points.

There are also open questions and free form text fields for Users to input their views/comments. The Users were guided or facilitated during the Walkthrough and all the questions required user input (i.e. *forced response*). This ensures no missing questionnaire responses¹⁵⁸. According to Lavrakas (2008) *forced response* may result in the collection of erroneous data as some respondents may not know how they feel about the issue or may not have the requested information. To avoid this, non-factual or non-statement type questions have the *don't know* option in the answer sets. Also, although the questionnaire is online it is not self-administered (except for one user in Group1¹⁵⁹). Users were given the opportunity to express their views during the Walkthrough, and the audio recorded Walkthroughs were also analysed. After the 4th user in UES Group1, the word *internal*¹⁶⁰ was added to *communication* for clarity. The same set of questions in the Questionnaire was used for both groups of users in the two UES i.e. Group1 and Group2. Figure 6-2 p 131 shows the high-level categories of the questions in the pre-Dashboard Questionnaire, content of the Dashboard and the questions in the post-Dashboard Questionnaire.

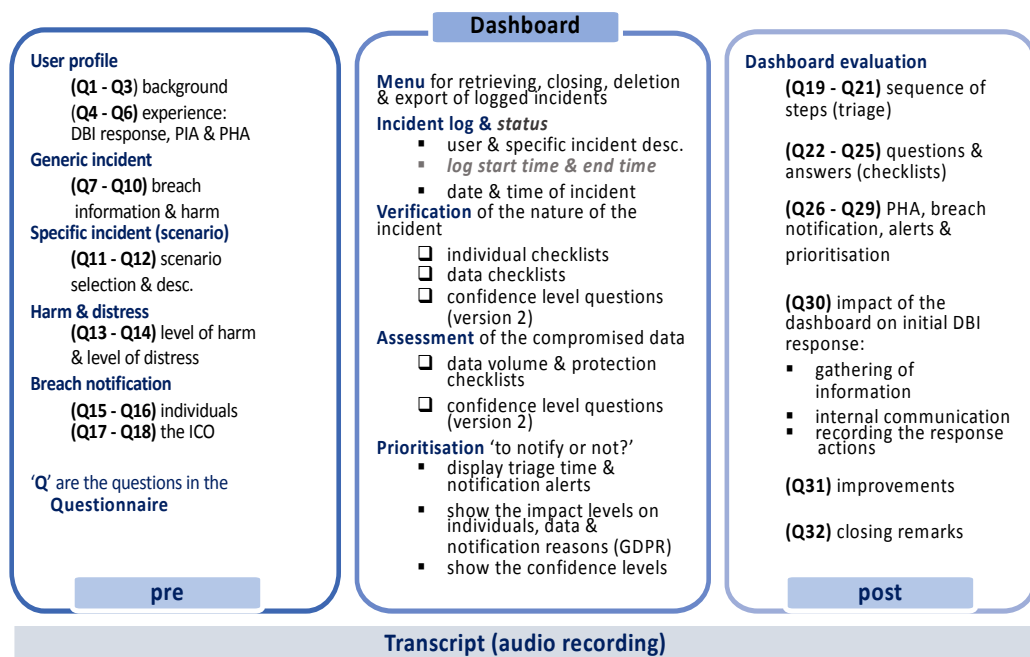


Figure 6-2 Summary view of UES Questionnaire & Dashboard

6.2.4 Walkthrough techniques

Various walkthrough¹⁶¹ techniques have been used/developed by software/system developers and researchers (e.g. Bias and Mayhew, 2005; Lottridge and Mackay, 2009; Mourouzis et al., 2011; Chari et al., 2013; Lepmets et al., 2014; Moore and Likarish, 2015; Parkin and Epili, 2015; Light et al., 2016;

¹⁵⁸ Somehow Q10 was not displayed by Qualtrics. Users f1, e2, o4 were contacted by email to get their answers. Their answers were input into Qualtrics by this researcher. Subsequently, a refresh was done to ensure all questions were shown by Qualtrics.

¹⁵⁹ b3 downloaded the Dashboard (a set of instructions was emailed to him) and he completed the Questionnaire without any assistance. He requested this mode of participation as he was traveling outside UK.

¹⁶⁰ Communication in Q10 can mean *external* communication. This was pointed out by o4. Communication was replaced with *Internal* communication.

¹⁶¹ For example, heuristic evaluations or walkthrough, cognitive walkthrough, generative walkthrough, socio-technical walkthrough, code and design walkthrough.

Shukor et al., 2017). In examining¹⁶² these walkthrough techniques, they appear to have these characteristics: are facilitated using a medium (system/actor/agent); involve some systematic or structured or organised processes or tasks or steps, and generally goal/aim driven (e.g. to test, or to evaluate or to examine or to diagnose or to study etc.).

As noted by Lottridge and Mackay (2009), both structured (code) walkthroughs and design walkthroughs involve *a systematic, step-by-step look at an artifact, with the goal of identifying as many problems (include viewpoints) as possible*. Chari et al. (2013) and Parkin and Epili (2015), both in the security context and non DSR, discuss walkthrough using prototype and dashboard.

For the UES, this researcher acted as a facilitator to guide the users in using the Questionnaire and the Dashboard by walking through the tasks i.e. resembling a task or step-driven walkthrough. Chari et al. (2013) and Light et al. (2016) mention task/step walkthrough. Chari et al. (2013) provide a demonstration that walks through a prototype dashboard system but appear not to involve users for evaluating the system. Light et al. (2016) develop – in discussion with their colleague and from literature – a step-by-step technical walkthrough technique for researchers to perform a critical analysis of a given application. Their claim is that the step-by-step walkthrough technique *is a way of engaging directly with an app's interface to examine its technological mechanisms and embedded cultural references to understand how it guides users and shapes their experiences*. However, the authors pointed out that the walkthrough method only serves as foundation methods with limitations – mainly the lack of interaction with application users¹⁶³. They suggested it requires a combination of the walkthrough method with content analysis or interviews to gain further insights. Hence this UES used facilitated, face-to-face, recorded walkthrough with users to evaluate the Dashboard using Questionnaire to capture a rich dataset of users' insights.

The values of using facilitated, face-to-face walkthrough with users are: the internal validity issues can be minimised as users are briefed on and guided to focus on the objective of the UES; consistency and reliability of the users' responses as the walkthrough process is systematic and interactive tasks-driven; and support rapport, building trust for safety and openness which enhance the quality of users' responses. According to McDermott (2011) *well-designed experiments with strong control, careful design, and systematic measurement go a long way toward alleviating concerns on internal validity*.

The associated challenges are: getting dedicated time from busy executives or senior managers proved to be difficult; resource intensive for planning, organising and executing the Walkthrough; and also, various types of data to sort, analyse, integrate and synthesise.

6.3 UES Walkthrough with Users

The steps used for facilitating the UES Walkthrough techniques:

- (a) Preliminary step to check and get the User's consent;
- (b) Briefing the Users on: the facilitator's role (this researcher); aim of the Walkthrough; format of the Walkthrough;

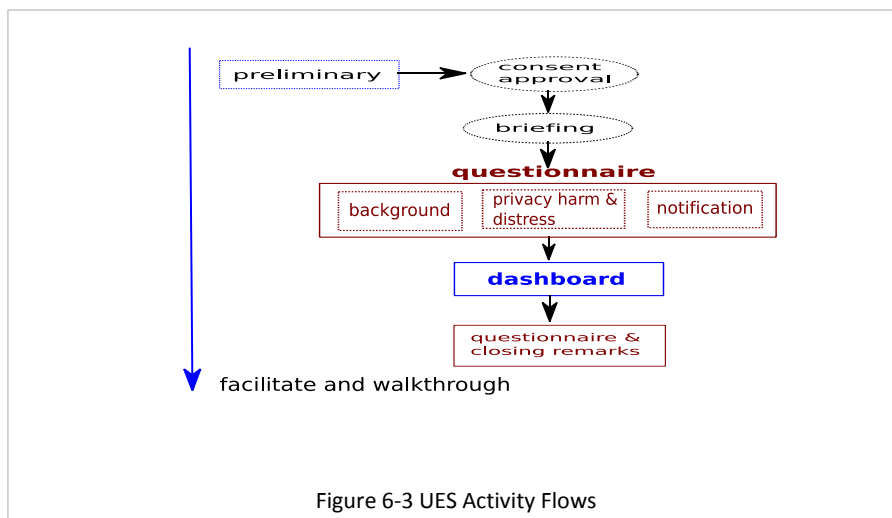
¹⁶² These papers have *walkthrough* and related search terms (i.e. facilitate, DSR, prototype, dashboard, security, response, incident or privacy) retrieved during second literature review.

¹⁶³ Their walkthrough does not directly collect and analyse user content, activity or attitudes (Light et al., 2016).

- (c) Helping users by guiding or facilitating them through the Questionnaire and the Dashboard and to re-assure them that any personal or sensitive material will remain private and confidential;
- (d) To be present to answer any queries or sort out any technical hitches with running the online Questionnaire and with using the standalone Dashboard; and
- (e) To ensure the audio recorded Walkthrough are conducted smoothly within the specified allocated one hour.

Unger and Nunnally (2013), provide a guideline for all facilitation under these headings: *sensitivity; leadership; preparation; a sense of humor; and sneakiness.*

Most of the Walkthroughs¹⁶⁴ were done in private rooms at Users' Offices/locations, or at City, University of London. Although the standalone Dashboard does not require internet access, the online Questionnaire does. The format and activities are shown in Figure 6-3 p 133.



After the User signed the consent forms, a short briefing was given on the format, aim of the Walkthrough and that he/she will be guided to use the Questionnaire and the Dashboard. As part of the rapport building, the briefing and the Walkthrough was done as informally (without reading a script and no taking of notes) as possible for opportunities to engage, build rapport and manage the User's expectations.

Two snapshots i.e. one from Group1(f8) and one from Group2(c10)¹⁶⁵ of the briefing were extracted from the transcribed files and shown in Appendix Y p 267. Figure 6-2 p 131, shows the questions (Q) in the Questionnaire and the Dashboard. The high-level Questionnaire sequences are:

- (1) Background & experience;
- (2) Views on privacy harm & breach notification;
- (3) Personal data incident scenario selection;
- (4) Questionnaire on harm & distress to affected individuals;

¹⁶⁴ Users: h5 (public library-no recording done); b11 (open plan meeting room-recording not too good); f17 (coffee shop-poor quality recording). These Users selected these venues due to their own work/personal situations. During the Walkthrough with c6, there was no internet access and an iPad with a keyboard was used to run an offline version of the Questionnaire (Qualtrics provide an offline version only for iPads or mobile handsets).

¹⁶⁵ f8 also participated in the interview study. c10 was recruited at a GDPR event, and was briefed about the study, so the UES briefing was shortened.

- (5) Questionnaire on incident notifications;
- (6) Pause the Questionnaire and use the Dashboard for the selected incident scenario;
- (7) Questionnaire on the Dashboard and impact of the Dashboard;
- (8) Closing remarks.

Apart from the Walkthrough with c6¹⁶⁶ where there were two users i.e. c6/K, c6/P, all the other UES Walkthroughs were with one user. During the Walkthrough with c6, c6/K did the data input and typing based on their answers to the questions. To run the Walkthrough, this researcher sat between c6/K and c6/P, and read aloud the questions from the screens (Questionnaire and Dashboard) for both the users. This Walkthrough showed the flexibility of the Walkthrough technique to gather users' viewpoints without compromising the nature and quality of the UES. Light et al. (2016) in inviting researchers to apply the walkthrough with other methods also said to apply the walkthrough flexibly. As the main focus of the UES was not to examine user's interaction behaviour with the Dashboard, the screen recordings¹⁶⁷ were not examined.

Unlike the Questionnaire where one version was used for both groups of UES, the Dashboard has two versions, DashboardV1 and DashboardV2. The Walkthrough was the same for both groups and as DashboardV2 has new checklists questions, the UES datasets consist of Group1 UES and Group2 UES data. To show some of the screenshots used during the Walkthrough, and the new checklists questions (confidence levels) in DashboardV2, some of the screens were extracted from the screen recordings for users¹⁶⁸, i.e. g7 in Group1 and l14 in Group2. The screenshots are shown in Appendix Z p 269 and AA p 281. Some notable remarks by Users during the Walkthroughs are also mentioned in Sections 6.3.2 to 6.3.4.

6.3.1 Preparation and user selection

Before execution of the Walkthrough, similar interview study preparation, planning and recruitment of users were done. A participant/user note and a consent form (submitted as part of the CSREC ethics application) are shown in Appendix W p 264. These were emailed to potential candidates who have expressed interest in taking part in the UES. The criteria for selecting users and a sample email invitation are shown in Appendix X p 266.

Faced with similar challenges with interviewee recruitment, interviewees with responsibilities for DBI response or managing DBI response or have experienced DBIs or have roles/titles related to data compliance or governance (e.g. Data Protection Officer) were invited to participate in the UES. In total eight users took part in Group1 UES and another set of nine users in the Group2 UES. These users with diverse roles/titles and experiences were from various industry sectors (Users). The final sampling sizes for both the groups were based on pragmatic resource consideration to achieve the objective of UES and

¹⁶⁶ c6/K was the new DPO manager (from a non-charity sector) in charge of c6/P who took part in the interview study.

¹⁶⁷ QuickTime (on MacBook) was used to record the screens. In some Walkthrough sessions the recordings were not done from start to the end or not done. The focus was on the audio recordings and the Questionnaire and Dashboard Walkthroughs.

¹⁶⁸ g7 and l14 were used as both screen recordings were done. g7 was paper-based and was a criminal investigation case, and l14 was the only legal user and digital-based and the longest triage time – nine mins in Group2.

the RA. The interview study discussions on purposeful sampling and sampling sizes (Section 4.1.2) are relevant for the UES.

The UES Walkthrough occurred between 10 January 2018 and 12 March 2018. The Users' profiles are discussed in Section 6.5.1. The interview study methods for pseudonymisation of the data and file naming conventions were also adopted for the UES. For example, the first UES with a user from the finance sector on 10 January 2018 has the following coding and data files:

- UES User profile: f1 (lower case)
- transcribed file: 10january2018-1
- recorded audio file: 10jan2018-f1

The UES Users' profiles are shown in Figure 6-11 p 144. On one occasion during Group1 Walkthrough, vetting of a candidate for suitability i.e. has the relevant experience or responsibility or role/title was not done thoroughly before the Walkthrough. It turned out that the candidate was interested to find out about the dashboard solution for his own business development. Subsequently, another business owner of a privacy solution/service provider company also had similar intentions. Based on these two experiences, this researcher then realised that the developed Dashboard has business value (due to the GDPR), and candidates were screened¹⁶⁹ before being invited to take part in the UES.

6.3.2 Pre-Dashboard

Upon completion of the briefing, the User starts to use the Questionnaire. The User selects a DBI scenario i.e. to respond to a hypothetical data incident or to respond to a data incident that she/he has had experience in, or to conduct a data incident response as part of a pre-incident response planning exercise. The chosen scenario was captured in the Questionnaire (Q11-Q12). The User was also informed that a brief description of the scenario is also input on the Dashboard and also, for the remainder of the Walkthrough. Users' views/actions on harm, distress and breach notification were also captured before the use of the Dashboard (Q13-Q18) (Figure 6-2 p 131), hence pre-Dashboard.

Snapshots of the pre-Dashboard screens are shown in Appendix Z, Figures Z- 1 p 269 to Z- 6 p 271. At Figure Z- 7 p 272, the Users were directed to the Dashboard.

6.3.3 Dashboard

On the welcome screen, Figure Z- 8 p 272, e.g. c6 and b12 liked the screen – the User selects **Log A New Data Incident**. This starts the triage of the incident. This triage time was used to record the duration of the use of the Dashboard from start of logging to the final prioritisation stage. At any time during the triage of the incident, the User can stop the triage at any point before reaching prioritisation stage. At the prioritisation stage, the triage is completed, and the triage timestamp **Triage completed in**, is shown. A test incident where the verification stage was stopped was created to show the User this feature. The ability to stop at any time during triage enables the User to start the triage, record the date the incident was first made aware or noted (**Date incident logged**), to gather the information that are needed to assess the harm and for breach notification.

¹⁶⁹ Candidate's profile was checked on LinkedIn and on their company or business websites.

Users were briefed on this feature once they have done the triage of their incident. c6 said *'Oh! It's tracking. That's interesting'*. Although the triage time is not critical for breach notification under the GDPR (noted by f1), it serves as DBI response alerts for organisations to support their decision-making and to take appropriate actions. For example, on alerts, e2 liked the alerts and wanted a real-time updated alert date/timestamps to be sent to his mobile for tracking/monitoring of the incident. c6/K said this: *'I think that's what you want, this incident is 70 hours old, what have you done about it?'* Both users in c6 like the alerts. g7 said: *'that's good. Notification alert is very useful. I like the clock. The countdown'*. l14 said: *'I think really for me the game changer here is the fact you have the 72 hours window so that really changes everything'*. f1 noted and stressed that the first made aware date/time stamp i.e. **Notification due on or reached on** date/time is critical for calculating the 72 hours breach notification deadline. This first made aware date/time stamp can be any date/time in the past or the date the incident is logged. Most DBIs are reported or alerted or identified well after the incident had occurred and hence the first made aware date/time rarely coincides with the actual/real date of the incident. Hence in terms of breach notification and to minimise the likely harm to the affected individuals, the GDPR requires organisations to notify the affected individuals without undue delay or as soon as possible (Article 29 Working Party, 2018). Most of the Users who chose *real incidents* scenario used the date/time calendars to select their *first made aware date/time*. The date/time calendars are shown in Figure Z- 9 p 273 and Z- 10 p 273. f1 from a global insurance company, introduced the concept of confidence factors or levels and requested a *bit more guidance around verify* during the verification stage. When this researcher said: *'verification means: to determine the nature of the incident. How about that?'* f1 replied with *'yeah'*. The verification screens are shown in Figures Z- 11 p 274 and Z- 12 p 274.

g7's incident involved several data types and during the assessment of the data types, he commented that it would help if he got prompted just once for all the data types for volume, data form and security as they are all the same answers for his scenarios. Each of the compromised data types is step-through during the assessment. This step is needed for scenarios whereby some of the data are not of the same form and/or not protected as shown by b16. Samples of the assessment screens are shown in Figure Z- 13 p 275 and Z- 14 p 275.

Upon completion of the triage, the prioritisation screen (Figure Z- 15 p 276) is displayed showing the outcome of the verification and assessment of the incident. As regards the information displayed, b13 said: *'it tells people what they need to do'*. On the triage, b16 said: *'Very clear and quick'*. In general users like the **why?** with the information on the reasons for why notify the individuals and/or the ICO (i.e. Figure Z- 16 p 276, Z- 17 p 277). c6 likes the triage colors used for the display. b13 noticed the need to hover over the display to see the results.

The DashboardV2 with the additional checklists of questions on confidence levels are shown in Figure AA- 2 p 281 to Figure AA- 5 p 282. These Users' selected confidence levels are shown in the prioritisation screens Figure AA- 6 p 283 and Figure AA- 7 p 283. Although DashboardV1 did not have the confidence level checklists, g7 and c6 were assessing their confidence levels during pre-Dashboard. g7 in answering Q10 about adverse effects of the breach e.g. emotional distress, asked this: *'based on high level of impact confidence level of distress? High level of distress in the event that they were lost because we are as much as you can't be 95% sure that they have dumped in the Thames ...'* During Q15 – notification

to individuals (pre-Dashboard) – c6 offered their answers and said: *‘we wouldn’t notify the individual, probably unless we couldn’t get reassurance that the data had been deleted’*. Similarly, f1 in suggesting the use of confidence levels, said this: *‘We would play with the law to a degree to not notify until our confidence factor has got to a certain level. To me that’s still part of verification’*. However, h9 suggested re-phrasing the confidence level questions as they are not too clear for him.

Also, DashboardV2 has help text designed to guide users along the triage steps and screens. For example, Figure AA- 1 p 281 shows the message **You can stop and continue (via Menu)** and the **incident created successfully**. Other help text also appeared on the assessment screens e.g. Figure AA- 4 p 282, when each of the data types has been assessed. On the **stop and continue** features, the following dialogues show some humour.

With f17 (I):

C: *Ok you can stop and continue as part of triage you can go and get info.*

I: *at this point we will say we **don’t know**.*

C: *if you say **don’t know** it would **say go and find out** [the help text for **don’t know** on verification is this: **Please try to find out**].*

I: *[laugh out loud]*

I: *so let’s say assume.*

C: *so in real life you would say let’s go and find out. Does that make sense?*

I: *yes.*

With I14 (U):

C: *So you can stop at any point so here for example I set up an example where you can stop if you don’t know how confident you are. You can pause and come back.*

U: *Right, okay. Pause for how long?*

C: *However long you like.*

U: *But you have got 72 hours.*

C: *Precisely. So the clock, you can see the clock - it’s due now, it’s finished.*

U: *alright (laughter).*

On a serious note, e.g. c6, g7, h9, b11, b12, b13 and b15 expressed their interests in the Dashboard and suggested improvements and/or commercialising the Dashboard. Following from the UES, h9 initiated a meeting with his business partners and with this researcher to explore building the Dashboard into their business portfolios.

6.3.4 Post-Dashboard

When the users completed the Dashboard, they were then guided to the Questionnaire screens. Some of the post-Dashboard screens are shown in Figures Z- 21 p 279 to Z- 24 p 280. I14 (U) was very concerned about confidentiality but towards the end of the Walkthrough he said this: *‘I think, having gone through the process now, obviously I was a bit apprehensive. I did it because obviously we had our chat. But I was’*. C: *‘That’s why I said you’re not expected to disclose any thing. Am I right?’* U: *‘you’re absolutely right’*. Also, he said the questions (the checklists) are *really, really good*. However, c6/K wanted more layers or more detailed questions. When asked what the layers of questions are, c6/K did not provide any

clear explanations or examples. Checklists were mentioned a couple of times by c6/P. Remarks on checklists:

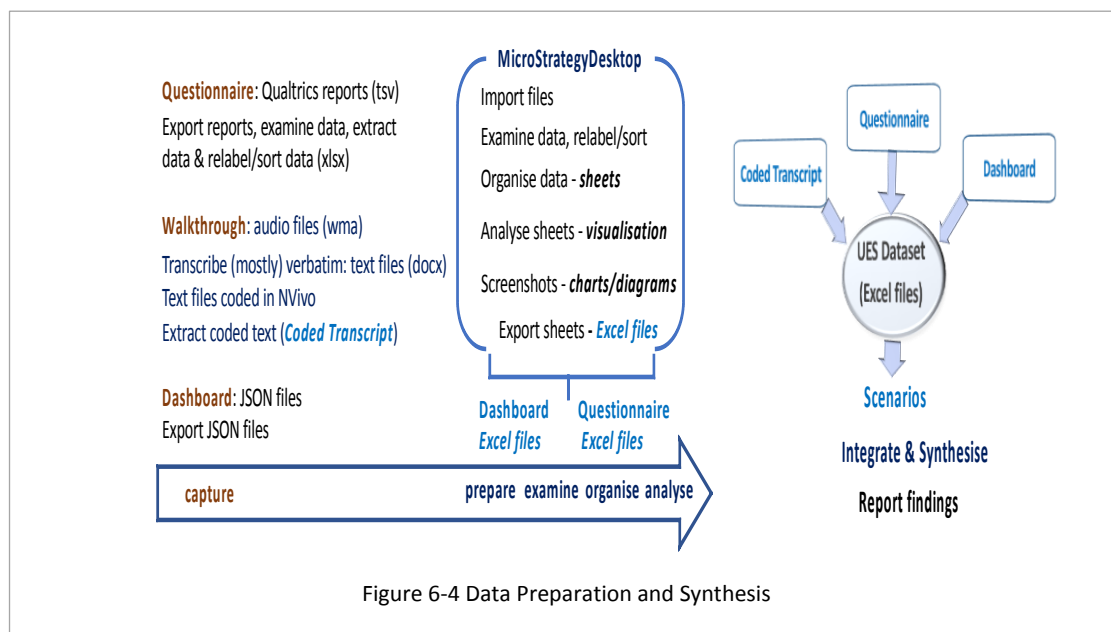
c6/P: *I do like checklists [laughter].*

c6/P: *I do like it. A framework for thinking, which as a practitioner, you're doing but you don't always put it that.*

c6/K: *...put it into that neat format.*

6.4 Data preparation and synthesis

As shown in Figure 6-4 p 138, there were three sets of data captured in the UES: Dashboard data exported in JSON format; Questionnaire data exported from Qualtrics reports; and Walkthrough audio files.



As all this data was mainly text in structured (JSON and Qualtrics) and un-structured (Transcripts and Qualtrics) form, Excel and MSD were used to prepare, transform and analyse the data. NVivo was used to do the initial coding of the Transcripts (snapshots in Appendix AF p 289). Compared to NVivo, MSD provided better data management and transformation tools and it has flexible visualisation or charting tools suitable for decision-support and analysis. The three sets of data were integrated and analysed using MSD. These integrated Excel files and MSD charts/diagrams were used for synthesis and reporting-driven by the UES objective and questions. The integrated and analysed Group1 and Group2 files are shown in Figure 6-5 p 140 and Figure 6-6 p 141. How these files were created i.e. the preparation, transformation and analysis are described in the next sections.

6.4.1 Dashboard files

The Dashboard captured and stored the Users' incident logs, breach details and the results of the triage and data harm assessment. These results are shown in the prioritisation screen of the Dashboard (Figure Z- 15 p 276). Besides exporting all (total of 17) the JSON files (via the Dashboard Menu), the Users' (except b3) prioritisation screens (via the Dashboard Menu) were also examined to verify the data in the

JSON files. The JSON files were imported into MSD, re-labelled and sorted (transformed). Appendix AB p 284 shows the screenshots of the JSON files examined in MSD for a user from Group1 and Group2.

These sorted Users' tables in MSD were exported into individual Excel files which were consolidated into Group1 and Group2 Dashboard Excel files. These grouped files were then imported into MSD and examined and analysed. These integrated and analysed Group1 and Group2 tables were exported for use in the synthesis and reporting. Screenshots of the group charts in MSD are shown in Appendix AC p 285. The exported Excel files (JSON outputs) were manually verified against the Dashboard data on the (individual user's) prioritisation screens. Both the datasets were verified to be identical. However, the derived results¹⁷⁰ (shown on the prioritisation screens) i.e. **Triage completed in** and **Notification due on or reached on** were not in the JSON files. For completeness these derived data were input into Excel sheets and shown in Figure 6-7 p 142 and Figure 6-8 p 142.

A total of 17 Questionnaire responses were stored in one project file in Qualtrics. Before the project file was exported, the ID (user's ID) fields/records were created in Qualtrics. The exported Qualtrics files, a sample in Figure AD- 1 p 286, were then examined and sorted (cleaned-up) in Excel. Once the data was cleaned-up, the Excel files (Group1 and Group2 Questionnaire reports) were imported into MSD as shown in Figure AD- 2 p 286 and Figure AD- 3 p 286. MSD was used to organise and analyse the questions (in Questionnaire) into topics/themes, samples are shown in Appendix AE p 287. These organised questions were exported into Excel files (Questionnaire Excel files). The Questionnaire Excel files were used for synthesis and reporting in Sections 6.5 to 6.8.

¹⁷⁰ The triage results (transactions) were derived from the captured incident details and logs.

Integrated & analysed Excel filenames - Group1 Excel files	Content of the Group1 Excel files	Brief Description	Focus for Synthesis & Reporting
questionnaire result-background-R	Questionnaire result - user background (background)	A chart showing profile of all participants	industry/company, role & experience (YR)
questionnaire result-experience-R	Questionnaire result - user experience (experience)	Generic incident: DBI response, PIA & PHA	users' incident response & privacy assessment experience
questionnaire result-generic views	Questionnaire result & Transcript (generic view)	Generic incident: information, harm & notification	views on breach information, breach harm & breach notification
questionnaire result-specific scenario	Questionnaire result & Dashboard (dataform) & Transcript (specific scenario)	Specific incident: incident type description & views	Real/Hypothetical/Pre-response
questionnaire result-sequence of steps	Questionnaire result & Transcript (questionnaire result-sequence of steps)	Specific incident: sequence of steps result	evaluate triage sequence of steps
questionnaire result-checklists	Questionnaire result & Transcript (questionnaire result-checklists)	Specific incident: checklists result	evaluate checklists
questionnaire result-breach harm-individual	Questionnaire result & Transcript & Dashboard result - individual (breach harm-individual)	Specific incident: views and dashboard results	examine harm, distress & impact on individual & data impact
questionnaire result-dashboard PHA-Notification	Questionnaire result & Transcript & Dashboard result - PHA-Notification	Specific incident: PHA, breach notification, alerts & prioritisation	examine PHA, breach notification, alerts & prioritisation
questionnaire result-notify individual	Questionnaire result & Transcript & Dashboard result - notify individuals	Specific incident: views & individuals notification	examine individual notification
questionnaire result-notify ICO	Questionnaire result & Transcript & Dashboard result - notify ICO	Specific incident: views & ICO notification	examine ICO notification
questionnaire result-dashboard PHA-Notification	Questionnaire result & Transcript & Dashboard result - PHA-Notification	Specific incident: breach notification supports and alerts	examine breach notification support/alerts
questionnaire result-impact	Questionnaire result & Transcript & Dashboard result (impact)	Specific incident: dashboard impact on organisation	impact on: gathering of information; internal communication; recording the response actions
questionnaire result-improvement-other	Questionnaire result & Transcript (other remark)	open views/remarks	open views/remarks

Figure 6-5 UES Integrated Excel files: Group1 lists

Integrated & analysed Excel filenames - Group2 Excel files	Content of the Group2 Excel files	Brief Description	Focus for Synthesis & Reporting
questionnaire result-background2	Questionnaire result - user background (background)	A chart showing profile of all participants	industry/company, role & experience (YR)
questionnaire result-experience2	Questionnaire result - user experience (experience)	Generic incident: DBI response, PIA & PHA	users' incident response & privacy assessment experience
questionnaire result-generic view2	Questionnaire result & Transcript (generic view)	Generic incident: information, harm & notification	views on breach information, breach harm & breach notification
questionnaire result-specific scenario2	Questionnaire result & Dashboard (dataform) & Transcript (specific scenario)	Specific incident: incident type description & views	Real/Hypothetical/Pre-response
questionnaire result-sequence of steps2	Questionnaire result & Transcript (questionnaire result-sequence of steps)	Specific incident: sequence of steps result	evaluate triage sequence of steps
questionnaire result-checklists2	Questionnaire result & Transcript (questionnaire result-checklists)	Specific incident: checklists result	evaluate checklists
questionnaire result-breach harm-individual2	Questionnaire result & Transcript & Dashboard result - individual (breach harm-individual)	Specific incident: views and dashboard results	examine harm, distress & impact on individual & data impact
questionnaire result-dashboard PHA-Notification2	Questionnaire result & Transcript & Dashboard result - dashboard PHA-Notification	Specific incident: PHA, breach notification, alerts & prioritisation	examine PHA, breach notification, alerts & prioritisation
questionnaire result-notify individual2	Questionnaire result & Transcript & Dashboard result - notify individuals	Specific incident: views & individuals notification	examine individual notification
questionnaire result-notify ICO2	Questionnaire result & Transcript & Dashboard result - notify ICO	Specific incident: views & ICO notification	examine ICO notification
questionnaire result-dashboard PHA-Notification2	Questionnaire result & Transcript & Dashboard result - PHA-Notification	Specific incident: breach notification supports and alerts	examine breach notification support/alerts
questionnaire result-impact2	Questionnaire result & Transcript & Dashboard result (impact)	Specific incident: dashboard impact on organisation	impact on: gathering of information; internal communication; recording the response actions
questionnaire result-improvement-other2	Questionnaire result & Transcript (other remark)	open views/remarks	open views/remarks
dashboard result-conflevelDistressR	Dashboard result - Confidence levels - Distress (conflevelDistressR)		
dashboard result-conflevelDataR	Dashboard result - Confidence levels - Data		

Figure 6-6 UES Integrated Excel files: Group2 lists

ID	Description	Triage completed in	Date incident logged	Notification due on or reached on
b3	Unauthorised access to and stealing of personal client	00:04:24	14 January 2018 12:00 AM	17 January 2018 12:00 AM
c6	Data of a child	00:10:52	22 January 2018 12:00 AM	25 January 2018 12:00 AM
e2	paper records left in a room	00:05:43	19 September 2017 12:00 AM	22 September 2017 12:00 AM
f1	Phishing	00:05:24	25 August 2016 12:00 AM	28 August 2016 12:00 AM
f8	Personal data from a stolen laptop	00:05:45	1 November 2013 12:00AM	4 November 2013 12:00 AM
g7	Investigation of data loss	00:06:47	3 April 2013 10:00 AM	6 April 2013 10:00 AM
h5	a near-miss email incident	00:08:36	1 January 2018 12:00 AM	4 January 2018 12:00 AM
o4	Email Phishing leading to data breach	00:05:07	1 October 2016 12:00 AM	4 October 2016 12:00 AM

Figure 6-7 UES Group1 Triage Results

ID	Description	Triage completed in	Date incident logged	Notification due on or reached on
b11	TalkTalk data incident	00:04:03	6 October 2015 12:00 AM	9 October 2015 12:00 AM
b12	web service redirect vulnerability	00:07:00	13 February 2018 12:00 AM	16 February 2018 12:00 AM
b13	Student access restricted health records	00:04:29	15 February 2018 12:00 AM	18 February 2018 12:00 AM
b15	bank account at risk	00:05:41	22 July 2017 10:00 AM	25 July 2017 10:00 AM
b16	Stolen data	00:05:36	10 March 2018 10:30 AM	13 March 2018 10:30 AM
c10	Error in coding and lack of verification checking (printing)	00:06:36	26 October 2010 12:00 AM	29 October 2010 12:00 AM
f17	USB stick lost on train	00:04:22	12 March 2018 12:00 AM	15 March 2018 12:00 AM
h9	Paper record stolen	00:05:39	7 February 2018 10:00 AM	10 February 2018 10:00 AM
l14	Network perimeter was breached	00:09:07	22 February 2018 04:10 PM	25 February 2018 04:10 PM

Figure 6-8 UES Group2 Triage Results

6.4.2 Transcript files

The Walkthroughs were captured using audio recorders. A total of 15 files were transcribed and the text files were pseudonymised before importing into NVivo for coding. NVivo was suitable for the initial coding of the transcripts but for subsequent data analysis of all the dataset (all in Excel files), however it has limited and inflexible decision-support and analysis tools for structured and non-structured data. Such limitations are also raised by Schönfelder (2011). Ose (2016) also recognised the issues raised

by Schönfelder (2011) and provided a simple method to sort and structure large amounts of unstructured data using Word and Excel tools. Besides, *no software can actually analyze qualitative data; only the human mind can do that* (Ose, 2016). Hence the coded texts were extracted into the integrated Excel files for further synthesis. The coding structures in NVivo are shown in Figure 6-9 p 143. Details of the exported coded Nodes are shown in Figure 6-10 p 143. Samples of NVivo screenshots are shown in Appendix AF p 289.

6.5 Results from the Questionnaire (RO4)

As the Questionnaire also captured the Users' backgrounds/profiles, the results were synthesised in Section 6.5.1. As shown in Figure 6-1 p 129, the UES objective-questions were mapped to the questions in the Questionnaire. In Qualtrics, the results for questions i.e. Q19 to Q30 were extracted and reported in Section 6.5.2. These questions were used to evaluate how well the triage playbook concepts meet Users' DBI response scenarios for assessing privacy harm to address initial breach notification i.e. proof-of-concept and proof-of-use. A brief summary and discussion of the results are in Section 6.5.3.

Name (Nodes)	Sources	References	Name (Nodes)	Sources	References
Dashboard	17	85	during	11	37
breach information	9	14	remark on Dashboard	6	12
breach notification	13	33	post	18	148
checklists	14	54	remark on Dashboard	15	68
harm assessment	12	28	remark on Questionnaire	5	9
impact on initial response	7	11	pre	14	57
improvement	7	20	remark on Questionnaire	7	9
notification alert	13	33	specific scenario	11	34
other remark	8	17	breach and harm	6	10
prioritisation 'to notify or not'	9	17	breach information	2	5
scenario	9	18	breach notification	5	10
sequence of steps	7	19	generic incident	9	17
			breach and harm	8	11
			breach information	4	5
			breach notification	1	1

Figure 6-10 NVivo Coded Nodes

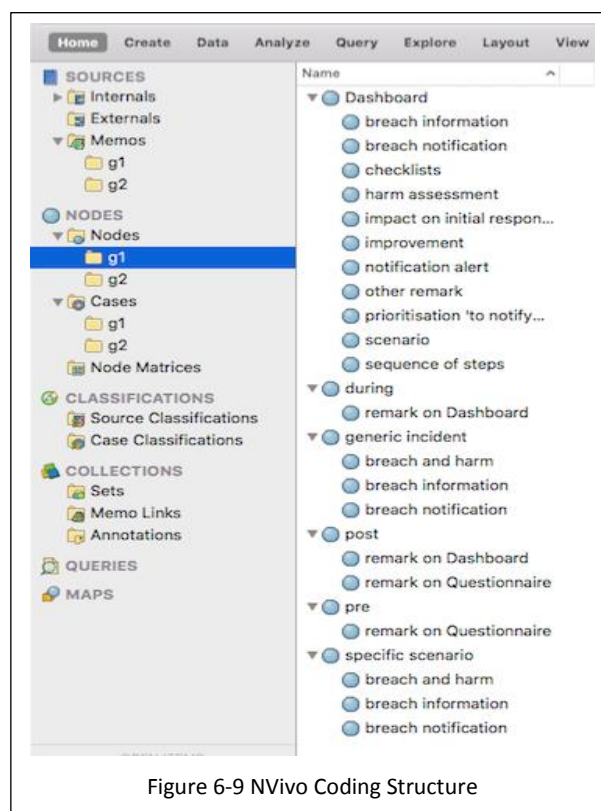


Figure 6-9 NVivo Coding Structure

6.5.1 Profile of Group1 & Group2 Users

The nine users who took part in the interview study (they were marked with upper case industry codes and all are in Group1) were also marked in Figure 6-11 p 144. The number of years in the roles/experiences were shown by the bubbles with numbers. UES Users were marked with lower case industry codes. These industry codes were the same as those used for the interview study. Similar to the interview study, the UES Users and the UES Walkthroughs were all based in/around London.

	User	b11	b12	b13	b15	b16	b3	c10	c6	e2	f1	f17	f8	g7	h5	h9	l14	o4
	Interviewee						B3		C14	E6	F21		F4	G15	H8	H7		O10
Company Type	Group																	
a University	1									3								
corp governance, control & fraud	1						30											
financial & national banks	1												15					
global specialty & commercial insurance	1									8								
large NHS Hospital Trust	1														6			
local authorities	1													18				
national charity	1								8									
small-medium institution	1																	8
consultancy (GDPR)	2	18																
GDPR consultant	2											30						
IM consultant	2			30														
international charity	2							20										
IT consultant	2				38													
large hospitality company	2					6												
legal-IT consultancy	2																15	
news services group	2	2																
public sector consultancy	2															6		
		Director	Software Engineer	IM Consultant	Independent Consultant	Deputy GM	CEO	Head of Infosoc	Chief DPO & DPM	Info. Compliance Officer	Underwriting Mgr & VP	GDPR Project Mgr	MD	Compliance & IG Mgr	IG	MD	Principal Consultant	CEO

Figure 6-11 UES Users' Profiles

6.5.2 Questionnaire results for Group1 & Group2 (Q19-Q30)

Appendix V p 260 shows the questionnaire for Q19 to Q30. The following sections present the results extracted from Qualtrics. There were eight users in Group1 and nine users in Group2. The Figures

6-12 p 145 to 6-14 p 145 show the number of users that responded to the questions (i.e. the number of responses) based on the Likert-style 5 points scales¹⁷¹ i.e. Strongly agree; Somewhat agree; Neither agree nor disagree; Somewhat disagree; and Strongly disagree.

6.5.2.1 How useful are the triage sequence of steps? (RO4-a)(RO4-b)

Figure 6-12 p 145 shows the Group1 and Group2 results for Q19 and Q20.

	Group1				Group2		
	Q19	Q20	Q21		Q19	Q20	Q21
Strongly agree	2	3	4		6	9	9
Somewhat agree	6	5	4		3		

Figure 6-12 Questionnaire results Q19-Q20 (Sequence of steps)

6.5.2.2 How useful are the checklists? (RO4-c)

Figure 6-13 p 145 shows the Group1 and Group2 results for Q22, Q23, Q24 and 25.

	Group1					Group2			
	Q22	Q23	Q24	Q25		Q22	Q23	Q24	Q25
Strongly agree	6	6	5	3		7	7	7	7
Somewhat agree	1	2	3	3		2	2	2	2
Neither agree nor disagree	1			2					

Figure 6-13 Questionnaire results Q22-Q25 (Checklists)

6.5.2.3 How useful is the dashboard? (RO4-d) (RO4-e) (RO4-f)

Figure 6-14 p 145 shows the Group1 and Group2 results for Q26 to Q29.

	Group1					Group2			
	Q26	Q27	Q28	Q29		Q26	Q27	Q28	Q29
Strongly agree	7	4	6	3		8	9	7	7
Somewhat agree	1	3	1	3		1		2	2
Neither agree nor disagree		1	1	2					

Figure 6-14 Questionnaire results Q26-Q29 (Dashboard and alerts)

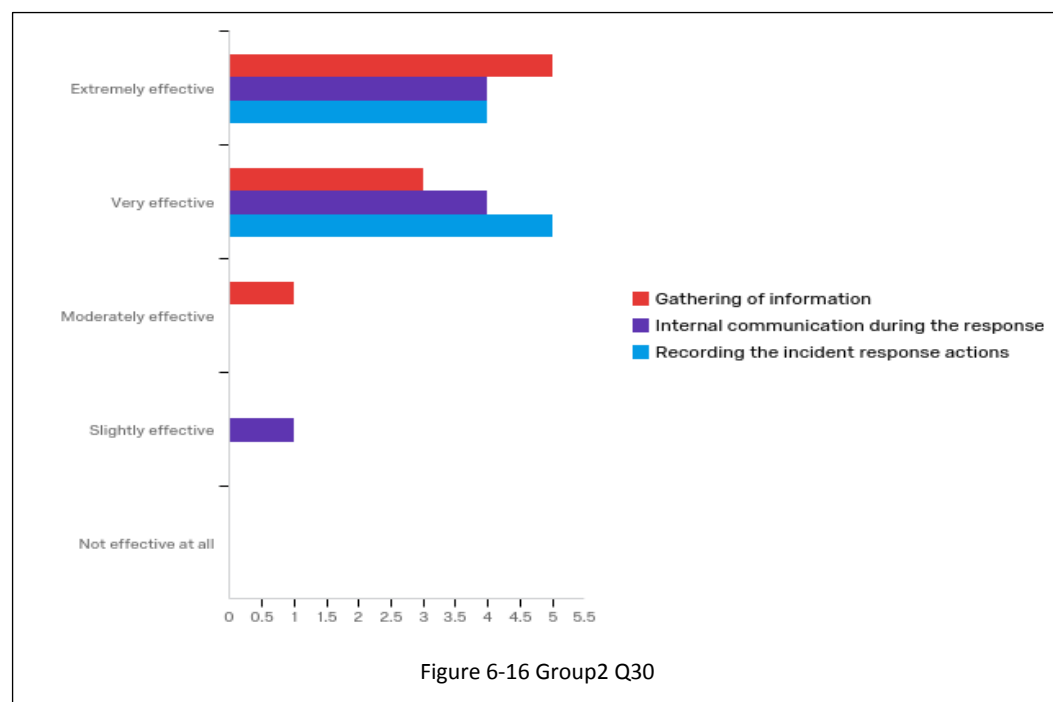
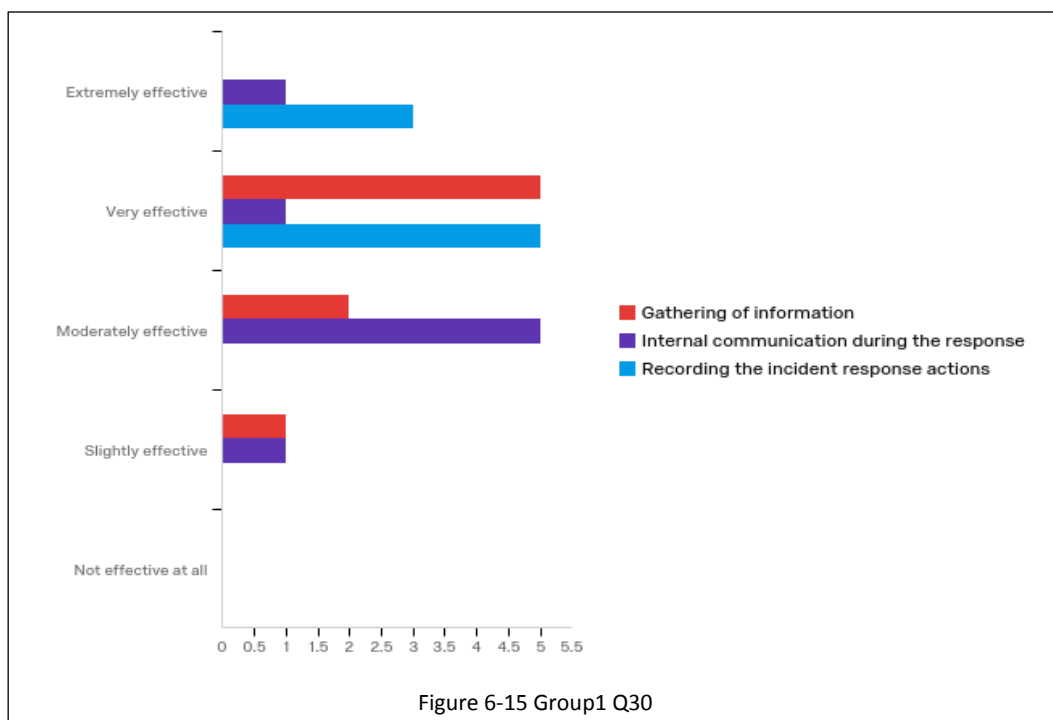
6.5.2.4 What are users' views on the impact of the dashboard on their initial DBI response? (RO4-g)

Figure 6-15 p 146 and Figure 6-16 p 146 are charts extracted from Qualtrics for Q30 results.

The Y-axis from top to bottom has these: Extremely effective; Very effective; Moderately effective; and Slightly effective. The X-axis¹⁷² represents the number of responses.

¹⁷¹ The Likert 5 point scales with no entries/responses are not shown in the figures.

¹⁷² The scales (in decimal points) are fixed (not configurable) by Qualtrics.



6.5.3 Summary and discussion on the Questionnaire results (RO4)

The figures shown in Section 6.5.2 provided an overall trend for all responses for Q19 to Q30. There were no responses for the *disagreement scales*. In order to examine any usage patterns within the agree or neutral (i.e. neither agree nor disagree) trending responses, the figures need to be further synthesised and examined. The percentage (% of the total responses) or frequency of the responses were extracted from Qualtrics and together with the Users' ID (input manually into Qualtrics during the data preparation stage), Figure 6-17 p 148 and Figure 6-18 p 149 were created.

For Group1 Users f1, e2 and b3, the prioritisation screen displayed the triage alert clock, but the notification countdown alert clock¹⁷³ was not displayed. However, on examining Figure 6-17 p 148, the results for these Users appeared not to be dramatically different from other Group1 Users. User f1 did notice and stressed that it would be useful to have a notification alert clock to start from the *first make aware* date/time. He was aware that the *first make aware* date/time was already captured on incident creation, and this can be used for calculating the notification alert clock. However, e3 on commenting on the triage clock, wanted an email/text alert to be automatically sent at various intervals before the 72 hour deadline to him. b3 was happy and remarked this: '*All very nice*'.¹⁷⁴ For the rest of Group1 Users, the counting down clock was displayed. This feature proved to be a *must have* requirement for breach notification during DBI response as noted e.g. by f1, e2, o4, c6, g7, b12, b16, l14.

Incorporating users' requirements during iterative development is a key feature of the RITE approach to ensure that useable software is built. Besides the 72 hour concerns, the iterative UES with Users also highlighted that breach reporting (i.e. notification or communication) to the individuals and to the ICO are important issues (e.g. c6, g7, h9). From Figures 6-17 p 148 and 6-18 p 149, these Users i.e. o4, h5, c6, g7 (Group1) and h9, b12, l14, f17 (Group2) appeared to show some patterns in their responses. For example, o4 and g7 both showed similar responses whereas b3¹⁷⁵, h5 and c6 showed different trends from the rest of the Group1 Users. In Group2, the noticeable patterns are that there were no users in the *other* column (i.e. neutral response) for Q19 to Q29, and the 100% response for Q20, Q21 and Q27. Some possible explanations for the observed patterns and trends in Group2 are: the facilitator was more experienced in the Walkthrough; the additional help text displayed on the various DashboardV2 screens; the additional checklists on confidence levels; or the Users' profiles or demographics (i.e. more experienced professionals). Similar patterns were also observed for Q30 in Group1 and Group2.

¹⁷³ The developer struggled with getting the alert clocks to work/display. This was not a major requirement for iteration 1.

¹⁷⁴ Emailed his consent form and his remark on 14 January 2018.

¹⁷⁵ b3 was self-administered and hence not selected for further synthesis. e3 and f1 were also excluded as they have slightly different display i.e. no counting down clock on their prioritisation screens.

Questions	Synthesised Results			
	50% or more	Less than 50%	Equal %	Other
How useful is the sequence of steps?				
Sufficient for initial DBI response (Q19)	somewhat agree	strongly agree		
	b3, c6, f1, f8, g7, h5	e2, o4		
Appropriate during initial DBI response (Q20)	somewhat agree	strongly agree		
	b3, e2, f1, f8, h5	c6, g7, o4		
For quick conducting PHA (Q21)			agree	
			b3, f8, g7, o4 strongly; c6, e2, f1, h5 somewhat	
How useful is the checklist of Q&As?				
Are simple to follow (Q22)	strongly agree	somewhat agree		neither agree nor disagree
	c6, e2, f1, f8, g7, o4	b3		h5
For quick checking of the necessary breach information (Q23)	strongly agree	somewhat agree		
	b3, c6, e2, f1, g7, o4	f8, h5		
For tracking of the gathered breach information (Q24)	strongly agree	somewhat agree		
	e2, f1, f8, g7, o4	b3, c6, h5		
For assessing privacy harm (Q25)			agree	neither agree nor disagree
			b3, g7, o4 strongly; e2, f1, f8 somewhat	c6, h5
How useful is the dashboard?				
Appropriate for conducting quick privacy harm assessment (Q26)	strongly agree	somewhat agree		
	b3, c6, e2, f1, g7, o4	h5		
For prioritising breach notification within a short timeframe (Q27)	strongly agree	somewhat agree		neither agree nor disagree
	b3, f8, g7, o4	e2, f1, h5		c6
Notification alerts are useful for the prioritisation of breach notification (Q28)	strongly agree	somewhat agree		neither agree nor disagree
	c6, e2, f1, f8, g7, o4	h5		b3
Provides a quick way to address the prioritisation question: 'whether to notify individuals or not?' (Q29)			agree	neither agree nor disagree
			b3, g7, o4 strongly; e2, f1, f8 somewhat	c6, h5
What are users' views on the impact of the dashboard on their initial DBI response? (Q30)				
Gathering of information (Q30a)	very effective	moderately effective		slightly effective
	c6, e2, f8, g7, o4	b3, h5		f1
Internal communication during the response (Q30b)	moderately effective		effective	
	b3, c6, f1, f8, o4		e2 extremely; g7 very; h5 slightly	
Recording the incident response actions (Q30c)	very effective	extremely effective		
	b3, c6, e2, f8, h5	f1, g7, o4		

Figure 6-17 Group1 Synthesised Charts Results

Questions	Synthesised Results			
	50% or more	Less than 50%	Equal %	Other
How useful is the sequence of steps?				
Sufficient for initial DBI response (Q19)	strongly agree	somewhat agree		
	b12, b13, b15, b16, h9, l14	b11, c10, f17		
Appropriate during initial DBI response (Q20)	100% strongly agree			
	b11, b12, b13, b15, b16, c10, f17, h9, l14			
For quick conducting PHA (Q21)	100% strongly agree			
	b11, b12, b13, b15, b16, c10, f17, h9, l14			
How useful is the checklist of Q&As?				
Are simple to follow (Q22)	strongly agree	somewhat agree		
	b11, b12, b13, b16, c10, f17	h9, 14		
For quick checking of the necessary breach information (Q23)	strongly agree	somewhat agree		
	b11, b12, b13, b16, h9, l14	c10, f17		
For tracking of the gathered breach information (Q24)	strongly agree	somewhat agree		
	b11, b13, b15, b16, f17, h9, l14	b12, c10		
For assessing privacy harm (Q25)	strongly agree	somewhat agree		
	b11, b12, b13, b16, h9, l14	c10, f17		
How useful is the dashboard?				
Appropriate for conducting quick privacy harm assessment (Q26)	strongly agree	somewhat agree		
	b11, b12, b13, b15, b16, c10, h9, l14	f17		
For prioritising breach notification within a short timeframe (Q27)	100% strongly agree			
	b11, b12, b13, b15, b16, c10, f17, h9, l14			
Notification alerts are useful for the prioritisation of breach notification (Q28)	strongly agree	somewhat agree		
	b11, b12, b13, b15, b16, h9, l14	c10, f17		
Provides a quick way to address the prioritisation question: 'whether to notify individuals or not?' (Q29)	strongly agree	somewhat agree		
	b11, b12, b13, b15, b16, h9, l14	c10, f17		
What are users' views on the impact of the dashboard on their initial DBI response? (Q30)				
Gathering of information (Q30a)	extremely effective	very effective		moderately effective
	b12, b13, b16, c10, l14	b11, b15, h9		f17
Internal communication during the response (Q30b)			effective	slightly effective
			b12, b13, b16, l14 extremely; b11, b15, c10, h9 very	f17
Recording the incident response actions (Q30c)	very effective	extremely effective		
	b11, b15, c10, f17, h9	b12, b13, b16, l14		

Figure 6-18 Group2 Synthesised Charts Results

In the next section, these Users were noted and further examined. However, all the Users' transcripts, other questions in the Questionnaire and the Dashboard results were also included in the integrated synthesis to address the UES objective and RA. Besides the additional checklists in iteration 2, DashboardV2 also has the long list of data categories displayed on the screen. On DashboardV1, the long list of data categories (i.e. selected by the user) was not wrapped and hence dropped off from the screens (e.g. as shown in Figure Z- 14 p 275). However, none of the Group1 Users i.e. e3, c6 and g7 with their long list of selected data types noticed or remarked on the screen display. One possible reason was that the Users were drawn by the checklists of Q&As while they step through the sequence of triage steps. The triage sequence of steps enabled minimal user screens for performing the triage. g7 (R) said this:

R: The sequence, works really well, verification, assessment and priority. I like that.

C: quick way?

R: Yeah. It's a good structure.

Although the UES was not evaluating how well the dashboard was designed, several users like the dashboard interface e.g. g7, h9, c6, b12, c10. A snapshot of h9 (S) dialogue:

S: have you looked at Datix?

C: I think you mentioned that¹⁷⁶.

S: yeah the one we use in health.

C: yes, someone¹⁷⁷ who uses Datix, said my user interface is better than Datix.

S: certainly for a targeted piece of work, this is definitely better...I can see lots of uses.

He also said this: 'it's a nice interface'. Similarly, b12 said: 'it looks nice' when she first saw the Welcome Screen. User b16 wanted screenshots of the prioritisation screens emailed to her at the end of the Walkthrough. It seems that automating checklists with the use of the triage steps can be done using simple and functional screen design (a low-fidelity prototype). From the Questionnaire results, with the overall *agree* or *effective* trend for RO4, the low-fidelity prototype design seems to work well using the iterative design of the dashboard for proof-of-concept and proof-of-use evaluation. The DBI scenarios as outlined in Q11 enabled the various incident types to be captured and evaluated as close to *real-time* mode as possible. In one scenario the DBI was not only *real* (live one week) but was still under investigation by the User (b13).

6.6 What did the UES reveal? (RO4)(RA)

The UES revealed that the dashboards that implemented the triage playbook provided support for organisations (users) to quickly assess privacy harms to affected individuals such that breach prioritisation i.e. to notify or not affected individuals and/or the ICO? can be addressed during the initial response to a DBI.

The integrated Excel files as shown in Figure 6-5 p 140 and Figure 6-6 p 141 were used to explore Users' incident scenarios (DBIs) and their views on privacy harm (e.g. distress) and breach notification (RA). As shown in Figure 6-2 p 131, there were pre-Dashboard questions in the Questionnaire that

¹⁷⁶ h5(S) also took part in the interview study and mentioned Datix.

¹⁷⁷ An audience remarked that the DashboardV1 – presented at a Privacy Focus group event: Privacy risk: harm, impact, assessment, metrics, organised by De Montfort University on 20 January 2018 – has a nicer interface than Datix. The 10 mins live demo was not recorded.

captured information on incident scenarios, privacy harm and breach notification. Examining the scenarios and Users' experiences/views, not only post-Dashboard but also pre-Dashboard and also the coded Transcripts – hence a rich dataset – exposed insights otherwise hidden or not revealed by just examining the Dashboard or the Questionnaire. Hence the broad question: *what did the UES reveal?* to address not only the UES objective but the RA. The broad question also sets the scope for the coded themes used in NVivo as shown in Figure 6-9 p 143. The open questions i.e. Q31 and Q32 were also examined.

Furthermore, this research was mainly qualitative without quantification of the harm or privacy risks. Hence scenario analysis based on users' experiences/views for examining the *likely* impact of the harm on individual(s) as a consequence of the DBI provided the necessary stories alongside the parameter-driven data harm matrix. Justification for the scenario and storytelling approach is discussed next.

6.6.1 Justification for scenario and storytelling

Researchers have used scenario approaches for their privacy or security or cyber related studies. For example, Woskov et al. (2011) and Williams et al. (2016), use scenario to explain the sequence of events or incidents or activities. Xu and Ning (2005) describe: *An attack scenario is a sequence of steps adversaries performed to attack victim machines. The essence of creating attack scenarios from security alerts is to discover causal relations between individual attacks.* Best et al.'s (2017) research on privacy risk uses a factorial vignette with factors and corresponding levels of risks for their use case scenario description. As pointed out by Rounsevell and Metzger (2010) and Maier et al. (2016) and in a comprehensive analysis on scenario literature by Amer et al. (2013), there are different meanings and types of scenario. This has led to abuses (Durance and Godet, 2010) and confusion or conflicting (Wilkinson and Eidinow, 2008; Molitor, 2009; Hughes, 2013) views in the use of scenario planning and scenario analysis. This is especially so in strategic decision-making and planning where the scenario was first developed for addressing complexity and uncertainty in business environments (Wilkinson and Eidinow, 2008; Bowman et al., 2013).

Besides, Moon (2010) associate scenario to story in that: *scenarios are generally brief stories that describe a situation or an incident.* Similarly, Wilkinson and Eidinow (2008) in referencing others said a scenario is a story, produced for a variety of purposes to enable sense making and to inform decision making. This is because a scenario narrates the potential future conditions and how they came about. Hence by analysing Users' DBIs scenarios in terms of their re-telling and unfolding of their experiences and/or views on privacy harm and breach notification (both complex events) may provide insightful stories. As the same Users' stories were also captured in the Dashboard, these enabled new stories or themes to be examined i.e. *what did the UES reveal?* By revealing these stories which give order and meaning to events; they help explain why things happened or could happen in a certain way (Bowman et al., 2013).

Although storytelling *is nebulous, ephemeral, subjective, and unscientific* as pointed out by Paradise (2007) and others, Paradise (2007) argued for and proposed a storytelling driven research model/program for computer-based decision support in the organisation context. However, Bowman et

al. (2013) took a generic stance in providing a process model for storytelling which is also theoretically driven and empirically grounded. At the conceptual level, their storytelling process model is designed around scenarios for prospective storytelling using two interventions based on inductive and deductive analysis.

According to Barber (2009) scenarios and questions are *universal futures tools as they exist to assist us to discover 'doubt' in our own thinking and overcome the Intelligence Trap*. However, Bowman et al. (2013) has shown how storytelling theory provides the conceptual lens, guided by their research question, for analysing their data inductively and deductively. As illuminated by Collins (2013), in researching organisational storytellers and researchers, stories have a deductive and/or inductive structural aspect. For example, notable storytelling researcher Gabriel (2000), advocates the narrative-deductive aspects of stories i.e. narratives may be defined *a priori*, whereas for Boje (2001) another notable storytelling researcher, stories are defined by their audience i.e. antenarrative and hence inductive approach is needed (Collins, 2013). Although not all storytellers use or agree on these two structural aspects in organisational stories, Collins (2013) in referencing others, points out that all stories *contain features which are also normally associated with a narrative definition of storytelling*. This is the story description: *A story describes a sequence of actions and experiences done or undergone by a certain number of people, whether real or imaginary. These people are presented either in situations that change or as reacting to such change. In turn, these changes reveal **hidden aspects of the situation** and the people involved, and engender a new predicament **which calls forth thought, action, or both**. This response to the new situation leads the story towards its conclusion* (Boje, 2001, p 22).

6.6.2 Storytelling approach and the plot

Boje's (2001) description of stories and storytelling and Bowman et al.'s (2013) approach in using inductive and deductive data analysis were adopted for the synthesis and reporting of the UES datasets. Adopting the storytelling approach also aligns with the pragmatic methodology of this research. The overarching abductive-deductive-inductive questions for interpreting and inferencing the stories from the UES datasets are shown in Figure 6-19 p 152.

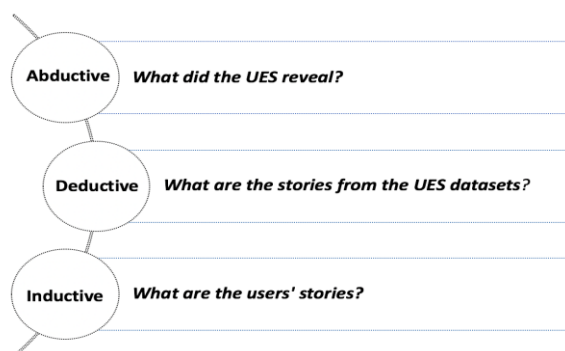


Figure 6-19 Abductive-Deductive-Inductive Storytelling

The plot centred on the user to focus and quickly assess harm to affected individuals during initial DBI response. This plot was created from the interview study where the storylines from the interviewees are:

- (a) *'The response **should be immediate** to actually make customers aware that their data may have been compromised, **even if it has not**' (B3).*
- (b) *'An immediate on the ground response was needed because it was a human type incident' (C14).*
- (c) *'The **response framework is far too slow**, even if it was unintentional...the **victim has to continually suffer the consequences of that**' (F4).*
- (d) *'Most people, most **organisations will look at harm** through **the lens of harm to the organisation**' (B11).*
- (e) *'It's very hard to put any guidelines around prioritisation together if you don't know what harm means arising from personal identifiable data. Unfortunately, the only clear links to data and harm are legal decisions that we don't have any statutes for. The harm threshold is completely different on the same types of data as they are currently categorised. So how do you prioritise unless this is fact specific?' (F21).*
- (f) *'Breach of privacy is a tricky thing to measure' (G15).*
- (g) *'Degrees of privacy harm, it's quite a subjective thing, so what I feel is a breach of privacy, another person wouldn't' (L19).*

During the discussion on privacy harm, interviewees (H7, B9, O10, B11, F12, C14, G15, F21) mentioned personal data or the types of data or data records. Also, F17 pointed out that there was a relationship between the type of industry sector and the type of *value* (i.e. humanitarian, fiscal and emotional aspects) attached to the lost or compromised data as perceived by the affected organisation.

Briefly, the storylines in the plot are:

- (a) Risk is an event e.g. the DBI that may or may not happen.
- (b) Impact is what will happen (the outcome or consequence) if or when the event occurs.
- (c) DBI response is conducted when the DBI has occurred or has been reported/logged/detected. DBI response can also be done during pre-response planning exercises i.e. as part of incident response management.
- (d) PHA addresses the likely impact of the DBI in terms of the likely privacy harm on individuals whose personal data have likely been compromised. An example of a harm is the distress that an individual may suffer as a consequence of the personal data being compromised.
- (e) The Dashboard uses a pre-set parameter-driven data harm matrix (built-in) for assessing the harm to affected individuals based on the user's input to the various checklists of questions and answers.
- (f) The user tells/re-tells his/her DBI stories in a sequence of scenarios or events. These are captured in the Dashboard, the Questionnaire and in the Transcript.
- (g) The user is able to play¹⁷⁸ with the stories using the Dashboard to address whether to notify or not the affected individuals and/or the ICO (i.e. **to call forth into thought, action or both**).
- (h) The final screen i.e. the prioritisation screen is where the user gets **the hidden aspects of the situation** (e.g. the level of impact on individuals and the impact of the compromised data).

¹⁷⁸ The Dashboard Menu has features to delete, to start a new incident, and/or to resume at any point during triage.

6.7 What are the stories from the UES datasets?

The stories were visually shown using extracts from the synthesised datasets and from MSD. Any **surprises** or observations and also any remarks from users are then reported.

6.7.1 Profiles and experiences (Q1-Q6)

Except for one user (f8), all the users in Group1 have DBI response experiences or responsibilities. f8 who took part in the interview study experienced a DBI response – a victim – as a result of her stolen personal data. Although o4 has no experience in PHA or PIA, he managed and responded to an incident which he also described for the interview study. As indicated by c6 and g7, PHA is not a formal or dedicated incident response procedure/process. In Group2, only user b15 has no direct DBI response experience or responsibility and no PIA and PHA experiences. b16 has DBI response responsibility but no PIA and PHA experiences. Although b12 has no direct DBI response responsibility, she has been involved in pre-incident response exercises which she described for one specific incident scenario. Users c10, b15 and b12 are IT/software professionals. Only one user, l14 is from the legal profession, there is none in Group1. The users' profiles and experiences are shown in Figure 6-20 p 155 (Group1) and Figure 6-21 p 156 (Group2).

Title: Role	Title Role (yr)	DBI response			PIA		PHA during DBI response		
		Yes	No	Other	Yes	No	Yes	No	Other
Information Compliance Officer: I am responsible for providing advice to C on its obligations under DPA/FOI and other associated legislation.	2.5	e2			e2		e2		
Information governance: All aspects of Information governance inc. Incident management and response.	5.5	h5			h5		h5		
CEO: Running & governance of my company.	30	b3			b3		b3		
Chief Data Protection Officer(K) & Data Protection Manager(P).	8	c6			c6				c6
Compliance and Information Governance Manager: Previously I have been nominated data protection officer at 3 local authorities. I have led on Freedom of Information, Records Management, Data Quality and Information Security Policy. Currently I lead for the College on writing the information security policy and associated codes of practice, as well as information risk, information asset management and working closely with colleagues to implement GDPR.	18	g7			g7				g7
Chief Executive Officer: Responsible for oversight of the Institute executive team and delivering agreed strategy. Accountable to the Board.	8	o4				o4		o4	
MD: Explaining what good governance is and how IT can support or diminish the quality of overall governance and performance.	15			f8		f8		f8	
Underwriting Manager, Vice President, Strategic Assets: Responsible for a portfolio of insurance business encompassing cyber risks and other intangible assets and specifically inclusive of privacy risks and the costs associated with them.	8			f1		f1			f1
Qualtrics results		75%	13%	13%	63%	38%	38%	25%	38%

Figure 6-20 Group1 profiles and experiences (DBI, PIA & PHA)

Title: Role	Title Role (yr)	DBI response			PIA			PHA during DBI response		
		Yes	Have responsibility	Other	Yes	No	Other	Yes	No	Other
Information Management Consultant: Ensuring data protection compliance, adequate controls are in place. Breach reporting.	30	b13			b13			b13		
Head of Infosec: Oversee ISMS. Manage Cyber Security Analyst/network engineers. Specify and oversee Cyber Security programme (rolling) based on Iso27001 risk assessment and Regulatory and statutory.	5 years STC company 20 years experience	c10				c10		c10		
Managing Director: I run and deliver consultancy on the appropriate use of personal data. Generally focused on legal compliance and sharing in complex environments.	6	h9			h9				h9	
Director: MD.	5 yrs + 10 yrs banking + 3 yrs consultancy		b11				b11		b11	
Deputy General Manager: I manage a team of 50 Catering staff members. My role includes hiring new employees which entails collating personal and sensitive data in order to set them up on our HR system, known as People Matters. I record all data in paper format in individual personnel files.	6		b16			b16			b16	
GDPR Project Manager: Responsible for all delivery work streams for the company's GDPR Programme including Business Analysis, IT systems analysis and development, Process Redesign, Policy design and update, training, communications. Supporting DPO in reporting definition.	9 months this role. 30 years overall.		f17		f17			f17		
Principal Consultant: Provide business intelligence, data warehousing, data security and cyber security strategy consultancy to private and public sector organisations.	15+		l14			l14		l14		
Backend Java Software Engineer: Developing microservices which provide most of the features of my company's site. - Maintaining them - Securing them - Architectural design.	2			b12	b12				b12	
Independent Consultant: Providing consultancy advice in IT-related matters.	8 years and 38 years in IT			b15		b15			b15	
Qualtrics results		33%	44%	22%	44%	44%	11%	44%	56%	

Figure 6-21 Group2 profiles and experiences (DBI, PIA & PHA)

6.7.2 Generic incidents stories (Q7-Q10)

6.7.2.1 On minimal breach information during initial DBI response

Q7	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
During the initial stage namely before a thorough investigation (e.g. digital forensics) of data incident, there is minimal available breach information	b12 b15 b16 f17 l14	b11 c10			b13 h9
Qualtrics results	56%	22%			22%

Figure 6-22 Group2 minimal breach information

Q7	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
During the initial stage namely before a thorough investigation (e.g. digital forensics) of data incident, there is minimal available breach information		c6 e2 f8 g7 o4	b3 f1 h5		
Qualtrics results		63%	25%	13%	

Figure 6-23 Group1 minimal breach information

Generic incidents mean no reference to specific DBI scenarios and also the Users' views were pre-Dashboard. It seems that h5 and h9 i.e. from the health sector where breach assessment and notification are mandatory (pre-GDPR) with established NHS frameworks, had views that differed from most of the users with respect to minimal breach information. Interestingly, b13 (who had just started investigating an NHS DBI case during the UES) also shared the same view as h9.

6.7.2.2 On data breaches and a person's risk

Q8	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
Data breaches increase a person's risk of identity theft or fraud and cause emotional distress as a result of that risk.	b11 b12 b13 b15 b16 c10 f17 h9 l14				
Qualtrics results	100%				

Figure 6-24 Group2 data breach and a person's risk

Q8	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
Data breaches increase a person's risk of identity theft or fraud and cause emotional distress as a result of that risk.	b3 e2 f8 g7 h5 o4	f1	c6		
Qualtrics results	75%	13%	13%		

Figure 6-25 Group1 data breach and a person's risk

There is a general agreement in Group1 and Group2 on the statement by Solove and Citron (2016): data breaches increase a person's risk of identity theft or fraud and cause emotional distress as a result of that

risk. However, f1 (M) who primarily works in the insurance sector said it is *fact specific* and expressed his reason for *somewhat agree*:

M: hence why I somewhat agree instead of strongly agree.

M: I probably would put that because. Do you want me to explain?

C: if you want you can, I'm happy to hear.

M: There are areas here for e.g. around meta data, tracking data, – fundamental rights – people being followed everywhere you go & travel. GDPR is leading towards that making the Google and the WhatsApp accountable for that – tracking everybody is and cross sell to people and using spamming them and annoy people with things they don't want to see. And why should anyone know where I am, but me.

C: so not just fraud, financial loss & physical harm.

M: no, I don't think so.

C: so it's wide.

M: a right to privacy.

In a charity sector, c6 (K & P) expressed their views:

K: I think people certainly worry about identity theft. I think it's probably if you ask an individual they would say that would be the key words. I am not sure it's a key risk. I think it's perceived risk.

P: It does causes anxiety.

P: I think at the NS (their organisation) we are more into the risk of people being caused very grave distress because we are often handling extremely sensitive social care records.

6.7.2.3 On data breaches and adverse effects on individuals

Q10	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
A data breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage.	b11 b12 b13 b15 b16 c10 h9 l14				
		f17			
Qualtrics results	89%	11%			

Figure 6-27 Group2 data breach and adverse effects

Q10	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
A data breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage.	b3 c6 e2 f1 f8 g7 h5 c4				
Qualtrics results	100.00%				

Figure 6-26 Group1 data breach and adverse effects

The ICO's (2017) statement that *a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage* clearly captured most of the Users'¹⁷⁹ views.

¹⁷⁹ f17 did not make any remarks.

6.7.2.4 On notification fatigue and breach notification

Q9		Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree	Note
To prevent <i>notification fatigue</i> to individuals, <i>only in cases</i> where a data breach is likely to adversely affect the privacy of the individual, for example in cases of identity theft or fraud, financial loss, physical harm, significant humiliation or damage to reputation, <i>should the individual be notified.</i>	c6						Notify individuals: case specific
	g7						
	h5						
				b3			Neither agree nor disagree
					e2		Notify individuals: not case specific
					f1		
					o4		
Qualtrics results		38%		13%	38%	13%	

Figure 6-28 Group1 notification fatigue and breach notification

Q9		Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree	Note
To prevent <i>notification fatigue</i> to individuals, <i>only in cases</i> where a data breach is likely to adversely affect the privacy of the individual, for example in cases of identity theft or fraud, financial loss, physical harm, significant humiliation or damage to reputation, <i>should the individual be notified.</i>	b12						Notify individuals: case specific
	b13						
	b16						
			b15				Notify individuals: case specific
			f17				
			h9				Neither agree nor disagree
				c10			
Qualtrics results		33%	33%	11%	11%	11%	

Figure 6-29 Group2 notification fatigue and breach notification

Q9 was extracted from Albrecht (2012). This question raised several remarks from Users. Although b13 answered *strongly agree*, he actually intended *strongly disagree*. His remarks: ‘*individual be notified? Should **always** notify them*’. However, b12 who deals with designing and implementing security protection said this: ‘*I would personally say that you only notify individual if something affects them, and if it doesn’t, from my experience, there are loads of people who will try to make an attack and get information. A lot of it doesn’t work they don’t get anything. So, if you keep on notifying people – false positive*’. However, a lawyer’s view is on the opposite spectrum and he said, ‘*it’s quite interesting*’. He opened up his stories and spoke in terms of the *trajectory and pendulum* of the legislation (mentioned the GDPR and other privacy related laws) *is continuing to swing on the side of the individuals*. l14 was very concerned on disclosing information. However, towards the end, the dialogue went:

U: *yeah. I think, having gone through the process now, obviously I was a bit apprehensive. I did it because obviously we had our chat. But I was.*

C: That's why I said you're not expected to disclose any thing. Am I right?

U: you're absolutely right.

U: But as a consultant, we learn, and we keep client confidentially.

o4 who answered, *somewhat disagree* also said 'it's an interesting question'. Unlike l14, o4 stories have no mention of GDPR or any regulations, but he also leans towards the individuals. Here are o4 stories: '...if you don't know the extent of the breach to begin with, you don't know how likely it is to adversely affect privacy of the individual. So, **waiting until you notify the individual could be too late**. So I would tend to, I think, **disagree**, certainly in my own experience. My concern was, when we had our breach, that there was, if I didn't tell them, that in telling them then they could be alert to the risk of anybody trying looking to maybe do some sort of phishing exercise or whatever. Whereas if they were aware at least they were alert to it.

C: so you don't think notification fatigue should be a problem and should just notify.

o4(l): I think it's a case of the lesser evil and **I think notification fatigue is less of an issue than the risk of financial loss or harm which you can't make a judgement on because you don't know enough information**. I think you should err on the side of caution and notify them rather than, I think the problem with this, **is it's likely to be used as an excuse on organisations not to notify**'.

f1, who stressed that data breach and privacy risks and harm are 'fact specific', also shared the same views as o4 and e2. f8 clearly expressed her experiences as a DBI victim in swinging her pendulums to the individuals.

This question is also interesting when users were asked on their specific DBI scenarios i.e. Q15. From this generic breach notification fatigue question, it appears that the answer to the question *to notify or not* affected individuals has two spectrums¹⁸⁰ i.e. notify individuals (**not case specifics**) or notify based on the nature of the case (**case or fact specifics**). Hence the *note* column in both the figures shows the synthesised spectrums i.e. **notify individuals: not case specific** and **notify individuals: case specific**. These spectra were used to dig deeper for other stories when specific incidents were examined and used in the Dashboard.

6.7.3 Specific incidents stories (Q11-Q18)

The specific incident scenarios described by the Users in Group 1 and 2 are shown in Appendix AG p 291. The short incident descriptions and the stories captured by the Dashboard are shown in various scenarios in Figures 6-30 p 161 and 6-31 p 162.

¹⁸⁰ Excluding the neutral response.

6.7.3.1 Scenarios of the triage of the incidents

ID	Incident type	Short description	Special individual	Individual number	Data volume	Data form	Data protected	Sensitive data	Date incident logged (first aware)	Triage completed in	Notification due on or reached on
e2	real	paper records left in a room	No	High	High	paper-based	No	Yes	19 September 2017 12:00 AM	00:05:43	22 September 2017 12:00 AM
h5	real	a near-miss email incident	Yes	Low	High	digital	No	No	1 January 2018 12:00 AM	00:08:36	4 January 2018 12:00 AM
b3	hypothetical	Unauthorised access to and stealing of personal client data	No	High	High	digital	No	Yes	14 January 2018 12:00 AM	00:04:24	17 January 2018 12:00 AM
c6	real	Data of a child	Yes	Low	Low	digital	No	Yes	22 January 2018 12:00 AM	00:10:52	25 January 2018 12:00 AM
g7	real	Investigation of data loss	No	Low	Low	paper-based	No	Yes	3 April 2013 10:00 AM	00:06:47	6 April 2013 10:00 AM
o4	real	Email Phishing leading to data breach	No	High	High	digital	No	No	1 October 2016 12:00 AM	00:05:07	4 October 2016 12:00 AM
f8	real	Personal data from a stolen laptop	No	Low	Low	digital	No	Yes	1 November 2013 12:00 AM	00:05:45	4 November 2013 12:00 AM
f1	real	Phishing	No	High	High	digital	No	Yes	25 August 2016 12:00 AM	00:05:24	28 August 2016 12:00 AM

Figure 6-30 Group1 scenarios of the triage

The **triage completed in** shows the total time taken from the start of the triage i.e. create/log a New Incident (e.g. Figure T- 2 p 246) to the end of triage i.e. prioritisation screen results (e.g. Figure T- 13 p 251). As shown in Figure 6-30 p 161, the **triage completed in** by c6 is the longest as there were two users and also a fair amount of discussion. The 72 hour countdown of the **Notification due on or reached on** clock starts from the *first aware* date i.e. the **Date incident logged**. As shown in Figure Z- 15 p 276, g7's incident happened in April 2013, hence the **Notification due reached on** in April 2013. For l14 his **Notification due in** was counting down from 72 hours as shown in Figure AA- 1 p 281. As mentioned in Section 6.5.3, Users find this real-time¹⁸¹ notification alert clock a useful feature due to the strict GDPR 72 hour breach notification deadline.

¹⁸¹ The 72 hours count down processing was not based on any legal or business calendar processing specification.

ID	Incident type	Short description	Special individual	Individual number	Data volume	Data form	Data protected	Sensitive data	Date incident logged (first aware)	Triage completed in	Notification due on or reached on
b13	real	Student access restricted health records	Yes	High	Low	digital	No	Yes	15 February 2018 12:00 AM	00:04:29	18 February 2018 12:00 AM
c10	real	Error in coding and lack of verification checking (printing)	No	High	High	digital	No	Yes	26 October 2010 12:00 AM	00:06:36	29 October 2010 12:00 AM
h9	real	Paper record stolen	Yes	Low	Low	paper-based	Yes	Yes	7 February 2018 10:00 AM	00:05:39	10 February 2018 10:00 AM
b11	response planning	TalkTalk data incident	No	Low	High	digital	No	Yes	6 October 2015 12:00 AM	00:04:03	9 October 2015 12:00 AM
b16	hypothetical	Stolen data	No	Low	Low	paper-based & digital	Yes/No	Yes	10 March 2018 10:30 AM	00:05:36	13 March 2018 10:30 AM
f17	hypothetical	USB stick lost on train	No	High	High	digital	Yes	No	12 March 2018 12:00 AM	00:04:22	15 March 2018 12:00 AM
i14	real	Network perimeter was breached	No	High	High	digital	No	Yes	22 February 2018 04:10 PM	00:09:07	25 February 2018 04:10 PM
b12	response planning	web service redirect vulnerability	No	Low	Low	digital	Yes/No	No	13 February 2018 12:00 AM	00:07:00	16 February 2018 12:00 AM
b15	hypothetical	bank account at risk	No	High	High	digital	Yes	Yes	22 July 2017 10:00 AM	00:05:41	25 July 2017 10:00 AM

Figure 6-31 Group2 scenarios of the triage

6.7.3.2 Stories on the individual and personal data types

As shown in the above figures Users' DBI scenarios (scenarios) included sensitive and non-sensitive data types and also special types of individuals. High means greater than 100 and Low means less than or equal to 100. In b13's scenario – incident just triggered – even though one individual's data was compromised, it was assessed for data breach consequences.

Also, various scenarios from unauthorised access, error/untested codes, fraud investigation, stolen laptop to USB stick left in train were shared by Users. Although f17(i) specified a *hypothetical* scenario during pre-Dashboard, he told a *typical* (also c6's stories) scenario and was asking questions just like the checklists in the Dashboard:

I: it's going to be typical, very typical.

I: initial is that before or after any formal investigation? (query during the notification questions in the Questionnaire).

C: before any formal investigation because its 72 hours.

I: ok, I am going to put no here because (typing).

C: ok, does it involve personal data?

*I: that's the key thing, in our scenario, because of the nature of our data we have, with commercial insurance, so depending on whether the personal information is included in that if not whether it's aggregated. So our first step is always - **what was the data? would it be? how was it protected?** [his checklists].*

*I: we would assume **we don't know** there is personal data.*

C: we can use the dashboard to help.

In performing triage of their incident scenarios, the first step was to verify the individuals (Figure Z- 11 p 274). There are data that are user specified and those derived (shown in *italics* in Figures 6-30 p 161 and 6-31 p 162) from the data harm matrix. If any *special individual* is identified, then the result *Yes* is shown. Similarly, if any *sensitive data* is involved, *Yes* is shown.

The list of individuals and personal data (data) types are shown in Figures 6-32 p 163 and 6-33 p 163. g7's scenario was for a criminal fraud investigation involving a *suspect*. As *suspect* was not on the checklists, he used *customer/client* for his scenario.

individuals	
	special
customer/client	patient
employee	child
subscriber/member	criminal/suspect
student/researcher	
donor	

Figure 6-33 Individual types

personal data	
	sensitive
name	genetic
identification number (ID)	health
online identifier	biometric
location data	sex life or sexual orientation
picture/image/videos	political opinions
<i>social (not-metadata)</i>	racial or ethnic origin
cultural	religious beliefs
	trade union membership
	economic/financial
	<i>social (metadata)</i>

Figure 6-32 Personal data types

Subsequently, for DashboardV2, *suspect* was added to the checklists. Similarly, f1 whose scenario was a US case which involved UK individuals, pointed out that *social* data could be metadata, and this was added for DashboardV2. Besides f1, g7 and c6 also mentioned the challenges with *social* data especially in the context of *social care* data. Although researchers have discussed personal data and data sensitivities (Section 6.3.3), the concept of *individual* data types is hardly mentioned in privacy or security literature. This is because little research has been conducted on privacy harm on individuals. However, as shown by the results, organisations **do collect and process personal data** that identify *individuals* such as their customers/clients and employees. In the social care sectors e.g. as highlighted by c6, they provide services to their customers/clients but instead of *customers* they use the term, *service users*. From such stories, Figures 6-34 p 163 to 6-37 p 164 were compiled to show the usage of the checklists of individuals and data types.

Individual Checklist Referenced	Individual Checklist Not Referenced	Other Individual types
Child (1)	Criminal	<i>Service user</i>
Customer/Client (5x)	Donor	<i>Dependents</i>
Employees (1)		
Patient (1)		
Student/Researcher (1)		
Subscriber/Member (1)		

Figure 6-35 Group1 individual checklist (usage)

Individual Checklist Referenced	Individual Checklist Not Referenced
Child (1)	Criminal/Suspect
Customer/Client (5x)	Subscriber/Member
Donor (1)	Student/Researcher
Employees (3x)	
Patient (2x)	

Figure 6-34 Group2 individual checklist (usage)

Data Checklist Referenced	Data Checklist Not Referenced	Other Data types
Cultural (2x)	Genetic	<i>Social (Sensitive)</i>
Economic/Financial (5x)	Biometric	
Health (2x)	Political opinions	
Identification number (6x)	Trade union membership	
Location Data (6x)	Picture/image/videos	
Name (8x)		
Online identifier (1)		
Racial or ethnic origin (3x)		
Religious or philosophical beliefs (2x)		
Sex life or sexual orientation (2x)		
Social (Not metadata) (3x)		

Figure 6-36 Group1 data checklist (usage)

Data Checklist Referenced	Data Checklist Not Referenced
Cultural (1)	Genetic
Economic/Financial (5x)	Biometric
Health (3x)	Political opinions
Identification number (4x)	Social (Not metadata)
Location Data (7x)	Social (Sensitive)
Name (8x)	
Online identifier (2x)	
Picture/Image/Video (1)	
Racial or ethnic origin (3x)	
Religious or philosophical beliefs (2x)	
Sex life or sexual orientation (1)	
Trade union membership (1)	

Figure 6-37 Group2 data checklist (usage)

The Users' scenarios and the checklists were used for deriving the data and individual impact levels as shown in Appendix AH p 292.

6.7.3.3 Stories on the protection of data

Some Users' identified data types were protected, and some were not, and these are shown as Yes/No e.g. b12 and b16 scenarios. In the triage assessment of the data types, if digital data (i.e. data form is digital) then *protection* means encrypted data, and *protection* for non-digital data (i.e. paper-based) means secured with physical mechanisms or security policies (i.e. technical and organisational measures as required under the GDPR). For example, b16 holds paper records which were locked up and some of these data were also held digitally, but not protected. h9's stories revealed that even organisational security measures e.g. policies for handling sensitive data were not adhered to, hence the data breach incidents.

6.7.3.4 Scenarios on privacy harm and breach notification: Group1 stories

In Figure 6-38 p 165, the Users' stories on level of harm and distress (pre-Dashboard) are shown alongside the results from the Dashboard. As different data types have different levels of harm based on the data types, volume affected and protected or not, the *likely data impact* column shows the derived levels from the pre-set data harm matrix in the Dashboard. However, all sensitive data have default *High impact*. For example, c6's data scenarios in Figure 6-39 p 166 show the *High/Medium* data impact for the different types of data. Although their health data was password protected, they also said it was not secured as the password was not encrypted, hence the default for sensitive data was high impact. The

pre-set parameters in the data harm matrix seems to align with Users' views as shown in Figure 6-38 p 165. o4's stories were that at the time of the incident, they assumed the worst case – before any detailed investigation – and notified the affected individuals and also the ICO. However, after the initial notification and with further investigation, the incident was viewed as low risk as no sensitive data was compromised.

Privacy harm & distress (Q13 & Q14)	Pre-dashboard: Level of impact			Dashboard	
	High	Medium	Low	Likely impact on individual	Likely data impact
The overall level of the actual, likely or could have <i>impact of the privacy harm</i> (harm) to the individuals whose personal data have been or may have been compromised. (same answers) The overall <i>level of distress</i> (for example, anxiety) that the individuals have or may have suffered as a consequence of the data incident	b3			Medium	High/Medium
	c6			High/Low	High/Medium
	e2			Medium	High/Medium
	f8			Medium	High/Medium
	g7			Low	High/Medium
		f1		Medium	High/Medium
		h5		High	Medium
			o4	Medium	Medium

Figure 6-38 Group1 level of impact – harm and distress

The Dashboard results showed Medium impact as the data was not protected. Under the GDPR, such an incident **may not** require notification to the affected individuals but the final ICO's decision may be different and hence the ICO needs to be notified as this is a breach of security. This is shown in Figure 6-41 p 168, with High/Medium or Medium data impact and Yes to notify ICO. As revealed by g7, pre-Dashboard, the ICO was notified but the individual was not notified. However, as shown by the Dashboard results, under the GDPR, the individuals would need to know when sensitive data was compromised.

As high risk and risk are not clearly defined in the GDPR, and there are different views on the sensitivity of data (Section 6.3.3) the non-sensitive data could potentially be *Medium impact* or has risk to the affected individuals. Hence for non-sensitive data even if low volume is compromised but if not protected, the likely impact is *Medium* i.e. has risk to the individual. This is because non-sensitive data can be combined or aggregated and used to profile the individual to cause harm. This was the case with f8 where she suffered distress (as told in the interview study).

Dashboard results: Data & Impact							
ID	Description of Incident	TypeOfData	VolumeOfData	DigitalForm (1:yes)	DataEncrypted or otherMeasures	TypeOfData sensitive (1:yes)	DataImpact Level
b3	Unauthorised access to and stealing of personal client data	Economic/Financial	HIGH	1	0	1	High
		Identification number	HIGH	1	0	0	Medium
		Location Data	HIGH	1	0	0	Medium
		Name	HIGH	1	0	0	Medium
		Online identifier	HIGH	1	0	0	Medium
c6	Data of a child	Cultural	LOW	1	0	0	Medium
		Economic/Financial	LOW	1	0	1	High
		Health	LOW	1	1	1	High
		Location Data	LOW	1	0	0	Medium
		Name	LOW	1	0	0	Medium
		Racial or ethnic origin	LOW	1	0	1	High
		Religious or philosophical beliefs	LOW	1	0	1	High
		Sex life or sexual orientation	LOW	1	0	1	High
		Social (Not metadata)	LOW	1	0	0	Medium

Figure 6-39 Data types and impact levels (e.g. c6's data scenarios)

Also, in the GDPR, economic/financial data is not listed as sensitive but in practice such compromised data can caused distress to the affected individuals e.g. as revealed by a victim, f8. Figure 6-40 p 166 shows f8, g7 and h5 data scenarios where low or high volume but not protected non-sensitive data were viewed as *Medium impact*.

Dashboard results: Data & Impact							
ID	Description of Incident	TypeOfData	VolumeOfData	DigitalForm (1:yes)	DataEncrypted or otherMeasures	TypeOfData sensitive (1:yes)	DataImpact Level
f8	Personal data from a stolen laptop	Economic/Financial	LOW	1	0	1	High
		Identification number	LOW	1	0	0	Medium
		Location Data	LOW	1	0	0	Medium
		Name	LOW	1	0	0	Medium
g7	Investigation of data loss	Economic/Financial	LOW	0	0	1	High
		Identification number	LOW	0	0	0	Medium
		Location Data	LOW	0	0	0	Medium
		Name	LOW	0	0	0	Medium
		Racial or ethnic origin	LOW	0	0	1	High
		Religious or philosophical beliefs	LOW	0	0	1	High
		Social (Not metadata)	LOW	0	0	0	Medium
h5	a near-miss email incident	Identification number	HIGH	1	0	0	Medium
		Name	HIGH	1	0	0	Medium

Figure 6-40 Data types and impact levels (e.g. f8, g7 and h5)

If low volume, non-sensitive data is protected, the likely impact is then *Low* in which case the ICO need not be notified. This is observed in Group2 stories. However, when it comes to DBI, usually more than one data type is compromised and usually involves sensitive data e.g. economic/financial data, which most organisations hold or process and which have intrinsic value to hackers/perpetrators. This is shown in Figure 6-36 p 164 and Figure 6-37 p 164 by the number of times this data was referenced.

Besides assessing the likely data impact levels, the data harm matrix also provided indicators for assessing the likely impact on *individuals*. Similar to *sensitive* data, *special* individual types are assigned

High impact. As shown in Figure 6-41 p 168, where the special *individual* is affected e.g. c6 and h5, impact on the individual is *High* and the question to notify or not the affected individuals is Yes. In scenarios b3, e3, f1, f8, g7 where no special individual is affected but there is *High* data impact, i.e. potentially high risk to individuals, they need to know. Where the data impact is *Medium* (risk) and no special *individual*, the answer is *No* as in o4's scenario. Individuals are notified if there is high risk (GDPR). However, as discussed in Section 6.7.2.4 on notification fatigue, o4 stressed the need to notify individuals. The dialogue with o4 (I) on the prioritisation screen indicated that the reputation of the organisation is also a criteria for notifying individuals.

C: ...an immediate assessment, it tells 'why' the reason, it tells you the likely impact, medium, because it's medium.

I: that's why you don't have to notify the individual.

C: but 'Do please notify the individuals as a matter of good business practice. Minimising distress to the individuals must be your first priority'... gives organisations a view.

I: I think that's helpful. Because that's actually where we felt we were. We had to be seen, if we didn't and they found out then it would reflect badly on our reputation.

As regards data sensitivities and the potential for distress, although the sensitivities are not shown on the prioritisation screen, c6/P, an experienced DPM noticed the *High* data impact:

*P: and this is driven by the **special categories**. Isn't it? The high ones. Because you know, it's special, therefore the **potential for distress and damage is going to be high**.*

C: does that make sense. Is that correct?

P: yup.

Beside c6/P, h9 in Group2 also remarked that the result '*has certainly the right outcome in terms of (his) relevant experiences*'.

However, the Dashboard also raised several remarks and discussions. With e2 (S), when asked whether the results make sense, he said '*yeah, nice*'. However, he needed clarification on *prioritisation* to which he was given this:

C: just like doing triage – do I treat you or not? Are you a serious case or not? Same concept in a different context.

C: Maybe I should say notify: Verify, assess but notify.

S: but sometimes you might not need to notify.

C: so – to notify or not – it still makes sense, ha?

S: indeed.

S: I'm still thinking...but we have prioritised it, this is the result. So what do we do next?

*C: that's a question you have to ask yourself. The research doesn't extend to – oh! Now you need to notify. This is the assessment, and this is a **guideline to show you the results** based on my own interpretation of all the sensitivities, on the nature of the data types (i.e. the GDPR reasons for the 'why?' as shown in Figure Z- 15 p 276 and Z- 16 p 276).*

S: yes.

ID	Dashboard results: Likely impact and notification							Pre-dashboard views		
	Description	individual record	Individual volume	Impact on individual	Data impact	Notify individual	Notify ICO	Notify individual (Q15)	Notify ICO (Q17)	Generic: case & notification fatigue (Q9)
b3	Unauthorised access to and stealing of personal client data	Customer/Client	HIGH	Medium	High / Medium	Yes	Yes	Yes	No	Neither agree nor disagree
c6	Data of a child	Child	LOW	High	High / Medium	Yes	Yes	No	No	Notify individual: case specific
c6	Data of a child	Customer/Client	LOW	Low						
e2	paper records left in a room	Customer/Client	HIGH	Medium	High / Medium	Yes	Yes	No	Yes	Notify individual: not case specific
f1	Phishing	Employees	HIGH	Medium	High / Medium	Yes	Yes	Yes (& spouses)	No (US)	Notify individual: not case specific
f8	Personal data from a stolen laptop	Customer/Client	LOW	Low	High / Medium	Yes	Yes	No	No	Notify individual: not case specific
g7	Investigation of data loss	Customer/Client	LOW	Low	High / Medium	Yes	Yes	No	Yes	Notify individual: case specific
h5	a near-miss email incident	Patient	LOW	High	Medium	Yes	Yes	Yes	No	Notify individual: case specific
o4	Email Phishing leading to data breach	Student/Researcher	HIGH	Medium	Medium	No	Yes	Yes	Yes	Notify individual: not case specific
o4	Email Phishing leading to data breach	Subscriber/Member	HIGH	Medium						

Figure 6-41 Group1 impact and notification

c6/K raised a concern:

*K: I think what would worry me slightly with what we went through is it essentially told us to notify the ICO and the individuals. So if you just did that **without any of the additional questions that we suggest** [she was unable to state these questions when asked], you would be notifying people of things that really there's no risk to them. In practice there is no actual risk.*

*P: because it's remedied. (However, to remedy, they do the assessment **first**, which is done by P as pointed out by K: we don't have a system to do it, it's P...).*

C: this is something perhaps I need to put a warning, that this is an initial triage. It's a prototype to test whether you can build a system.

K: Yeah yeah.

C: Then hopefully you tailor it according to your own organisation's way of handling incidents. Because I think all orgs have different way of handling.

P: yeah.

K: within our org, we would make it work. As you said you tailor it, you would tailor it, and make sure it's one of our team is completing it so we wouldn't just run off and notify the ICO instantly without that knowledge. But someone coming in this never having dealt with an incident before and just typing it all in, might literally get that. Ok, I need to notify the ICO and tell the individuals. It might cause distress in the long term.

C: yes, you're right. the system allows you to think, I am not saying you must notify,

K: laugh

C: that's why I got the question marks (as shown on the prioritisation screen for why?)

K: yeah

c6/K's fear stories are in contrast with g7's. When g7 saw the dashboard results he said this: *'as someone who had done this for quite a while, you would know instinctively that you would need to notify in this particular incident. But for those people that aren't quite that experienced or people operating in smaller organisations that doesn't have structure for information security. That's where this (Dashboard) comes in. Particularly for medium or small sized voluntary sector orgs, where one person is head of IT, risk and information security manager. This will help focus'*. However, c6/K noticed that the various bits of information collected during triage and in the Dashboard are useful for the notification message to the ICO. This was also noticed by g7, e2, f1 and f17. Both o4 and f1 notified the individuals without investigation and as soon as possible. b3's notifications to individuals were done after investigation and within 72 hrs. h5 was after investigation and outside 72 hrs. c6 said there was no obligation to notify the ICO (pre-GDPR).

6.7.3.5 Scenarios on privacy harm and breach notification: Group2 stories

The Group2 data scenarios stories are shown in Figure 6-42 p 170, and the impact and notification stories are shown in Figure 6-43 p 170. Although DashboardV2 has some new features as mentioned in Section 6.3.3, the data and individual impact assessment logic and approach are the same as for DashboardV1 used for Group1. For the confidence level: High means greater than or equal to 60%; Medium means less than 60%, greater than or equal to 30%, and Low means less than 30%. When b11 said High to *Individuals suffered distress*, it means he was High level confident that the individuals suffered Medium levels of distress as shown in Figure 6-42 p 170. He was also High level confident that his identified data types have been compromised i.e. Personal Data Compromised. The confidence level questions in DashboardV2 are shown in Appendix AA, Figure AA- 2 p 281 to AA- 5 p 282. Interestingly, b11's views on level of distress was Medium for a High privacy impact. His Dashboard results (Appendix AH, Figure AH- 4 p 294) indicated the impact on individuals is Medium (i.e. no *special* individuals in the TalkTalk case) and data impact is High/Medium as economic/financial data was compromised (Appendix AH, Figure AH- 2 p 293).

The main stories from Group2 that are not in Group1 are: instances where the scenarios have Low data impact (i.e. b12, b16, h9); mixed data form and their protection (i.e. b12, b16); different levels of harm and distress (in Group1, they are the same). In h9 scenarios there were policies for the paper records hence the data impact was Low. b11's stories on the TalkTalk incident were based on his experiences and what he heard in the news. According to b11, it was not clear whether the individuals and the ICO were notified. b16 and c10 notified the individuals after investigation and within 72 hours. l14 said No (individuals not notified) but then also said they were notified within reasonable time but not immediately. f17 performed the *primary step of quantifying/qualifying lost data – only communicate if presence of unprotected personal data confirmed*. For h9, the organisation chose not to notify the individuals but the ICO was notified. c10 contacted the ICO informally as it was not viewed as a privacy breach (pre-GDPR).

The data scenarios for b11, b12, b16 and h9 are shown in Figure 6-44 p 171. During the triage assessment of the data, b12 and b16 explained the way they handled data and their protection. For future iteration of the Dashboard one identified improvement is to enable such remarks to be captured.

Privacy harm & distress (Q13 & Q14)	Pre-dashboard: Level of impact			Dashboard		Confidence Level			
	High	Medium	Low	Likely impact on individual	Likely data impact	Individuals suffered distress	Personal Data Compromised	Volume of Data Compromised	Personal data protection & safety
The overall level of the actual, likely or could have impact of the privacy harm (harm) to the individuals whose personal data have been or may have been compromised.	b11			Medium	High/ Medium		High	High	High
	b15			Medium	High/ Medium		High	High	Medium
	b16			Low	High/ Medium/ Low		High	High	High
	h9			High	High/ Low		Medium	High	High
	l14			Medium	High/ Medium		High	High	High
	b13			High	High		High	High	High
	f17			Medium	Medium		Medium	High	High
			b12	Low	Medium/ Low		Medium	High	High
			c10	Medium	High/ Medium		High	High	High
The overall level of distress (for example, anxiety) that the individuals have or may have suffered as a consequence of the data incident	b15			Medium	High/ Medium	High			
	b16			Low	High/ Medium/ Low	High			
	h9			High	High/ Low	High			
	l14			Medium	High/ Medium	High			
	b11			Medium	High/ Medium	High			
	b12			Low	Medium/ Low	Low			
	f17			Medium	Medium	Low			
			b13	High	High	Low			
			c10	Medium	High/ Medium	Low			

Figure 6-42 Group2 level of impact – harm and distress

ID	Dashboard results: Likely impact and notification							Pre-dashboard views		
	Description	Individual record	Individual volume	Impact on individual	Data impact	Notify individual	Notify ICO	Notify individual (Q15)	Notify ICO (Q17)	Generic: case & notification fatigue (Q9)
b11	TalkTalk data incident	Customer/Client	HIGH	Medium	High/ Medium	Yes	Yes	No	No	Notify individuals: not case specific
b12	web service redirect vulnerability	Customer/Client	LOW	Low	Medium / Low	No	Yes	No	No	Notify individuals: case specific
b13	Student access restricted health records	Patient	LOW	High	High	Yes	Yes	No	No	Notify individuals: not case specific
b15	bank account at risk	Customer/Client	HIGH	Medium	High/ Medium	Yes	Yes	No	Yes	Notify individuals: case specific
b15	bank account at risk	Employees	HIGH							
b16	Stolen data	Employees	LOW	Low	High/ Medium / Low	Yes	Yes	Yes	Yes	Notify individuals: case specific
c10	Error in coding and lack of verification checking (printing)	Donor	HIGH	Medium	High/ Medium	Yes	Yes	Yes	No	Neither agree nor disagree
f17	USB stick lost on train	Customer/Client	HIGH	Medium	Medium	No	Yes	No	No	Notify individuals: case specific
h9	Paper record stolen	Child	LOW	High	High/ Low	Yes	Yes	No	Yes	Notify individuals: case specific
h9	Paper record stolen	Patient	LOW							
l14	Network perimeter was breached	Customer/Client	HIGH	Medium	High/ Medium	Yes	Yes	No	Yes	Notify individuals: not case specific
l14	Network perimeter was breached	Employees	HIGH							

Figure 6-43 Group2 impact and notification

ID	TypeOfData	VolumeOfData	DigitalForm (1:yes)	DataEncrypted or otherMeasures	TypeOfData sensitive (1:yes)	DataImpact Level	Note (Transcript)
b11	Economic/Financial	HIGH	1	0	1	High	
b11	Location Data	HIGH	1	0	1	Medium	
b11	Name	HIGH	1	0	1	Medium	
b11	Online identifier	HIGH	1	0	1	Medium	
b12	Identification number	LOW	1	1	0	Low	password (hashed protected)
b12	Name	LOW	1	0	0	Medium	username
b16	Economic/Financial	LOW	1	0	1	High	HR system
b16	Health	LOW	0	1	1	High	key locked
b16	Identification number	LOW	0	1	0	Low	key locked
b16	Location Data	LOW	0	1	0	Low	key locked
b16	Name	LOW	1	0	0	Medium	HR system
b16	Picture/Image/Video	LOW	0	1	0	Low	passport photo
b16	Racial or ethnic origin	LOW	0	1	1	High	key locked
b16	Religious or philosophical beliefs	LOW	0	1	1	High	key locked
b16	Trade union membership	LOW	0	1	1	High	key locked
h9	Cultural	LOW	0	1	0	Low	
h9	Health	LOW	0	1	1	High	
h9	Identification number	LOW	0	1	0	Low	
h9	Location Data	LOW	0	1	0	Low	
h9	Name	LOW	0	1	0	Low	
h9	Racial or ethnic origin	LOW	0	1	1	High	
h9	Religious or philosophical beliefs	LOW	0	1	1	High	
h9	Sex life or sexual orientation	LOW	0	1	1	High	

Figure 6-44 Data types and impact levels (e.g. b11, b12, b16 and h9)

6.8 What are the Users' stories? (RO4-h) (RO4-i)

The Users' stories are presented in Figure 6-45 p 172 and Figure 6-46 p 173. These stories were used for reflection in Chapter 7.

ID	<i>What improvements would you make to the dashboard?</i>	<i>In closing this study, what else would you like to add?</i>
b3	Need greater clarity on 'volume' metrics. Should be able to switch between the 'view' & 'recording' functions without having to exit and reload the dashboard.	It would be nice to be able to download and install the software with a single click.
c6	A section about initial response/actions taken and how that might affect risk gap between incident occurring and becoming aware of it (not usually at the time it happened). To be useful internally, a description of data (in helpline record) would be helpful. Ability to pull information out into a notification (standard) for the ICO Email/text alerts from system when nearing 72 hours.	None
e2	Interval alerts before 72hrs.	None
f1	A confidence % would be useful with regards to your knowledge of the facts of the case. This would then log a very strong story to the ICO about the decision-making for notification. A clock counting down 72 hours from time of awareness which would be entered, not just time of the event as it may be discovered quite sometime later.	
f8	overall, a very useful tool to help people record and assess an incident. It provides calm objectivity in times of panic and stress. Some of oral explanation given to me could be included in the form. Overall usability? Give it back to me in 3 months time a real working toolkit, to work through on my own. Then I will let you know.	This has great potential. Firms should want and value this. And, looking to the future, possibly an app for individuals to use if they think their personal data has been breached.
g7	Extra category regarding data supporting criminal investigation. Link to the ICO notification form – or even just reporting guidance. Where dealing with data over several categories, is there a way of bundling up answers so I don't have to click LOW, NO, NO for each of the 7 types?	Assumption this form would be hosted? Or available in the cloud? Also out of hours provision? E.g. I become aware of an incident at 6pm on Friday. To what extent could this be shared with data providers – e.g. the social care system hosted by someone is compromised – data processor finds out but doesn't tell data controller for 48 hours. Reporting for the Senior Information Risk Owner? Could the incidents page be exported in PDF format for consumption by steering groups? Already covered!
h5	There are some mechanisms in particular sectors/industries such as NHS(Health)/Banking and Telecomms. Based on existing ones, dashboard attributes/criteria can be improved by risk matrix. e.g. categories of volume method.	Correlation with Privacy Harm Risk Matrix.
o4	Could be developed to take you on to the next steps in the investigation and response.	No thank you.

Figure 6-45 Group1 users' remarks

ID	<i>In closing this study, what else would you like to add?</i>
b11	Easy to use during a crisis.
b12	Incidents Response is very important and logging incidents are not just beneficial for legal purposes but also for resolving the incidents. The dashboard is a very good centralized auditing system which can be used to log incidents and share knowledge of the incidents with the team and external stakeholders.
b13	Run a pilot with the enhanced features. Look at W29 articles for further enhancement.
b15	The quicker it can be transferred to organisations for their use the better.
b16	It is a very quick and easy to navigate system. My hypothetical scenario took only 5 minutes and 30 seconds to complete during first use therefore it is a quick dashboard – ideal for use by those with a hectic work schedule but need to find out answers within the time restraints. Upon reflection, it is possible to have both digital and non-digital formats of the same data therefore the question in the dashboard asking if there is non-digital data. This neglects the fact that there is both digital and non-digital. It would be helpful if there was some help text to direct users that a separate incident needs to be logged to cover both digital and non-digital in the prototype. Post prototype for a real system, maybe additions need to be made to include both for efficiency purposes.
c10	A good foundation for sound analysis of incident and the impact of incidents; further development of the tool could provide a very useful management decision-making and the technical aspects of incident response.
f17	For dashboarding at high level, fine as is. Maybe for future and to be able to make more relevant to different organisations, maybe some parameter-driven elements.
h9	I think this tool has huge potential to support organisations with a simple structured assessment in an area where there is little knowledge or understanding.
l14	As this is work in progress/a prototype, continuous improvement based on the answers from participants is key to the continuous modelling of the dashboard.
ID	<i>What improvements would you make to the dashboard?</i>
b11	Integration with other data inventory or asset management or CMDB.
b12	The dashboard is user friendly, easy to use and very clear. The menu options are simple and not confusing. It is great to have the incident alert which would be triggered after 72 hours.
b13	Allow summary of reported incidents and alerts assigned to management showing high risks. Use numbers and appropriate colors to show relative levels of risk.
b15	It is very pertinent to the solutions of a very important problem.
b16	No improvements – very clear and quick. Would like a printout of the summary screen.
c10	Expand the information gathering activities. Build intelligence into the dashboard – decision algorithm. A platform for further development – aiding or supporting analysis and decision-making, additionally more reporting capabilities for different categories e.g. technical team information.
f17	Internal comms: dashboard / questions talk about the data subject and the ICO – to support internal comms, need to also identify other interested stakeholders e.g. current client has an "Incident Response Team" and an "IT Security Group" that would also need to be notified immediately. Gathering of info: may be other forms of protection that could influence impact e.g. end-point encryption, file passwording or high-level questions such as "Is data aggregated?" Notification: Assumes 72 hour response? If acting as a processor, may need to respond more quickly to the controller so that they can meet their own deadline – so maybe need to be able to influence countdown. Overall: good, simple format – useful to support internal comms and audit evidence.
h9	As a deployed tool, it might be useful to have internal notifications sent automatically.
l14	Initial thoughts are that the dashboard is intuitive and provide the requisite checkpoints for recording all the relevant information to undertake an investigation. The questions prompt as well as direct the would be responder to think carefully and precisely about the answers to provide, as these drive the manner in which the output directs the responder to respond to the incident. Suggestions: 1) Alert notification could be more impactful i.e. appear in red or in bold, or provide the possibility of sending a text alert or email notification.

Figure 6-46 Group2 users' remarks

6.9 Summary of the stories

In summary some notable quotes from the Users are presented here. These stories were reflected on in Chapter 7.

6.9.1 Some quotes from the Group1 Users

f1: A **confidence %** would be useful with regards to your knowledge of the facts of the case. This would then log a **very strong story** to the ICO about the decision-making for notification.

f1: You can have very sensitive data and not much of it got leaked and you could have a lot of something that is less sensitive – medium sensitivity and it's still a matter of determination. And there is no guardian by ICO for example as to which one is a high, medium or low risk. **You've bring this forward**. So we came out with high – I agree. I agree in this case. But so **many grey areas**, aren't there?

f1: Get the **ICO** to do this and they should **build it into their website** so they really know what to do.

b3: Need greater clarity on **volume** metrics (& c10).

h5: Correlation with **Privacy Harm Risk Matrix**.

c6/K: if you going to notify the ICO, there is various information that you have to include in that notification, **you're putting that in anyway**, if you could pull it out into a template. It might be helpful.

C6/P: **information about the individual**, who may be identified by name or other factor, may be anonymous, but still identifiable. The individual who reported the concerns about the child.

c6/P: oh! **It's tracking**, that's interesting. c6/K: yes. Really interesting.

C6/P: **I do like checklists**. I do like it. **A framework for thinking**, which as a practitioner, you're doing but you don't always put it that. C6/K: **put it into that neat format**.

g7: **Extra category** regarding data supporting criminal investigation. **Link to the ICO notification form – or even just reporting guidance**.

f8: Overall, **a very useful tool** to help people record and assess an incident. **It provides calm objectivity in times of panic and stress**. This has **great potential**. Firms should want and value this.

6.9.2 Some quotes from the Group2 Users

c10: **Pulls it together nicely** (on the prioritisation screen).

b12: The **menu options are simple** and not confusing. It's great to have **the incident alert thingy, 72 hour thingy**.

b16: More about **how quick it is to do**, it only takes 5 mins of your time, but long term – 5 mins – **might save you when breached**.

b11: **Integration with data inventory**, data management and CMDB (Configuration Management Database).

b11: **Easy to use during a crisis**.

l14: **My issue is that you should be alerted** and an alert is there should be either a beep or some kind of flashing. I think really for me **the game changer** here is the fact you have the **72 hours window** so that really changes everything.

b15: It is very pertinent to the **solutions of a very important problem**.

*f17: Assumes 72 hour response? **If acting as a processor, may need to respond more quickly to the controller** so that they can meet their own deadline – so maybe need to be able to influence countdown.*
*Overall: **good, simple format – useful to support internal comms and audit evidence.***

Chapter 7 Reflection and Conclusion

This chapter completes the DSR reflection and conclusion activities and the knowledge contributions as shown by the red arrow in Figure 1-2 p 24. During the development and evaluation steps any limitations or constraints were identified and described during the relevant discussions about the interview study, DSR and UES. In any research study, there are limitations e.g. Fereday and Muir-Cochrane (2006) on coding and themes identified and analysed by one researcher to allow for consistency in the method but fails to provide multiple perspectives which require several individuals developing themes and discussions with other researchers. As multiple perspectives with other researchers were not pursued in this research, a list of assumptions and other limitations is identified in Section 7.3. The research implications are presented in Section 7.4. Firstly, Figure 7-1 p 176 provides a summary view of the research question (RQ), research objectives/sub-objectives (RO), activities conducted in Chapter 2 and 4 and on the findings in Chapter 6. This is discussed in Section 7.1. The research contributions (RC) are also mapped to the research objectives and are discussed in Section 7.2.

Research Aim (RA)	
To explore personal data incident (DBI) response, data privacy harms and breach notifications under the GDPR.	
Research Question (RQ)	
<i>How can a triage playbook be used to address data privacy harms for breach notification prioritisation during the initial response to a personal data incident?</i>	
Research Objectives/sub-objectives (RO)	Research Activities
(RO1) To examine the underlying concepts/principles/theories/approaches or rationales that are applied in the construction/design of the incident frameworks.	Literature review (Chapter 2)
(RO1-1) To synthesise existing incident frameworks/models or incident approaches.	Literature review (Chapter 2)
(RO1-2) To apply Peirce semiotics-ternary for the triage steps.	Application of Peirce ternary (Chapter 3)
(RO2) To gauge the extent and nature of DBI responses by organisations in the UK.	Interview Study (Chapter 4)
(RO3) To develop a triage playbook for organisations in the UK to assess privacy harm for breach notification during initial DBI response.	Design & Build Prototype Dashboard (Chapter 5) and 2 nd literature review
(RO3-1) To iteratively design and build the prototype dashboard (Dashboard) to address the initial breach notification question: <i>to notify or not affected individuals and/or the ICO?</i>	Design & Build Prototype Dashboard (Chapter 5)
(RO4) To validate the triage playbook using a prototype dashboard (Dashboard).	User Evaluation Study (UES) (Chapter 6)
Overarching Research Contribution (RC)	(RC) mapping to (RO)
This research's novel contribution is expanding the knowledge of how triage, checklists and a data matrix can be used to support organisations in the UK to address privacy harm to affected individuals for prioritising breach notifications during the initial response to a personal data breach incident.	
(RC-1) This research advances understanding of data privacy (data) harm to the individual as a consequence of data breaches.	(RO1), (RO1-1), (RO2), (RO3-1) and (RO4)
(RC-2) This research demonstrates a novel triage playbook for data harm assessment (PHA) to support quick breach notification (i.e. as required under the GDPR) during initial data incident response through a proof-of-concept and proof-of-use prototype dashboard.	(RO3-1) and (RO4)
(RC-3) This research illustrates the application of Peirce semiotics-ternary for contextualising the triage principles and the steps.	(RO1-2), (RO3), (RO3-1) and (RO4)
(RC-4) This research provides a pre-theory design playbook for initial data incident response through the use of checklists, triage principles (i.e. <i>first do no harm</i>), and a harm entities approach to data harm assessment.	(RO3) and (RO3-1)

Figure 7-1 Summary view of research question (RQ), objectives (RO) and contributions (RC)

7.1. Reflection

As shown in Figure 7-1 p 176, research objectives/sub-objectives (RO) were framed to address the research question (RQ), guided by the overall research aim (RA). To address RO1 and RO1-1, questions RO1-a, RO1-b, RO1-c, RO1-d and RO1-e (in Figure 2-1 p 30) were framed to conduct the SSM literature review (Chapter 2). Similarly, the interview study aims and the explanatory questions (in Figure 4-1 p 81) were framed to address RO2. Apart from Howard and Gulyas' (2014) research on data incidents, there is little research on DBI. Furthermore, PIA and breach notifications are new concepts (Custers et al., 2018), and existing DPIAs and PIAs or risk assessment approaches are not suitable for assessing privacy harm on individuals e.g. (Wright et al., 2013; Oetzel and Spiekermann, 2014; Poller et al., 2014; Wright and Raab, 2014). Hence an interview study was designed driven by the RA, and a set of explanatory questions (EQ1, EQ2 and EQ3 in Figure 4-1 p 81) was used to gather insights on DBI response. Hybrid thematic analysis (Section 4.3.3) was used to code and analyse the themes and report the findings.

From the SSM and interview study findings, (RO3) and (RO3-1) were framed to address the identified problem, namely organisations will need to conduct data privacy harm assessment (PHA) during initial DBI response to meet the GDPR breach notification requirements. A research gap was also identified, namely the lack of research on data privacy harm to affected individuals as a consequence of DBIs. The research then proposed a triage playbook solution and a visual prototype dashboard was designed and built (Chapter 5). The triage playbook was suggested as there is **currently no dedicated incident response framework in use by the interviewees** for responding to a DBI during the initial or early stages of incident response. Also, there are many incident response frameworks used in industry (Figures 4-13 p 97, L- 5 p 229), but when it comes to responding to a DBI, viewed as a crisis event, mostly ad hoc or non-formal, intuitive procedures were used. Furthermore, DBI response requires examining the privacy harm to the affected individuals in order to address the breach notification requirements especially in the GDPR era. In the GDPR era, ad hoc and/or not recorded formal response procedures may not meet the stringent breach notification requirements. Even in a large commercial bank with many frameworks and tools already place for handling security incidents, the interviewee (F16) said they will need to evaluate their procedures to address GDPR.

7.1.1 Why triage for DBI response?

Although there is no dedicated incident response framework for DBI, triage was mentioned by the interviewees (F1, E6, B9, B11, F12, F16, L19, O10, G15, C18, O20) and also by researchers (e.g. Brownlee and Guttman (1998); ENISA (2012); Hove and Tårnes (2013); Moser and Cohen (2013). Hove and Tårnes (2013) in referencing ENISA (2010), described triage as: *This stage consists of the three phases verification, initial classification and assignment*. There are many digital forensics frameworks (Section 2.2.5.2), but only Rogers et al. (2006) has mentioned triage in a digital forensics framework. Rogers et al. (2006) referred to triage in their framework as *speedy initial triage*. Furthermore, there is a lack of consensus in the digital forensics field regarding what exactly constitutes triage. Pollitt (2013) described: *triage is often understood as a way to maximise the use of scarce resources by prioritisation*. Even though triage has been used by CERT/CIRTs (Mundie et al., 2014), none of the reviewed literature outlined or operationalised the triage steps and/or the principles of triage as used in security incident response and

in digital forensics investigations. Hence, a sequence of triage steps i.e. verify, access and prioritise was formulated from a synthesis of existing security incident response activities (Figure 2-10 p 61) and from analysis of the working of triage as described by researchers in the medical domains (Section 2.2.6.1). The use of triage and the underlying ethical principles – *first do no harm* – as used in the medical domain (Enemark, 2008; Domres et al., 2010) were examined for addressing the nature of DBI response. In particular triage is used when the need to respond ethically with limited resources i.e. where time is of the essence to minimise, avoid or inflict harm to people during a crisis or disaster, appeared to be relevant for responding to a DBI.

Furthermore, interviewees have relied on using ad hoc approaches based on their intuition or experience or common sense to respond to their DBIs – viewed as a business crisis or a disaster (e.g. F4, H7, B9, B11, O10, F21). During DBIs, people panic or over react, ‘*all over the place*’ or were under time pressure to respond (e.g. B9, B11, F12, G15). According to Chen et al. (2007) in a crisis response where time is of the essence, reliable information is usually not available, and a decision needs to be made under conditions of uncertainty. This aptly described the conditions under which triage has been used to sort the wounded in combat or in emergency situations (Section 2.3.2). Interviewees viewed triage as intuitive and based on experience, and with systematic steps i.e. gathering and assessing information for actionable outcome. Moreover, the interview study also uncovered the fact that breach assessment indicators such as industry sector types and/or data or record types provided the thresholds that trigger and/or direct the types of response. The identification of the gap and a triage solution in the form of a visual prototype dashboard then led to the framing of the RQ and the formulation of RO4. With the completion of RO4, the RQ was addressed by the multi-method evaluation and the findings (UES in Chapter 6).

How the first study informed the second was shown by the use of DSR framework. This shows how the triage playbook was designed and built using a set of requirements identified from the literature review and the interview study as described in Sections 5.2 (high level requirements), 5.2.2 (checklists), and 5.2.7.1 (data types for privacy harm). The interview study also revealed that DBI requires a crisis response (i.e. speedy response with minimal information) and an outcome of using triage is actionable response (i.e. a solution that can be used quickly for initial DBI response to meet the 72hr notification requirements). The solution to address these issues were reflected in the design of the dashboard (Sections 5.3.2 and 5.3.3). This researcher could have stopped at the design stage (i.e. just the conceptual model) and not proceed to the build and evaluation (i.e. Action Research). As this research proceeded in building and evaluating the artefact (DSR), the first study (interview study) influenced the second study (UES) in terms of elicitation of the users’ requirements from interview study which informed the UES i.e. suggestion of a triage solution (artefact). As the UES was to evaluate the artefact, the interview study results – as embedded in the triage playbook – were used for the story plots (Section 6.6.2).

7.1.2 Why DSR and Peirce semiotics-ternary?

During the SSM literature review, DSR was identified as a systematic and rigorous research design approach. Based on the nature of the RA – being exploratory and with the focus on solving practical real-world problems – DSR and the underlying Peirce’s pragmatism theory provided the methodological and

theoretical lenses to address the RQ. Also, Peirce semiotics and ternary (semiotics-ternary) was adopted (Chapter 3) for formalising and rationalising the triage sequence of steps i.e. verify, assess and prioritise that was synthesised (Section 2.3.3) from the SSM study. The Triage Semiotics (Figure 3-4 p 70) provided a semiotic approach for PHA. As discussed in Section 3.1, finding a theory that addresses the practical or pragmatic nature of the phenomenon under observation requires finding a theory that can change with the changing nature of the phenomenon. Besides the need to address practical real world problem i.e. GDPR breach notifications (Section 2.2.2), this research needed a theory that can support or describe the privacy harm topologies (Section 2.2.4.1), visual modeling (Section 2.2.7.2), digital forensics and incident management approaches (Section 2.2.5) , including triage principles (Section 2.2.6.2). As this researcher is interested in visual modeling, visual communication theory (Section 3.1.1) was examined which led to the discovery of Peirce's semiotics. Peirce's semiotics and ternary (Peirce semiotics-ternary) (Section 3.1.2) have been used by researchers in various multidisciplinary settings including organisational, visual communication and modelling but not in security or personal data incident response. Furthermore, Pollitt (2013) in stating that triage is a practical solution, also highlighted the challenges with digital forensics investigation in our interconnected world. He called for a new forensics approach i.e. to seek better sociology paradigms. Although Everaert-Desmedt (2011) did not discuss sociology paradigms, the author stressed that Peirce's ternary of three categories of *Firstness*, *Secondness* and *Thirdness* is necessary and sufficient to account for all human experience. Interestingly, an interviewee (B11) also highlighted that a *new way of thinking* is needed in organisations when it comes to addressing privacy harm, the harm affecting their customers/clients.

One challenge in using Peirce semiotics-ternary for this research was that his ternary - being useful for accounting for all human experience - was a difficult subject to assimilate, especially as it has not been used or described extensively by security researchers or by privacy researchers.

7.1.3 Why is there a need to address privacy harm to affected individuals?

A real case story from the interview study:

F4 was directly involved in a DBI which involved fraudulent use of personal data taken from a laptop stolen from her house. Her personal data was used by fraudsters to buy goods from catalogue companies and used for utilities billing. She had to deal with mail order catalogue companies, home shopping companies, utility companies, credit card companies, personal credit scoring companies and bailiffs. The incident spread over two plus years, and when she complained and/or reported her case to the relevant authorities she was given the '*brush-off*'. She was told that because the incidents did not involve any direct financial loss to her, they were below their thresholds to get involved in. As a result of the lack of actions taken by the various companies, and also the relevant authorities, including the Police and Action Fraud, her personal credit rating was affected. The consequences of the DBI, although there was no direct financial loss, were that the indirect financial (from affected credit rating) and non-financial consequences caused nuisance, annoyance, and the whole episode of dealing with the various companies and authorities. This meant that she had to endure immense disruption to her personal and professional life.

'So, is it at risk of disrupting the privacy of that individual? The answer is yes, high, ...so it is high impact' (F4).

Other interviewees also shared their stories and concerns about privacy harm. In the GDPR era, victims or individuals whose personal data have been compromised have the right to claim for non-financial consequences e.g. distress – a privacy harm. For organisations, the potential litigations and compensation claims from affected individuals (i.e. the *human costs* as noted by C18) could potentially cripple them. In the interweaved and interlinked data world, where DBI is nuanced (Howard and Gulyas, 2014) as shown by the various incident data types (Figure L- 6 p 230) and DBI scenarios (Figures AG- 1 p 291, AG- 2 p 291), the impact of the privacy harm to affected individuals is *'tricky to measure'* (G15). For example: *'The harm threshold is completely different on the same types of data' (F21).; 'One piece of data might be very small but might have a high impact. And you got a huge volume of data ... but that's not impacting, so it's incredibly difficult' (F12).*

7.1.4 How to tackle a 'tricky to measure' privacy harm?

Researchers e.g. ittman et al. (2014), in recognising that measuring privacy harm is difficult, have suggested using alternative remedies, including digital ethics. In any risk assessments, there is the implicit assumption that we can firstly identify or categorise the risk event or the types of harm/damage. To quantify privacy risk or harm would require identification or tracing of the DBI that resulted or caused the harm. As shared by C18: *'because you can't trace the consequence to a single or even a set of events because data is data and it's all over the place'* especially in cyberspace. Although difficult to value or quantify privacy harm or the human costs, there is value attached to personal data as shared by the interviewees (e.g. F17, F21). However, an assessment approach (for prioritisation as well) was shared by an interviewee (F17), who pointed out that there was a relationship between the type of industry sector and the type of *'value'* attached to the lost or compromised data as perceived by the affected organisation. This sectorial and/or data type view were also shared by B3, H7, B9, O10, B11, F12, F16, C18 and F21. Also, interviewees (e.g. B9, O10, C14, G15, C18, O20, F17, F21) mentioned data types (Figure L- 6 p 230) and pointed out that some data types are more harming than others. These views provided a way to tackle the *'tricky to measure'* aspects of privacy harm. As risk is inherently subjective (Jahankhani, 2012), a simplified approach was adopted by drawing on the suggestion by De and Le Métayer (2016a) i.e. to separate the interests of the organisations (data controllers) and those of the individuals (data subjects). De and Le Métayer (2016b) outline a definition for privacy harm and acknowledge that *some subjectivity is unavoidable*.

Moreover, existing security risk assessment approaches are primarily driven by vulnerability indicators aimed at targeting risks to devices/systems (i.e. tangible harms). Privacy risk especially privacy harm assessment that focuses on the intangible such as distress – a type of a privacy harm as a consequence of a DBI – requires a different harm indicator approach as discussed in Section 5.2.7.2. One such harm assessment approach was discovered from the interview study namely the use of checklists during DBI response for gathering information and assessing the nature of the breach (B2, H7, B9, B11, B13, C14, C18, O20). These insights oriented this researcher towards examining checklists for privacy harm assessment for breach notifications.

As discussed in Sections 5.2.3 and 5.2.4, checklists have appeared in various research fields but there is little literature under DBI response. This research deployed checklists into a triage playbook conceptual model to enable prompt identification of the nature of the breach for decision support in prioritising breach notifications. In essence, checklists are a type of informational artefact – a conceptual model as used in the triage playbook accords with the detailed study on checklists by Reijers et al. (2017) and with the abstraction aspects for digital forensics frameworks (DFRWS, 2001; Beebe and Clark, 2005).

7.1.5 A data matrix to address a breach notification prioritising question: to notify or not?

In order to operationalise the triage playbook and to address (RO3) and (RO3-1), besides the creation of the triage semiotics (Figure 3-4 p 70), the triage entities (Figure 5-2 p 112), the conceptual model (Figure 5-3 p 113), the sequence of triage steps with the checklists (Figures N- 1 p 233, N- 2 p 234, N- 3 p 235), a data matrix (Figure O- 1 p 236) was also created. The outcome of (RO3) and (RO3-1) is a visual prototype dashboard that implemented the triage playbook. The dashboard instantiated the triage playbook with the triage sequence of steps to verify, assess and prioritise using the checklists of questions and answers and the data matrix to systematically, accurately and quickly perform the response steps and derive the data impact and individual impact levels (Section 5.3.2.1). The outcome of the triage addresses the breach notification prioritisation question: *to notify or not affected individuals and the ICO? (RO3-1)*. This final triage prioritisation question is relevant as when a DBI happened, the damage or harm was already done i.e. the genie was out of the bottle. In order to minimise further harm, speedy response (also as required under the GDPR) is required to ensure affected individuals were informed so that appropriate steps can be taken by the individuals. However, the conflicting GDPR breach notification requirements (Callahan, 2017) i.e. notification driven by high risk or risk of harm will likely create breach notification fatigue issues (discussed by BEUC (2011), ENISA (2011), Bolson (2014) and Esayas (2014)). The approach and rationale for the data matrix are summarised below:

- (a) The GDPR (2018) and the associated ENISA i.e. (ENISA, 2012; 2013) and ICO i.e. (ICO, 2012; 2018) reports/publications were the main sources for identifying the regulatory breach notification requirements and the entities as specified in the data matrix in Appendix O, Figure O- 1 p 236.
- (b) The breach scenarios and information driven by the triage sequence of steps and captured by the checklists of questions and answers were used with the data matrix (shown in Appendix O p 236), to derive the level of data impact and impact on individuals.
- (c) The data matrix provided the breach indicators, harm entities and pre-set parameters to derive the risk scores and the outcomes in terms of data impact and impact on individuals.
- (d) ENISA (2012) and ENISA (2013) have discussed the use of various privacy and security-related indicators but these have not been operationalised into practise or examined by privacy and security researchers.
- (e) There are numerous risk assessment methodologies, but there is no universal PIA framework which could be used for referencing or comparative privacy risk analysis. Even in the established information security risk domains, there is a lack in agreed reference benchmarking, as well as in

the comparative framework for evaluating information security risk methods and information security risk (Shamala et al., 2013).

- (f) As there is no benchmark data for privacy harm to individuals as a consequence of a DBI, and existing DPIAs and PIAs were not suitable for privacy harm assessment (Wright et al., 2013; Wang and Nepali, 2015; Article 29 Working Party, 2018), these papers: ENISA (2012; 2013); Harel et al. (2010); Liu and Terzi (2010); Best et al. (2017), were examined to expose their privacy scoring methods or approaches.
- (g) In particular, the intuitive privacy scoring properties/factors outlined by Liu and Terzi (2010) provided the basis for the data harm scoring approach adopted for this research, namely the notion *of sensitivity of data being revealed increases the data harm score* and hence the likely harm to individuals can be estimated and computed.
- (h) In order to estimate and compute the likely data harm, although the notion of sensitivity of data type, have been debated e.g. (Turn, 1976; Al-Fedaghi, 2007; McCullagh, 2007; Wang and Jiang, 2017), there is little research on the notion on special individual categories, except that mentioned in ICO (2018a) and CMS LawNow (2018). This research drew on Al-Fedaghi's (2007): *sensitivity is a notion that is hard to pin down as it seems to depend on the context, and this cannot always be captured in a linguistic analysis*. Hence, a heuristically set value of 100 was used for determining the high or low of affected individuals i.e. beyond 100 was considered as high. Note that in the GDPR, *high* – is undefined – to denote a risk level for rights and freedoms of individuals.
- (i) These researchers, Chen et al. (2007), Oetzel and Spiekermann (2012), Williams et al. (2017) and Savage (2017) have used simple high, medium, low labels for their privacy related measurements. To align with GDPR Article 33 and 34, the simple *high, medium, low* labels were used to show the likely level of data and individual impact (e.g. in Appendix Z, Figure Z- 15 p 276). These values then enabled decision support in terms of the prioritisation question: *why notify?* as shown against the GDPR requirements (Appendix Z, Figures Z- 16 p 276, 17 p 277).
- (j) Also, unlike indicators of threat or threat indicators or *indicators of compromise* (IOC) as discussed by Mell et al. (2006), Rowell (2017) and Williams et al. (2017), there are no formal descriptions or definitions for data harm i.e. data likely to harm individuals as a consequence of a DBI. Note the *negative impact of the use of the system on a data subject* in De and Le Métayer's (2017) description: *A privacy harm is a negative impact of the use of the system on a data subject, or a group of data subjects (or society as a whole) as a result of a privacy breach*. For addressing the concept of privacy harm, this research drew on the harm indicators description provided by Hinkel (2011).
- (k) Although there are privacy harm topologies and types of privacy harm e.g. Solove (2006) and Calo (2011), these are theoretical concepts (Fuchs, 2011) with little research on operationalising privacy harm in organisational contexts. This research addressed this gap with the data matrix implemented in the dashboards and evaluated with users in organisations.
- (l) The data matrix provided a pragmatic way to assess privacy harm such that early breach notification can be prioritised. Early breach notifications to affected individuals provide a means to minimise further harm.

7.1.6 Concluding remarks on research question (RQ)

As to whether triage is useful or appropriate for a crisis DBI response, these remarks by users during the evaluation of the dashboards (triage playbook) gave snapshot answers to the (RQ):

b11: *Easy to use during a crisis.*

f8: *This is going to be very useful. The big hit for me was, it gives me a chance to focus all that panic. It provides a calm objectivity in time of stress, panic of stress. Because you're going to be stressed, you immediately think your personal reputation and your organisation's reputation. Would we be fined & all these things come in rather than actual thinking of the consequences - and this helps you to get on the ground.*

Overall the two dashboards were well received by the UES users with mostly positive remarks for RO4 as shown in Section 6.5. However, as shown in Figure 6-17 p 148 there are three (i.e. b3, h5, c6) Group1 UES users who 'neither agree or disagree' on 'How useful is the dashboard?' Further supporting findings as revealed in Sections 6.6, 6.7 and 6.8, addressed the broad RA and showed how a triage playbook can be used to address data privacy harms for breach notification prioritisation during the initial response to a DBI (RQ). In addressing the RQ, the overarching research contribution was formulated and discussed next.

7.2 Contributions

The novel contribution of this research (RC) is an expansion of the knowledge of how triage, checklists and a data matrix can be used to support organisations in the UK to address privacy harm to affected individuals for prioritising breach notifications during the initial response to a personal data breach incident. The research contribution is broken down and discussed in terms of research objectives as outlined in the following sections.

7.2.1 Research contribution – (RC-1)

(RC-1) This research advances understanding of data privacy (data) harm to the individual as a consequence of data breaches.

Research objectives: **(RO1) (RO1-1) (RO3-1) (RO2) (RO4);**

The detailed SSM study **(RO1) (RO1-1)** and the second literature review **(RO3-1)** revealed that researchers have primarily focused on privacy harm or the risks to data and organisation (e.g. Clarke, 2013) or devices/systems (e.g. De and Le Métayer, 2016a; Williams et al., 2017). Existing security risk approaches (models and frameworks) and DPIAs or PIAs generally address the harm or risk to the organisation (e.g. Wright et al., 2013; Oetzel and Spiekermann, 2014; Wright and Raab, 2014; Poller et al., 2014). Furthermore, such security and privacy risk approaches are not suitable for assessing privacy harm on individuals as they are primarily driven by security CIA principles and IT governance policies/procedures. As pointed out by Calder and Moir (2009, p 97) IT Governance standards e.g. ISO/IEC 38500:2008 do not help organisations simultaneously to deploy any of the other standards or frameworks. The interview study also confirmed that existing security and privacy standards were not used. As regards DPIAs/PIAs, Article 29 Working Party (2018) also reinforced that *a different risk focus is needed for assessing the damage or harm to the data subject*.

According to Custers et al. (2018), PIA and breach notifications are new concepts. However, Esayas (2014), Bolson (2014) and ENISA (2011) have raised the challenges with data breaches, breach

notifications and notification fatigue. Although ENISA (2012) has a procedure for personal data breach handling (Figure G- 1 p 216) and ENISA (2013) made *more precise the levels of severity of a data breach* than in ENISA (2012), neither paper addresses privacy harm assessment to affected individuals.

Solove (2006), Calo (2011), Mulligan et al. (2016) and De and Le Métayer (2016a) have examined privacy harm and suggested models/frameworks or typologies but these have not been operationalised for organisations for addressing privacy harm to affected individuals during DBI response. De and Le Métayer have adopted different privacy harm definitions to address the context of their privacy harm research. However, in this research the notion of privacy harm is framed in terms of harm e.g. distress to affected individuals as a consequence of a DBI.

In summary the examined literature primarily focused on design and engineering, theoretical risk model or risk management, policy-making and not on the operational aspects. In the GDPR era, with the high penalties on organisations for data breaches, any privacy risk model will need to address harm to individuals and it can be operationalised for use by organisations.

This research contributed by addressing the gap, namely the privacy harm to individuals, and advanced understanding on privacy harm with the findings from a comprehensive interview study with 21 practitioners (interviewees) from different industry sectors in organisational settings **(RO2)**. Besides, such interview study has not appeared in the reviewed literature. The knowledge gained from interviewees covered not only the issues with DBI response and concerns on privacy harm but also insights into how organisations handled and responded to their DBIs. These led to a triage playbook solution which was operationalised or instantiated into two versions of visual prototype dashboards. These dashboards were iteratively designed and built **(RO3-1)** and validated with two groups of practitioners (i.e. eight Users in Group1 and nine Users in Group2) from diverse industry sectors **(RO4)**.

As existing privacy harm approaches have not been operationalised in organisational settings, **(RO3-1)** and **(RO4)** further contributed knowledge on the operational design, feasibility and utility aspects on privacy harm assessment (PHA) for initial DBI response.

7.2.2 Research contribution – (RC-2)

(RC-2) This research demonstrates a novel triage playbook for data harm assessment (PHA) to support quick breach notification (i.e. as required under the GDPR) during initial data incident response through a proof-of-concept and proof-of-use prototype dashboard.

Research objectives: **(RO3-1) (RO4)**;

In this research – which involved abstract concepts where there are no unequivocal rules or definitions for ‘personal data’ (Elliot et al., 2016), ‘data breach’ and ‘privacy’ (examined in Chapter 1) – Peirce’s pragmatism and the rigorous DSR approach were used to operationalise these concepts in a triage playbook and validate in real world situations. This was done in the context of data breach notification and DBI response in organisations in the UK under the GDPR. During the interview study, the GDPR was not the main focus but for the UES and the demonstration of the dashboards, breach notifications requirements under the GDPR were examined **(RO3-1)**. As the triage playbook has three conceptual components i.e. the triage sequence of steps, the checklists and the data matrix, the demonstration validated these conceptual components.

Although there are categories of privacy harm or damage e.g. physical, material or non-material (GDPR Recital 85) and various breakdowns of these harms (e.g. Solove, 2008; Calo, 2011; Solove and Citron, 2016; De and Le Métayer, 2016b), there is little research done on harms affecting individuals as a consequence of a DBI. Savage (2017) performed a preliminary characterisation of harms, focusing on genomic privacy from literature review and identified harms into four groups: harms to individuals; harms to relatives; harms to populations; harms to institutions (**RO3-1**). This research contributed understanding on the harms to individuals in terms of distress as a consequence of a DBI. As DBI is nuanced with diverse scenarios and different stakeholders, this research focused on the perspectives of organisations on privacy harm and breach notification during DBI response. Such data were captured via the interview study and the multi-method UES using two prototype dashboards.

The triage playbook was demonstrated with the prototype dashboards and used by practitioners (Users) (**RO4**). Users provided insights via an online questionnaire conducted using a facilitated, face-to-face and audio-recorded walkthrough using the dashboards (UES). The dashboards were used for proof-of-concept and proof-of-use of the triage playbook. The findings as outlined in Chapter 6 show how the triage playbook supported organisations to conduct PHA such that breach notification can be addressed and prioritised. As shown in Figures 6-30 p 161, 6-31 p 162, the triage durations for the diverse DBI scenarios are all completed in relatively short time (under 15 minutes) during the walkthrough. A user's remark on the *quick assessment and systems* (dashboard):

e2: Even with the ICO approach, remember this is uncharted waters in terms of this reporting functionality. Once you have systems like this place to be able to make a quick assessment as whether to notify or not. And you come to the decision to notify. They will not expect you to have all the details at hand straight away.

Although there exists little research on PHA for breach notification under the GDPR, *timely notification* can allow individuals *to take significant steps to reduce potential personal harm* (Rotenberg and Jacobs, 2013). This is because when a DBI happened, the genie was out of the bottle out in the wild, the harm was already done. Also, given that the *speed in which misuse of data* can take place, *any notification of breach must be timely to be effective* (Holm and Mackenzie, 2014). Moreover, organisations are required to notify affected individuals without undue delay and/or the ICO within 72 hours from first becoming aware of the breach (**RO3-1**).

The demonstration (**RO4**) also gained insight on how a practitioner (f1) in a large insurance organisation addressed the breach notification: '*We would **play** with the law to a degree to not notify until **our confidence factor** has got **to a certain level**. To me that's still part of verification*'. This insight contributed a new knowledge i.e. the use of confidence factors during DBI response. Confidence levels type questions and answers were added to the checklists for the second iteration with Group2. This also advanced the understanding of the use of checklists of questions and answers for PHA and DBI response. As the dashboard was designed to enable the user to stop/pause at any point during the DBI response from the start of logging to before the end of assessment i.e. the start of prioritisation, users can conduct the triage as many times as they want i.e. play with it (before the prioritisation) and also deleting the incident and starting again until they are confident with the outcome. Each triage of the same data incident will have different outcomes if the answers to the checklists are different. The only limiting legal

factor is the need to respond within 72 hours or without undue delay and the dashboard provides an alert to support this such that prioritising i.e. to notify or not? affected individuals and/or the ICO can be addressed.

Although researchers have not used checklists for PHA or for DBI response, checklists and confidence level¹⁸² have appeared in an industry GDPR whitepaper (Alienvault.com, 2018). The checklists enabled the diverse DBI scenarios to be captured for prompt identification of the nature of the breach. The captured breach information was used alongside the scoring parameters as defined in the data matrix to derive the level of data harm and the level of harm to individuals. Such captured and collected breach information (in the Dashboard and extracted into Excel sheets) provide a rich set of incident data which can be used for future research on privacy harm on affected individuals, including from perspectives of affected individuals or from other stakeholders e.g. the ICO.

McCullagh (2007) raised this: *Is it possible to formulate **an objective category of sensitive information despite claims that sensitivity is relative to the individual**; and a function of the **context** in which the information is used rather than the type of information itself?*. The demonstrated triage playbook showed that in the context of DBI response, there is a pragmatic way to categorise the sensitive personal data types relative to the individuals by formulating also the individual record types. As organisations are held accountable for the safe keeping of personal data (identifiable to a data subject/individual) and when a data breach occurred, they have a legal duty to notify the affected individuals. Hence the context of data harm, e.g. distress on the affected individuals, is from the intuitive and/or subjective perspective of the organisations. Furthermore, distress is a recognised non-pecuniary harm in the UK Court under DPA 1998 in Google vs Vidal-Hall 2015 case.

Besides showing the conceptual working (proof-of concept) of the triage playbook, a list of high-level personal data types (Figures 6-36 p 164, 6-37 p 164), individual record types (Figures 6-34 p 163, 6-35 p 163), and the breach information parameter-driven scoring approach for data harm (Figure O- 1 p 236) were also validated (proof-of-use) and snapshots of the outputs are in Appendix AH p 292. These data harm entities contributed to understanding of sensitivity of personal data in relation to the special categories of individual records. In terms of data harm e.g. distress, the notion of *sensitivity of data being revealed* (Liu and Terzi (2010) (*i.e. unprotected*) *increases the data harm score* and hence the likely distress to individuals can be estimated.

Although the security status of the compromised data is relevant in terms of breach notification under the GDPR, when it comes to breach notifications, there was consensus by interviewees that breach notification to their customers/clients was seen as the *right thing* to do. However, the findings from the UES show that although it was the *right thing to do*, users (included interviewees) revealed (pre-dashboard) their decision to notify individuals and the ICO were based on their subjective views of what is a breach (with the identification of a breach scenario) and their notions on privacy harm and distress. These findings can be captured using the labels high, medium, low as shown in Figures 6-38 p 165, 6-42 p 170. Such a simple labelling approach also enabled the likely level of data impact and impact on individuals to be shown.

¹⁸² The question in the whitepaper: 'What level of confidence do you have in your security tools?'

Similarly, on breach notification and notification fatigue (Figures 6-28 p 159, 6-29 p 159, 6-41 p 168, 6-43 p 170) the pre-dashboard findings indicated that the decision to notify – to notify or not? – is case or incident specific. The outcome of the triage playbook provided decision support during DBI response as shown on Appendix T, Figures T- 13 p 251 to 16 p 252. However, some users (e.g. f1, e2, o4, f8) expressed that irrespective of the GDPR and/or without detailed investigation (i.e. as soon as possible), individuals should be notified (Section 6.7.2.4). However, the reputation of the organisation was also a criterion for notifying individuals.

The open remarks from users during the UES walkthrough provided insightful knowledge not directly addressed or asked in the dashboard or in the questionnaire. For example, several users (e.g. e2, c6, b3, g7, h9, b12, b11, b13, b15, c10) expressed their ‘likes’ or interests when they saw the dashboard display and the workings of the triage sequence of steps and the checklists. The dashboard also captured not only *what is good* but also *what is bad about an idea* (Omar, 2014). For example, the concerns expressed by c6/K on the dashboard (Section 6.7.3.4) and by o4 on notification fatigue (Section 6.7.2.4).

In essence the dashboards provided an effective, interactive and tangible system to capture users’ experiences (e.g. Naumann and Jenkins (1982)) and deeper insights on the sensitive topics i.e. privacy harm and breach notifications. The use of the dashboards, besides proof-of-concept and proof-of-use of the triage playbook, also contributed knowledge on the use of low fidelity and pragmatic design concepts for display of appropriate notification alerts, electronic checklists and triage principles.

In terms of DSR knowledge types (Figure A- 3 p 209), the triage playbook contributed to definitional, descriptive and predictive knowledge.

7.2.3 Research contribution – (RC-3)

(RC-3) This research illustrates the application of Peirce semiotics-ternary for contextualising the triage principles and the steps.

Research objectives: **(RO1-2) (RO3) (RO3-1) (RO4);**

Peirce semiotics and ternary (Peirce semiotics-ternary) have been used by researchers in various multidisciplinary research (Section 3.1.2) but not for privacy harm, DBI response or triage. This research contributed in using Peirce semiotics-ternary and for structuring and contextualising the various descriptions, concepts and principles of triage into a sequence of steps i.e. verify, assess, prioritise **(RO1-2)**. These steps were formulated during the SSM study (Sections 2.3.2; 2.3.3) and shown in Figure 2-11 p 61 and 3-4 p 70. The stages of the creation of the triage steps and the DBI response activities are reflected in Figure 2-10 p 61, 2-11 p 61, 3-4 p 70, 4-14 p 101 and 5-2 p 112.

The iterative design and building of the prototype dashboards **(RO3) (RO3-1)** contributed micro-evaluations or testing/verification (Vaishnavi et al., 2017) of the triage playbook. The multi-method UES with practitioners **(RO4)** contributed towards understanding of the applicability or utility of the theoretically derived and synthesised (from existing knowledge bases or literature) triage steps and DBI entities. As shown in Figure A- 3 p 209, applying Peirce semiotics-ternary contributed a descriptive knowledge.

7.2.4 Research contribution – (RC-4)

(RC-4) This research provides a pre-theory design playbook for initial data incident response through the use of checklists, triage principles (i.e. *first do no harm*), and a harm entities approach to data harm assessment.

Research objectives: **(RO3) (RO3-1);**

In developing a triage playbook **(RO3)** - using the iterative RITE approach **(RO3-1)** (Sections 3.5 and 5.4) and the DSR method for describing the artefacts and outputs (Section 3.4) – contributed to understanding of the application of DSR and the pre-theory design framework (Baskerville and Vaishnavi, 2016) (Figure 3-11 p 77). As far as this researcher is aware there is little research on the use of DSR in DBI response and privacy harm research domains. The triage steps and checklists (Appendix N, p 233) and the data matrix (Appendix O, p 236) could be enhanced e.g. with more levels of checklists and harm entities such that the pre-theory design playbook could evolve into a design theory triage playbook.

7.3 Limitations and assumptions

This research addressed privacy harm as a consequence of a DBI i.e. compromised personal data that may harm affected individuals. Although technologies can create or result in privacy harm to individuals, this research only examined personal data that can cause harm – not the technologies – and in the context of breach notifications under the GDPR. Also, GDPR was not examined for addressing technologies or the impact of fast technologies on the GDPR¹⁸³. However, security researchers have started discussions on AI ethics, privacy and accountability as expressed in the GDPR (Abrams et al., 2019). Although not in the context of DBI response, Abrams et al. (2019) highlighted that as these AI applications proliferate, the possibility of tangible harm becomes more likely, and stressed that *organisations will need to understand and evaluate data processing and how it might benefit or harm those associated with these data*. In terms of security incidents, Cormack (2016) stressed that incidents are *rarely visible to their victims until significant harm is done. The fact that someone has access to sensitive personal information may only become apparent when that information is published or otherwise misused*. Hence under GDPR, the onus is on organisations who process the protected personal data to conduct harm assessment during initial DBI response and notify affected individuals. This research is limited to assessing the privacy harm from the perspectives of organisations, i.e. harm to affected individuals due to the compromised personal data in a DBI.

7.3.1 Limitations

This researcher is based in London with easy access to offices or headquarters of organisations across a range of industry sectors. Hence London provided the base for conducting the interviews and the UES of this PhD. In an ideal situation, other cities in UK besides London would be added to the sample population and the 21 interview samples and the 17 UES samples would be extended. However, as highlighted by Ritchie et al. (2014, p 117) *if the data are properly analysed, there will come a point where very little new evidence is obtained from each additional fieldwork unit*. Almost all the industry sectors were represented in the final list of industry sectors i.e. interviewees' profiles (Figure L- 1, L- 3 p 227); UES

¹⁸³ GDPR is non prescriptive and is supposed to be technologically neutral.

users (Figure 6-11 p 144). As only a few participants (i.e. interviewees and UES users) were from the legal/justice and public sectors, the results from this research are not generalisable across these sectors. The sample populations covered large or global, medium, and also small sized organisations, and represented professionals and practitioners in the fields or domains related to the research themes. This provided the *depth of observation* contained in the interview and UES data, besides the *range* and *number* as suggested by Guest et al. (2017).

Given that there was little research on the multidisciplinary research themes – as shown by the thorough SSM literature review – there was little guidance on the overall interview approach and the sampling approach for this qualitative research. Hence a pragmatic, structured and purposive sampling approach (Appendix H, H-3 p 218) drove the overall selection and sampling of the population for the interview and also for the UES. Moreover, the purpose of the interview study was not to understand phenomena deeply or in detail, i.e. not to discover theory in data or for theoretical sampling or for generalising across industry sectors. Instead the intended outcomes of the interviews were to support and/or to inform further study. Although rigorous hybrid TA were conducted using explanatory questions to drive the final analysis and reporting of the themes (Section 4.3.3.6), no independent reviewer was involved in validating or testing this researcher's themes. Independent reviewers were recommended by Miles and Huberman (1994) and further discussed by Alhojailan (2012). The limitations in TA was also raised by Fereday and Muir-Cochrane (2006). Another limitation is that the TA itself lacks a semiotic interpretation.

The final reporting in Chapter 4 and the discussions in Chapter 6 would be more reliable and better informed if such additional themes review was conducted. Even so, there are limitations and invariably biases introduced in conducting the interviews and in the UES. Furthermore, due to the sensitive nature of this research themes, organisations were reluctant to share or talk about their DBIs. For example, this researcher approached TalkTalk but was unable to get any response. Companies such as TalkTalk who had a data breach that could have contributed to the sample population were not represented. Hence, the reports on the TalkTalk DBI response by other interviewees are not fully conclusive. Also, of those who participated, not all interviewees have direct or recent experiences in DBI response, hence compromising the reliability or dependability of the analysed interview and UES data.

Having identified these key limitations, and recognising the nature and various limitations of qualitative research e.g. *No attempt is made to assign frequencies to the linguistic features; Ambiguities, which are inherent in human language; The main disadvantage is that their findings cannot be extended to wider populations* (Atieno, 2009), a list of assumptions is outlined in Section 7.3.2. However, in combination with the detailed SSM literature review, the application of Peirce semiotics-ternary, the use of DSR and multi-method UES should ensure the validity and reliability of the overall research activities and studies.

7.3.2 Assumptions

- (a) The application of Peirce's ternary i.e. *Firstness*, *Secondness* and *Thirdness* for exploring and describing the triage sequence of steps aligns with the descriptive knowledge types as outlined in knowledge types and forms in Johannesson and Perjons (2014, p 21-28). The automation of the

checklists of questions and answers and the incorporation of the checklists into the triage steps constituted the prescriptive knowledge for the triage playbook during initial DBI response.

- (b) The constructed data harm matrix was appropriate for use by organisations in the UK during initial DBI response. The data harm matrix used existing definitional knowledge extracted from the GDPR, and similar prescriptive knowledge for the scoring approach as done in ENISA (2012) and ENISA (2013).
- (c) Any apparent or perceived biases in the selection of the themes and the coding as used during hybrid thematic analysis (hybrid TA) in the interview study and the User Evaluation Study were unintentional or unconscious acts of this researcher. Some amount of *subjectivity in the form of personal bias or opinion inevitably creeps into the (research) process* (Freund and Jones, 2015, p 18). Such biases were avoided or minimised by clearly documenting the coding steps and research approaches.
- (d) This research is mostly qualitative in nature and involved topics that are sensitive in nature with diverse stakeholders. Although terms and concepts are described and also documented in the glossary, this researcher recognises that there are subjective interpretations when it comes to privacy risks and privacy harm. Hence any measurements and parameters as pre-set in the data matrix and the findings are also open to further subjective interpretation. This subjective interpretation is also captured by Peirce semiotics-ternary.
- (e) The triage playbook conceptual model (Figure 5-3 p 113), faithfully represented the scope and context of this research.
- (f) The triage playbook components (Section 5.1.1) were *good enough* representation. Peirce's abductive logic, Peirce semiotics-ternary and the good enough pragmatism (Vaishnavi et al., 2017) provided the underlying theoretical basis for explaining and justifying the phenomenon investigated in this research.
- (g) The prototype dashboard was a *good enough* instantiation of the triage playbook conceptual model.
- (h) The triage playbook constituted a pre-theory design framework based on Baskerville and Vaishnavi (2016).
- (i) The prototype dashboard, namely the two tested and evaluated versions, were considered DSR artefacts and hence provide potential building blocks for further DSR theory building studies.
- (j) The artefacts i.e. the triage entities, the triage sequence of steps, the triage playbook conceptual model, the checklists of questions and answers, and the data harm matrix contributed to the domain knowledge of PHA, breach notifications and DBI response under the GDPR.

7.4 Implications for practice

DBIs are nuanced with diverse stakeholders across industry sectors as shown by the findings in Chapter 4, e.g. Figures 4-7 p 89 and 4-12 p 96, and Chapter 6, e.g. Figure 6-11 p 144, Figure AG- 1 p 291 and AG- 2 p 291. Any data harm metric has to strike a balance to address the diverse stakeholders' perspectives or views on the various data harm entities i.e. personal data types and categories of individual records, the volume of compromised data and security measures/protection. Also, the checklist

of questions and answers and the pre-set data harm entities and parameters would need to address the various description and interpretation for personal data, data breach and data harm. In adopting a pragmatic approach and drawing on research conducted on personal data and data harm, the triage playbook was shown to be useful to users during DBI response as shown by the findings in Chapter 6. For example, in Section 6.5.2 where the majority of the users from both groups of the UES indicated *strongly agree or somewhat agree* or without any disagreement to the raised questions on the usefulness of the dashboard.

Furthermore, a company expressed interest in developing the prototype dashboard into a commercial product. When this happened, besides the knowledge contributions as outlined in Section 7.2, a practical implication for organisations in the UK is that they would have access to a triage playbook designed specifically for addressing privacy harm such that breach notification can be prioritised during initial DBI response. Besides, in the GDPR era with high breach fines, organisations can no longer ignore the consequences of not reporting the breach to the ICO and in certain cases to notify the affected individuals. With the use of the triage playbook, organisations should be better prepared (unlike the TalkTalk DBI, October 2015) for responding to a DBI. At present, very few organisations (16% of businesses and 11% of charities) have formal cyber security incident management processes in place (Vaidya, 2019). Commercialisation of the triage playbook solution will help to address this gap. However, without the industry practitioners' participation, the triage playbook – one that addresses the business needs or solves real-world problems – would not have been conceived and implemented.

7.5 Suggestions for further research and concluding personal remarks

7.5.1 Further research

The following is a list of identified suggestions from the UES findings (Sections 6.8 and 6.9) for further research.

- (1) More checklists to gather more information and reporting for other incident teams (e.g. technical teams) (c10).
- (2) Provide parameter-driven elements (instead of the pre-set matrix) or business intelligence functionalities to enable customisation by organisations (f17, c10).
- (3) Provide integration capabilities e.g. to other data inventory or asset management or configuration management databases (b11).
- (4) Incorporate other privacy harm risk matrix (h5).
- (5) Integrate/develop investigative steps/processes i.e. post triage investigative response steps (o4).
- (6) Develop a triage app for use by individuals to check/assess whether their personal data has been breached (f8).
- (7) Improve the display (e.g. use sound/flashing, levels of alerts) of the notification alerts (l14, b13).
- (8) Provide interval notification alerts before 72 hrs (e2).
- (9) Automate/provide/integrate notification alerts to internal communications (h5).
- (10) Provide recording of actions taken and free text fields for user to describe the data (c6).

- (11) Export the information for ICO (c6, g7).
- (12) Export the information for reporting to other stakeholders e.g. for Senior Information Risk Owner (SIRO) (g7); for senior managers with alerts assigned (b13).
- (13) Capture more information on other forms of protection and check if the data is aggregated (f17).
- (14) Provide notification to other interested stakeholders (f17).
- (15) Provide separate checklists for non-digital data (b16).

The above identified suggestions for improvements also provide opportunities for future research. In particular, the data harm entities in the pre-set matrix could be improved to include more levels of difference, types of personal data and individual types. More checklists of questions and answers could be formulated such that these are driven and customisable by the users instead of by the pre-set data matrix.

As there is currently little research on privacy harm on individuals as a consequence of a DBI, further research is required to gather more information from the perspectives of the victims of DBI. The additional data harm information will enable a more comprehensive and elaborate data matrix. As there are diverse DBI scenarios and each breach is complex, the checklists and the data matrix would need to capture the nuances of DBI. This research provides a foundation for future researchers to develop a more complex data matrix and the use of checklists such that comprehensive privacy harm rules engines or algorithms or AI can be designed to automate the breach assessment and breach notifications to relevant stakeholders, including affected individuals. In order to design any privacy harm rules, the conceptual challenges of privacy and what constitutes harm from the perspectives of the various stakeholders will need to be addressed. In this research, the breach notification rules were driven by the GDPR breach notification requirements and the privacy harm to affected individuals were from the perspectives of organisations. The triage playbook i.e. the dashboard captured relevant breach information and can be enhanced to automate initial breach notification to the ICO¹⁸⁴. Future research needs to include the ICO such that speedy notification can be achieved via direct automatic notification which will ensure minimal harm to affected individuals can be realised. Currently breach notification to the ICO is done via download of an online form or via phone calls during office hours¹⁸⁵.

Also, in the race to address the various online and related social media harms or harms from *user-generated content*, policy makers (DCMS, 2019) have taken actions with the publication of a white paper - *Online harms*¹⁸⁶. Researchers need to join the race and help to shape and influence the issues identified by policy makers with pragmatic and sustainable ethical solutions in our ever-changing technological landscapes. As pointed out by Trope (2019) in a survey on concealment of major cyber incidents, cyber incidents became corporate ethical crisis.

¹⁸⁴ The ICO was contacted but did not participate in this research.

¹⁸⁵ <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/> [Accessed 1-May-2019].

¹⁸⁶ Directed on regulating all companies of all sizes dealing with user-generated online content i.e. text, image, video, audio with the aim to protect child-safety online.

7.5.2 Concluding personal remarks

This researcher went through several unwelcome changes and disruptions i.e. personal and academic challenges with supervisors and departmental changes. Even half-way into the interview study, Brexit cropped up and questions on the relevance of GDPR were raised/discussed (e.g. B13 and F17). Brexit will not change GDPR. Furthermore, the UK has implemented GDPR into UK laws¹⁸⁷ (Woods, 2017) without any changes to the core data principles and the breach notification requirements. As long as GDPR remains enacted, the outcomes from this research will remain relevant within the defined scope of this exploratory research.

If this researcher could start all over again, a dashboard would be developed and built using visualisation tools and techniques.

Throughout the duration of this research, besides this researcher's motivated interests, one message from Prof. Kevin Jones (initial supervisor) – *stretch the boundary* – stuck throughout this PhD. His message resonated with this researcher's own motto – *make a difference* – in any undertakings. Invariably there will be challenges in pursuing any research, so a final remark to future researchers – have perseverance and most importantly be humble.

¹⁸⁷ UK DPA 2019 and UK-GDPR for Brexit scenarios.

References

- Aacharya, R. P., Gastmans, C., & Denier, Y. (2011). Emergency department triage: An ethical analysis. *BMC Emergency Medicine*, 11.
- Abrams, M., Abrams, J., Cullen, P., & Goldstein, L. (2019). Artificial Intelligence, Ethics, and Enhanced Data Stewardship. *IEEE Security & Privacy*, 17(2), 17–30.
- ACPO. (2012). ACPO Good Practice Guide for Digital Evidence. 5.0. (UK). <http://www.digital-detective.net/acpo-good-practice-guide-for-digital-evidence/>. [Accessed 30-December-2018].
- ACSC. (2018). Data Spill Management Guide. Australian Government, Australian Cyber Security Centre. https://acsc.gov.au/publications/protect/Data_Spill_Management_Guide.pdf [Accessed 30-December-2018].
- Agarwal, A., Shankar, R., & Tiwari, M. K. (2006). Modeling the metrics of lean, agile and leagile supply chain: An ANP-based approach. *European Journal of Operational Research*, 173(1), 211–225.
- Akhtar, J., Koshul, B.B., and Awais, M.M., 2013. "A Framework for Evolutionary Algorithms Based on Charles Sanders Peirce's Evolutionary Semiotics." *Information Sciences* 236: 93–108.
- Ahmad, Arniyati. (2016). A cyber exercise post assessment framework: In Malaysia perspectives. University of Glasgow.
- Albrecht, J. P. (2012). Draft report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf [Accessed 30-December-2018].
- Alienvault.com. (2018). GDPR Compliance Checklist. Alienvault.com. https://www.alienvault.com/docs/whitepapers/gdpr-compliance-checklist.pdf?utm_internal=compliancegdprlookbook&x=lcc-kv&xs=13165 [Accessed 11-October-2018].
- Alhojailan, M. (2012). Thematic analysis: a critical review of its process and evaluation. *West East Journal of Social Sciences*, 1(1), 39–47.
- Al-Fedaghi, S. (2007). How Sensitive is Your Personal Information? In *Proceedings of the 2007 ACM Symposium on Applied Computing* (pp. 165–169). Seoul, Korea: ACM.
- Al-Fedaghi, S. A., & Thalheim, B. (2008). Databases of Personal Identifiable Information. In *Signal Image Technology and Internet Based Systems, 2008. SITIS '08. IEEE International Conference on* (pp. 617–624).
- Alshammari, M., & Simpson, A. (2018). Towards an Effective Privacy Impact and Risk Assessment Methodology: Risk Assessment. In S. Furnell, H. Mouratidis, & G. Pernul (Eds.), *Trust, Privacy and Security in Digital Business* (pp. 85–99). Springer International Publishing.
- Alturki, A., & Gable, G. G. (2014). Theorizing in design science research: An abstraction layers framework. Presented at the Proceedings - Pacific Asia Conference on Information Systems, PACIS 2014.
- Amer, M., Daim, T. U., & Jetter, A. (2013). A review of scenario planning. *Futures*, 46, 23–40.
- Amrollahi, A., Lukyanenko, R., & Castellanos, A. (2017). Multi-Paradigmatic Theorizing: Mixing Design and Exploration. *AMCIS*.
- Article 29 Working Party. (2018). *Guidelines on Personal data breach notification under Regulation 2016/679* (Guidelines). EU: European Union. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 [Accessed 5-September-2018].
- Asokan, N. (2017). Ethics in Information Security. *IEEE Security & Privacy*, 15(3), 3–4.
- Åsvoll, H. (2014). Abduction, deduction and induction: can these concepts be used for an understanding of methodological processes in interpretative case studies? *International Journal of Qualitative Studies in Education*, 27(3), 289–307.
- Atieno, O. P. (2009). An analysis of the strengths and limitation of qualitative and quantitative research paradigms. *Problems of Education in the 21st Century*, 13(1), 13–38.
- Attride-Stirling, J. (2001). Thematic networks: an analytic tool for qualitative research. *Qualitative Research*, 1(3), 385–405.
- Auchard, E. (2015). TalkTalk cyberattack: who, what and why? | Reuters. <http://uk.reuters.com/article/2015/10/23/uk-talktalk-cyberattack-questions-idUKKCN0SH27E20151023> [Accessed 30-December-2018].
- Audi, R., 1999. *The Cambridge Dictionary of Philosophy*. Second. Cambridge University Press 1995, 1999.
- Baggini, J., & Stangroom, J. (2004). *Great Thinkers A-Z*. London: Bloomsbury UK.
- Barber, M. (2009). Questioning scenarios. *Journal of Futures Studies*, 13(3), 139–146.
- Barbosa, O., & Alves, C. (2011). A systematic mapping study on software ecosystems. *Proceedings of the Workshop on Software Ecosystems, IWSECO-2011.*, 15–26.
- Barreiros, E., Almeida, A., Saraiva, J., & Soares, S. (2011). A Systematic Mapping Study on Software Engineering Testbeds. *2011 International Symposium on Empirical Software Engineering and Measurement*, 107–116.
- Barron, T. M., Chiang, R. H., & Storey, V. C. (1999). A semiotics framework for information systems classification and development. *Decision Support Systems*, 25(1), 1–17.
- Baskerville, R. L., & Stage, J. (1996). Controlling Prototype Development through Risk Analysis. *MIS Quarterly*, 20(4), 481–504.

- Baskerville, R., & Vaishnavi, V. (2016). Pre-theory design frameworks and design theorizing (Vol. 2016-March, pp. 4464–4473). Presented at the Proceedings of the Annual Hawaii International Conference on System Sciences.
- Baur, A. W. (2017). Harnessing the social web to enhance insights into people's opinions in business, government and public administration. *Information Systems Frontiers*, 19(2), 231–251.
- BBC News. (2016). *TalkTalk profits halve after cyber attack*. <http://www.bbc.co.uk/news/business-36273449> [Accessed 30-December-2018].
- BCI. (2014). *Horizon Scan 2014*. <https://www.thebci.org/resource/horizon-scan-2014.html>. Report not available online [Accessed-30-December-2018].
- Becker, J., Rosemann, M., & von Uthmann, C. (2000). Guidelines of Business Process Modeling. In W. van der Aalst, J. Desel, & A. Oberweis (Eds.), *Business Process Management* (Vol. 1806, pp. 30–49). Springer Berlin Heidelberg.
- Beebe, B. (2003). Semiotic Analysis of Trademark Law. *UCIA I. ReV.*, 51, 621.
- Beebe, N. L., & Clark, J. G. (2005). A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation*, 2(2), 147–167.
- Bellovin, S. (2008). Security by Checklist. *IEEE Security & Privacy*, 6(2), 88–88.
- Berger, A. A. (2016). Media and communication research methods: an introduction to qualitative and quantitative approaches (Fourth). Los Angeles: SAGE Publications.
- Bergman, A., & Verlet, A. (2006). Security breaches: to notify or not to notify—that is the question. *Network Security*, 2006(5), 4–6.
- Best, D. M., Bhatia, J., Peterson, E. S., & Breaux, T. D. (2017). Improved cyber threat indicator sharing by scoring privacy risk. In *2017 IEEE International Symposium on Technologies for Homeland Security (HST)* (pp.1–5).
- BEUC. (2011). ePrivacy Directive Personal Data Breach Notification. <http://www.beuc.eu/publications/2011-09742-01-e.pdf>. [Accessed 13-March-2016].
- Bharosa, N., Meijer, S., Janssen, M., & Brave, F. (2010). Are we prepared?: Experiences from developing dashboards for disaster preparation. In *Proceedings of the 7th International Conference on Information Systems for Crisis Response and Management (ISCRAM2010)*.
- Bias, R. G., & Mayhew, D. J. (2005). *Cost-Justifying Usability : An Update for an Internet Age*. San Francisco: Elsevier Science & Technology.
- Bishop, M., & Frincke, D. A. (2005). Teaching secure programming. *IEEE Security & Privacy*, 3(5), 54–56.
- Boje, D. M. (2001). Narrative methods for organizational & communication research. Sage.
- Bold, C. (2012). Using narrative in research. London;Los Angeles; SAGE.
- Bollinger, J., Enright, B., & Valites, M. (2015). Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan. O'Reilly.
- Bolson, A. (2014). If Not All Data Breaches Are Created Equal, Why Are All Data Breach Notifications Treated the Same? <https://iapp.org/news/a/if-not-all-data-breaches-are-created-equal-why-are-all-data-breach-notifications-treated-the-same/> [Accessed 30-December-2018].
- Bonner, B. (2012). The problem of the 'problem' of privacy. In *Privacy: Management, Legal Issues and Security Aspects* (pp. 101–114). Nova Science Publishers, Inc.
- Bowman, G., MacKay, R. B., Masrani, S., & McKiernan, P. (2013). Storytelling and the scenario process: Understanding success and failure. *Scenario Method: Current Developments in Theory and Practice*, 80(4), 735–748.
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101.
- Braun, V., & Clarke, V. (2013). Successful qualitative research: A practical guide for beginners. Sage.
- Briggs, R. O., & Schwabe, G. (2011). On expanding the scope of design science in IS research. In *International Conference on Design Science Research in Information Systems* (pp. 92–106).
- Brownlee, N., & Guttman, E. (1998). Expectations for Computer Security Incident Response. *RFC Editor*
- Bryman, A., & Bell, E. (2015). *Business research methods* (Fourth). United Kingdom: Oxford University Press.
- Budak, J., Ivan-Damir, A., & Rajh, E. (2013). Public attitudes towards privacy and surveillance in Croatia. *Innovation (Abingdon, England)*, 26(1–2), 100–118.
- Budgen, D., Turner, M., Brereton, P., & Kitchenham, B. (2008). Using Mapping Studies in Software Engineering. In *Proceedings of PPIG 2008* (pp. 195–204). Lancaster University.
- Burdon, M., Lane, B., & von Nessen, P. (2012). Data breach notification law in the EU and Australia—Where to now? *Computer Law & Security Review*, 28(3), 296–307.
- Burkert, H. (1997). Privacy-enhancing technologies: Typology, critique, vision. In *Technology and privacy* (pp. 125–142). MIT Press
- Burns, R. B. (2000). *Introduction to research methods* (4th ed.). London: SAGE.
- Bygrave, L. (1998). Data protection pursuant to the right to privacy in human rights treaties. *International Journal of Law and Information Technology*, 6(3), 247–284.
- Calcutt, D., QC. (1990). Report of the Committee on Privacy and Related Matters (HMSO) (p. 7). London: HMSO.
- Calder, A., & Moir, S. (2009). IT governance: implementing frameworks and standards for the corporate governance of IT. Ely, Cambridgeshire, United Kingdom: IT Governance Publishing.
- Caldwell, T. (2012). Reporting data breaches. *Computer Fraud & Security*, 2012(7), 5–10.
- Callahan, M. E. (2017). Once More Into The Breach. *Criminal Justice*, 32(2), 20–23.

- Calo, M. R. (2011). The Boundaries of Privacy Harm. *Indiana Law Journal*, 86(3), 1131–1162.
- Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, 11(3), 431–448.
- Carrier, B., Spafford, E. H., & others. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence*, 2(2), 1–20.
- Casey, E. (2013). Triage in digital forensics. *Triage in Digital Forensics*, 10(2), 85–86.
- Casey, E., Katz, G., & Lewthwaite, J. (2013). Honing digital forensic processes. *Triage in Digital Forensics*, 10(2), 138–147.
- Chandler, D. (2007). *Semiotics: The Basics*. Routledge.
- Chari, S., Habeck, T., Molloy, I., Park, Y., & Teiken, W. (2013). A BigData platform for analytics on access control policies and logs (pp. 185–188). Presented at the Proceedings of ACM Symposium on Access Control Models and Technologies, SACMAT.
- Chatterjee, S. (2015). Writing My Next Design Science Research Master-piece: But How Do I Make a Theoretical Contribution to DSR? In *ECIS*.
- Chen, R., Sharman, R., Rao, H. R., & Upadhyaya, S. (2007). Design principles for critical incident response systems. *Information Systems and E-Business Management*, 5(3), 201–227.
- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *NIST Special Publication*, 800, 61.
- Citron, D. K. (2010). Mainstreaming privacy torts. *California Law Review*, 98(6), 1805–1852.
- Clarke, R. (2009). Privacy impact assessment: Its origins and development. *Computer Law & Security Review*, 25(2), 123–135.
- Clarke, R. (2013). Data Risks in the Cloud. *J. Theor. Appl. Electron. Commer. Res.*, 8(3), 59–73.
- Cleven, A., Gubler, P., & Hüner, K. M. (2009). Design Alternatives for the Evaluation of Design Science Research Artifacts. In *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology* (pp. 19:1-19:8). Philadelphia, Pennsylvania: ACM.
- CMS LawNow. (2018). GDPR HR audit - mapping out project success. http://www.cms-lawnow.com/ealerts/2018/01/gdpr-hr-audit-mapping-out-project-success?cc_lang=en [Accessed 17-August-2018].
- Collins, D. (2013). In search of popular management: Sensemaking, sensegiving and storytelling in the excellence project. *Culture and Organization*, 19(1), 42–61.
- Conboy, K. (2009). Agility from First Principles: Reconstructing the Concept of Agility in Information Systems Development. *Information Systems Research*, 20(3), 329–354.
- Cooper, Harris, & Hedges, Larry. (2009). *The Handbook of Research Synthesis and Meta-Analysis*. Russell Sage Foundation CY - New York.
- Cormack, A. (2016). Incident Response: Protecting Individual Rights Under the General Data Protection Regulation. *SCRIPT-Ed*, 13(3), 258–282.
- Costa, D. L., Albrethsen, M. J., Collins, M. L., Perl, S. J., Silowash, G. J., & Spooner, D. L. (2016). An Insider Threat Indicator *Ontology* (TECHNICAL REPORT). CERT® Division. http://resources.sei.cmu.edu/asset_files/technicalreport/2016_005_001_454627.pdf [Accessed 30-December-2018].
- Costermans, J., Lories, G., & Ansay, C. (1992). Confidence level and feeling of knowing in question answering: The weight of inferential processes. *Journal of Experimental Psychology: Learning, Memory, and Cognition*, 18(1), 142–150.
- Creswell, J. W. (2003). *Research design: qualitative, quantitative, and mixed methods approaches* (2nd ed.). Thousand Oaks, Calif; London; Sage.
- Cross, N. (2001). Designerly Ways of Knowing: Design Discipline versus Design Science. *Design Issues*, 17(3), 49–55.
- Cruzes, D. S., & Dyba, T. (2011). Recommended Steps for Thematic Synthesis in Software Engineering. In *2011 International Symposium on Empirical Software Engineering and Measurement* (pp. 275–284).
- Custers, B., Dechesne, F., Sears, A. M., Tani, T., & van der Hof, S. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law & Security Review*, 34(2), 234–243.
- Cyphort. (2014). *Dissecting The Target Breach*. <https://www.youtube.com/watch?v=hiKoBxn3smY>. [Accessed 30-December-2018].
- Daly, A. (2018). The introduction of data breach notification legislation in Australia: A comparative view. *Computer Law & Security Review*, 34(3), 477–495.
- Danagher, L. (2012). An Assessment of the Draft Data Protection Regulation: Does it Effectively Protect Data? *European Journal of Law and Technology*, 3(3).
- David, J. (2003). Incident Response. *Network Security*, 2003(9), 17–19.
- Davis, A., Dieste, O., Hickey, A., Juristo, N., & Moreno, A. M. (2006). Effectiveness of Requirements Elicitation Techniques: Empirical Results Derived from a Systematic Review. In *14th IEEE International Requirements Engineering Conference (RE'06)* (pp. 179–188).
- DCMS (2019). *Online harms* [White Paper] Department for Digital, Culture, Media & Sport: <https://www.gov.uk/government/consultations/online-harms-white-paper> [Accessed 2-May-2019].
- de Fuentes, J. M., González-Manzano, L., Tapiador, J., & Peris-Lopez, P. (2017). PRACIS: Privacy-preserving and aggregatable cybersecurity information sharing. *Security Data Science and Cyber Threat Management*, 69, 127–141.

- De, S. J., & Le Métayer, D. (2016a). PRIAM: A Privacy Risk Analysis Methodology. In G. Livraga, V. Torra, A. Aldini, F. Martinelli, & N. Suri (Eds.), *Data Privacy Management and Security Assurance: 11th International Workshop, DPM 2016 and 5th International Workshop, QASA 2016, Heraklion, Crete, Greece, September 26-27, 2016, Proceedings* (pp. 221–229). Cham: Springer International Publishing.
- De, S. J., & Le Métayer, D. (2016b). Privacy Harm Analysis: A Case Study on Smart Grids. In *2016 IEEE Security and Privacy Workshops (SPW)* (pp. 58–65).
- De, S. J., & Le Métayer, D. (2017). A Refinement Approach for the Reuse of Privacy Risk Analysis Results. In E. Schweighofer, H. Leitold, A. Mittrakas, & K. Rannenberg (Eds.), *Privacy Technologies and Policy: 5th Annual Privacy Forum, APF 2017, Vienna, Austria, June 7-8, 2017, Revised Selected Papers* (pp. 52–83). Cham: Springer International Publishing.
- Dekker, M., Karsber, C., & Daskala, B. (2012). Cyber Incident Reporting in the EU. <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/studies/cyber-incident-reporting-in-the-eu>. [Accessed 12-February-2018].
- Densham, B. (2015). Three cyber-security strategies to mitigate the impact of a data breach. *Network Security*, 2015(1), 5–8.
- Department for Digital, Culture, Media & Sport. (2019). Online harms [White Paper]. <https://www.gov.uk/government/consultations/online-harms-white-paper> [Accessed 2-May- 2019].
- Devey, C.S. (2008). Electronic Discovery/disclosure: From Litigation to International Commercial Arbitration. *The International Journal of Arbitration, Mediation and Dispute Management* 74 (4): 375.
- DFRWS. (2001). A Road Map for Digital Forensic Research. In The Digital Forensic Research Conference DFRWS 2001 USA Utica, NY (Aug 7th - 8th). Utica, New York. http://live-dfrws.pantheonsite.io/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf. [Accessed 30-December-2018].
- Dsouza, Z. (2018). Are Cyber Security Incident Response Teams (CSIRTs) Redundant or Can They Be Relevant to International Cyber Security? *Federal Communications Law Journal*, 69(3), 201–198.
- Dictionary.com. (2016). Breach | Define Breach at Dictionary.com. *Dictionary.com*. <http://www.dictionary.com/browse/breach>. [Accessed 30-December-2018].
- Domres, B., Kees, T., Gromer, S., Braitmaier, P., & Granzow, T. (2010). Ethical Aspects Of Triage. *German Institute for Disaster Medicine and Emergency Medicine*.
- Domres, B., Koch, M., Manger, A., & Becker, H. D. (2001). Ethics and Triage. *Prehospital and Disaster Medicine*, 16(1), 53–58.
- Doorn, N. (2017). Resilience indicators: opportunities for including distributive justice concerns in disaster management. *Journal of Risk Research*, 20(6), 711–731.
- Durance, P., & Godet, M. (2010). Scenario building: Uses and abuses. *Strategic Foresight*, 77(9), 1488–1492.
- Dyba, T., Dingsoyr, T., & Hanssen, G. K. (2007). Applying Systematic Reviews to Diverse Study Types: An Experience Report. In *First International Symposium on Empirical Software Engineering and Measurement (ESEM 2007)* (pp. 225–234).
- Eaton, C. (2003). *Essentials of immediate medical care* (2nd Edition). London, UK: Churchill Livingstone.
- Edwards, M. (2009). Triage. *The Lancet*, 373(9674), 1515
- Elliot, M., Mackey, E., O'Hara, K., & Tudor, C. (2016). *The Anonymisation Decision-Making Framework*. Published in the UK in 2016 by UKAN University of Manchester Oxford Road Manchester M13 9PL. <http://ukanon.net/wp-content/uploads/2015/05/The-Anonymisation-Decision-making-Framework.pdf> [Accessed 10-August-2018].
- Enemark, C. (2008). Triage, Treatment, and Torture: Ethical Challenges for US Military Medicine in Iraq. *Journal of Military Ethics*, 7(3), 186–201.
- ENISA. (2009). Good Practice Guide on Incident Reporting. <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/good-practice-guide-on-incident-reporting>. [Accessed 30-December-2018].
- ENISA. (2010). Good Practice Guide for Incident Management. <https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management> [Accessed 30-December-2018].
- ENISA. (2011). Data Breach Notifications in the EU Report. <https://www.enisa.europa.eu/news/enisa-news/new-report-data-breach-notifications-in-europe> [Accessed 30-December-2018].
- ENISA. (2012). Recommendations for Technical Implementation of Art.4. https://www.enisa.europa.eu/publications/art4_tech [Accessed 30-December-2018].
- ENISA. (2013). Recommendations for a methodology of the assessment of severity of personal data breaches. <https://www.enisa.europa.eu/publications/dbn-severity> [Accessed 30-December-2018]
- Erbacher, R. F., Christiansen, K., & Sundberg, A. (2006). Visual network forensic techniques and processes. In 1st Annual Symposium on Information Assurance: Intrusion Detection and Prevention (p. 72).
- Esayas, S. (2014). Breach Notification Requirements under the European Union Legal Framework: Convergence, Conflicts, and Complexity in Compliance. *John Marshall Journal of Information Technology and Privacy Law*, 31(317).
- Evans, D., & Kowanko, I. (2000). Literature Reviews: Evolution Of A Research Methodology. *Australian Journal of Advanced Nursing*, 18(2).
- Everaert-Desmedt, N. (2011). *Peirce's Semiotics*. Rimouski (Quebec) in Louis Hébert (dir.), Signo [online]. <http://www.signosemio.com/peirce/semiotics.asp>. [Accessed 30-December-2018].
- Eze, E. U. (2013). Context-based Multimedia Semantics Modelling and Representation. University of Hull.

- Fereday, J., & Muir-Cochrane, E. (2006). Demonstrating Rigor Using Thematic Analysis: A Hybrid Approach of Inductive and Deductive Coding and Theme Development. *International Journal of Qualitative Methods*, 5(1), 1–11.
- Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics*, 46(3), 541–562
- Few, S. (2006). Information dashboard design: the effective visual communication of data. Sebastopol, Calif;London; O'Reilly
- Fink, D., & Nyaga, C. (2009). Evaluating web site quality: the value of a multi paradigm approach. *Benchmarking: An International Journal*, 16(2), 259–273.
- Flach, P. A., & Kakas, A. C. (2000). Abductive and inductive reasoning: background and issues. In *Abduction and Induction* (pp. 1–27). Springer.
- Freund, J., & Jones, J. (2015). *Chapter 2 - Basic Risk Concepts*. In J. Freund & J. Jones (Eds.), *Measuring and Managing Information Risk* (pp. 13–23). Boston: Butterworth-Heinemann.
- Fuchs, C. (2011). Towards an alternative concept of privacy. *Journal of Information, Communication & Ethics in Society*, 9(4), 220–237.
- Gabriel, Y. (2000). *Storytelling in organizations: Facts, fictions, and fantasies: Facts, fictions, and fantasies*. OUP Oxford.
- Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. The Proceedings of the Tenth Annual DFRWS Conference, 7, Supplement, S64–S73.
- Garratt, A. M., Helgeland, J., & Gulbrandsen, P. (2011). Five-point scales outperform 10-point scales in a randomized comparison of item scaling for the Patient Experiences Questionnaire. *Journal of Clinical Epidemiology*, 64(2), 200–207.
- Gawande, A. (2011). *The Checklist Manifesto: How to get things right*. New York, USA: Picador.
- Gazendam, H., & Liu, K. (2005). *The Evolution of Organisational Semiotics*. Filipe, J., & Liu, K.(Eds.), *Studies in Organisational Semiotics*, Dordrecht. Kluwer Academic Publishers.
- GDPR. (2018) Regulation (EU) 2016/679 of the European Parliament of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2018). <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> [Accessed 20-August-2018].
- Ghanbari, M. (2007). Visualization overview (pp. 115–119). Presented at the Proceedings of the Annual Southeastern Symposium on System Theory
- Gillham, B. (2000). *Developing a Questionnaire*. New York;London; Continuum.
- Gillham, B. (2000a). *The Research Interview*. London: Continuum.
- Giupponi, C., & Biscaro, C. (2015). Vulnerabilities-bibliometric analysis and literature review of evolving concepts. *Environmental Research Letters*, 10(12), 123002.
- Goguen, J. A., & Linde, C. (1993). Techniques for requirements elicitation. In *Requirements Engineering, 1993., Proceedings of IEEE International Symposium on* (pp. 152–164).
- Gonzalez, R. A. (2009). Validation of crisis response simulation within the design science framework. *ICIS 2009 Proceedings*, 87.
- Good, L. (2008). Ethical Decision Making in Disaster Triage. *Journal of Emergency Nursing*, 34(2), 112–115
- Goodman, S. E., & Lin, H. S. (2007). *Toward a Safer and More Secure Cyberspace* US: National Research Council and National Academy of Engineering. https://www.nitrd.gov/cybersecurity/documents/NRC_Toward_a_Safer_and_More_Secure_Cyberspace_Full_report.pdf [Accessed 30-December-2018].
- Gough, D., Oliver, S., & Thomas, J. (2012). *An introduction to systematic reviews*. London;Los Angeles; SAGE.
- Greenwald, S. J., Snow, B. D., Ford, R., & Thieme, R. (2008). Towards an Ethical Code for Information Security? In *Proceedings of the 2008 Workshop on New Security Paradigms* (pp. 75–87). New York, NY, USA: ACM
- Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly*, 37(2).
- Gregory, R. W., & Muntermann, J. (2011). Theorizing in design science research: Inductive versus deductive approaches (Vol. 2, pp. 888–904). Presented at the International Conference on Information Systems 2011, ICIS 2011.
- Gubrium, J. F., & Holstein, J. A. (2001). *Handbook of Interview Research*. SAGE Publications, Inc
- Guest, G., MacQueen, K., & Namey, E. (2017). *Validity and Reliability (Credibility and Dependability) in Qualitative Research and Data Analysis*. In *Applied Thematic Analysis* (pp. 79–106). Thousand Oaks, California: SAGE Publications, Inc.
- Gunasekara, G. (2014). Paddling in unison or just paddling? International trends in reforming information privacy law. *International Journal of Law and Information Technology*, 22(2), 141–177.
- Gutting, G. (1980). Review: Progress and Its Problems: Toward a Theory of Scientific Growth by Larry Laudan. *Erkenntnis* (1975-), 15(1), 91–103.
- Hafkamp, W. (2006). IT security vulnerability and incident response management (pp. 387–395). Presented at the ISSE 2006 - Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2006 Conference.
- Haggerty, J., Haggerty, S., & Taylor, M. J. (2013). Visual triage of email network narratives for digital investigations (pp. 102–111). Presented at the Proceedings of the European Information Security Multi-Conference, EISMC 2013.

- Haggerty, J., Haggerty, S., & Taylor, M. (2014). Forensic triage of email network narratives through visualisation. *Information Management and Computer Security*, 22(4), 358–370.
- Haim, B., Menahem, E., Wolfsthal, Y., & Meenan, C. (2017). Visualizing Insider Threats: An Effective Interface for Security Analytics. In *Proceedings of the 22Nd International Conference on Intelligent User Interfaces Companion* (pp. 39–42). Limassol, Cyprus: ACM.
- Hales, B. M., & Pronovost, P. J. (2006). The checklist—a tool for error management and performance improvement. *Journal of Critical Care*, 21(3), 231–235.
- Hanid, M. (2014). Design Science Research as an Approach to Develop Conceptual Solutions for Improving Cost Management in Construction. University of Salford.
- Hardy, M. (2014). The Target Store Data Breaches: Examination and Insight. Nova Science Publishers, Inc.
- Harel, A., Shabtai, A., Rokach, L., & Elovici, Y. (2010). M-score: Estimating the potential damage of data leakage incident by assigning misuseability weight (pp. 13–20). Presented at the Proceedings of the ACM Conference on Computer and Communications Security.
- Hartman, R. G. (2003). Tripartite triage concerns: Issues for law and ethics. *Critical Care Medicine*, 31(5 SUPPL.), S358–S361.
- Haynes, J.D. (2015). Risk and Regulation of Access to Personal Data on Online Social Networking Services in the UK. City University London. <http://openaccess.city.ac.uk/11972/>. [Accessed 23-September-2015].
- Hendee, W. R., & Wells, P. N. T. (1993). *Perception of Visual Information*. New York, NY: Springer New York.
- Henriksen-Bulmer, J., Faily, S., & Jeary, S. (2019). Privacy risk assessment in context: A meta-model based on contextual integrity. *Computers & Security*, 82, 270–283.
- Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, 75–105.
- Hevner, A. R. (2007). A three cycle view of design science research. *Scandinavian Journal of Information Systems*, 19(2), 4.
- Hickey, A. M., & Davis, A. M. (2003). Elicitation technique selection: how do experts do it? In *Requirements Engineering Conference, 2003. Proceedings. 11th IEEE International* (pp. 169–178).
- Hinde, C., & Ophoff, J. (2014). Privacy: A review of publication trends. In *2014 Information Security for South Africa* (pp. 1–7).
- Hinkel, J. (2011). “Indicators of vulnerability and adaptive capacity”: Towards a clarification of the science–policy interface. *Global Environmental Change*, 21(1), 198–208.
- Hogan, D. E., & Burstein, J. L. (2007). *Disaster medicine*. Lippincott Williams & Wilkins.
- Holm, E., & Mackenzie, G. (2014). The importance of mandatory data breach notification to identity crime. In *2014 Third International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)* (pp. 6–11).
- Hong, I., Yu, H., Lee, S., & Lee, K. (2013). A new triage model conforming to the needs of selective search and seizure of electronic evidence. *Triage in Digital Forensics*, 10(2), 175–192.
- House, A., Power, N., & Alison, L. (2014). A systematic review of the potential hurdles of interoperability to the emergency services in major incidents: recommendations for solutions and alternatives. *Cognition, Technology & Work*, 16(3), 319–335.
- Hove, C., & Tårnes, M. (2013). *Information Security Incident Management An Empirical Study of Current Practice.*, Norwegian University of Science and Technology. <https://brage.bibsys.no/xmlui/handle/11250/262845> [Accessed 30-December-2018].
- Howard, J. D. (1997). An Analysis of Security Incidents on the Internet 1989-1995. Pittsburgh, Pennsylvania. <http://www.dtic.mil/dtic/tr/fulltext/u2/a389085.pdf> [Accessed 30-December-2018].
- Howard, J. D., & Longstaff, T. A. (1998). *A Common Language for Computer Security Incidents*. Sandia National Labs., Albuquerque, NM (US); Sandia National Labs., Livermore, CA (US). <http://www.osti.gov/scitech/biblio/751004> [Accessed 30-December-2018].
- Howard, P. N., & Gulyas, O. (2014). *Data Breaches in Europe: Reported Breaches of Compromised Personal Records in Europe, 2005-2014 | CMDS* (CMDS Working Paper 2014.1). Center for Media, Data and Society School of Public Policy Central European University. <http://cmds.ceu.hu/article/2014-10-07/data-breaches-europe-reported-breaches-compromised-personal-records-europe-2005> [Accessed 31-December-2018].
- Hoyer, S., Zakhariya, H., Sandner, T., & Breitner, M. H. (2012). Fraud prediction and the human factor: An approach to include human behavior in an automated fraud audit (pp. 2382–2391). Presented at the Proceedings of the Annual Hawaii International Conference on System Sciences.
- Huang, S-C. (2006). A semiotic view of information: semiotics as a foundation of LIS research in information behavior. *Proceedings of the American Society for Information Science and Technology*, 43(1), 1–17.
- Hughes, N. (2013). Towards improving the relevance of scenarios for public policy questions: A proposed methodological framework for policy relevant low carbon scenarios. *Scenario Method: Current Developments in Theory and Practice*, 80(4), 687–698.
- Humphries, D. (2015). To BI or Not to BI? How Dashboards Impact SMB Confidence in Data Analytics. <http://www.softwareadvice.com/resources/how-bi-dashboards-impact-smb/> [Accessed 31-December-2018].
- Hunter, I. (2006). The History of Theory. *Critical Inquiry*, 33(1), 78–112.
- ICO. (2012). What is personal data? https://ico.org.uk/media/for-organisations/documents/1549/determining_what_is_personal_data_quick_reference_guide.pdf [Accessed 31-December-2018].

- ICO. (2012a). Guidance on data security breach management. UK: ICO. https://ico.org.uk/media/for-organisations/documents/1562/guidance_on_data_security_breach_management.pdf [Accessed 17-September-2016]. A copy is available offline.
- ICO. (2012b). Notification of data security breaches to the Information Commissioner's Office (ICO) Version: 1.0. https://ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf [Accessed 17-September-2016]. A copy is available offline.
- ICO. (2014). Conducting privacy impact assessments code of practice. <https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf> [Accessed 17-September-2016]. A copy is available offline.
- ICO. (2017). TalkTalk gets record £400,000 fine for failing to prevent October 2015 attack. Retrieved from <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/> [Accessed 31-December-2018].
- ICO. (2018). Guide to the General Data Protection Regulation (GDPR). The ICO. <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/> [Accessed 15-September-2018].
- ICO. (2018a). The ICO Documentation. <https://ico.org.uk/media/for-organisations/documents/2172937/gdpr-documentation-controller-template.xlsx> [Accessed 17-August-2018].
- Iivari, J. (2007). A paradigmatic analysis of information systems as a design science. *Scandinavian Journal of Information Systems*, 19(2), 5.
- Iivari, J., Hansen, M. R. P., & Haj-Bolouri, A. (2018). A Framework for Light Reusability Evaluation of Design Principles in Design Science Research. Presented at the DESRIST 2018, Chennai, India.
- Ines, D., Sebastien, I., Jean-Marie, G., Madeth, M., & Serge, G. (2017). Towards adaptive dashboards for learning analytic an approach for conceptual design and implementation (Vol. 1, pp. 120–131). Presented at the CSEDU 2017 - Proceedings of the 9th International Conference on Computer Supported Education
- Iseron, K. V., & Moskop, J. C. (2007). Triage in Medicine, Part I: Concept, History, and Types. *Annals of Emergency Medicine*, 49(3), 275–281.
- Jahankhani, H. (2012). The behaviour and perceptions of on-line consumers: Risk, risk perception and trust. *International Journal of Information Science and Management (IJISM)*, 7(1), 79–90.
- Jennings, B., & Arras, J. (2016). Ethical Guidance for Public Health Emergency Preparedness and Response: Highlighting Ethics and Values in a Vital Public Health Service. https://www.cdc.gov/od/science/integrity/phethics/docs/white_paper_final_for_website_2012_4_6_1_2_final_for_web_508_compliant.pdf [Accessed 31-December-2018].
- Joffe, H. (2011). Thematic Analysis. In *Qualitative Research Methods in Mental Health and Psychotherapy* (pp. 209–223). John Wiley & Sons.
- Johannesson, P., & Perjons, E. (2014). *An introduction to design science*. Springer.
- Johnson, L. (2014). Computer incident response and forensics team management: conducting a successful incident response. Rockland: Syngress.
- Johnston, C. (2015). TalkTalk customer data at risk after cyber-attack on company website | Business | The Guardian <http://www.theguardian.com/business/2015/oct/22/talktalk-customer-data-hackers-website-credit-card-details-attack> [Accessed 31-December-2018].
- Kane, G. (1985). Empirical development and evaluation of prehospital trauma triage instruments. *The Journal of Trauma*, 25(6), 482.
- Kane, G., & Koppel, L. (2013). *Information Security Playbook*. Boston: Elsevier
- Karunakaran, S., Mathew, S. K., & Lehner, F. (2017). Privacy protection Dashboard: A study of individual cloud-storage users information privacy protection responses (pp. 181–182). Presented at the SIGMIS-CPR 2017 - Proceedings of the 2017 ACM SIGMIS Conference on Computers and People Research.
- Kennedy, K., Aghababian, R. V., Gans, L., & Lewis, C. P. (1996). Triage: Techniques and Applications in Decisionmaking. *Annals of Emergency Medicine*, 28(2), 136–144.
- Kerrigan, M. (2013). A capability maturity model for digital investigations. *Digital Investigation*, 10(1), 19–33.
- Killcrece, G., Kossakowski, K.-P., Ruefle, R., & Zajicek, M. (2003). Organizational Models for Computer Security Incident Response Teams (CSIRTs). CMU/SEI. http://resources.sei.cmu.edu/asset_files/handbook/2003_002_001_14099.pdf [Accessed 31-December-2018].
- Kitchenham, B., and Charters, S. (2007). Guidelines for Performing Systematic Literature Reviews in Software Engineering. *School of Computer Science and Mathematics, Keele University*. Technical Report EBSE-2007-01.
- Kitchenham, B., Budgen, D., and Brereton, P. (2010). The Value of Mapping Studies: A Participant-Observer Case Study. In *International Conference On Evaluation And Assessment In Software Engineering* (Vol. 14).
- Kitchenham, B. A., Budgen, D., & Pearl Brereton, O. (2011). Using mapping studies as the basis for further research – A participant-observer case study. *Special Section: Best Papers from the APSEC Best Papers from the APSEC*, 53(6), 638–651.
- Kitchenham, B., & Brereton, P. (2013). A systematic review of systematic review process research in software engineering. *Information and Software Technology*, 55(12), 2049–2075.
- Kitkowska, A., Wästlund, E., Meyer, J., & Martucci, L. A. (2018). Is it harmful? Re-examining privacy concerns (Vol. 526).

- Kohn, M. D., Eloff, M. M., & Eloff, J. H. P. (2013). Integrated digital forensic process model. *Cybercrime in the Digital Economy*, 38, 103–115.
- Komoto, T., Taguchi, K., Mouratidis, H., Yoshioka, N., & Futatsugi, K. (2011). A Modelling Framework to Support Internal Control. In *Secure Software Integration & Reliability Improvement Companion (SSIRI-C), 2011 5th International Conference on* (pp. 187–193).
- Koven, J., Bertini, E., Dubois, L., & Memon, N. (2016). InVEST: Intelligent visual email search and triage. *Digital Investigation*, 18, S138–S148.
- Krishnamurthy, B., & Wills, C. (2009). Privacy Diffusion on the Web: A Longitudinal Perspective. In *Proceedings of the 18th International Conference on World Wide Web* (pp. 541–550). Madrid, Spain: ACM.
- Krüger, U., Wucholt, F., & Beckstein, C. (2012). Electronic checklist support for disaster response. Presented at the ISCRAM 2012 Conference Proceedings - 9th International Conference on Information Systems for Crisis Response and Management.
- Kvale, S. (2007). *Doing Interviews*. Sage Publications Ltd.
- Lane, B., Burdon, M., Miller, E., & von Nessen, P. (2010). Stakeholder perspectives regarding the mandatory notification of Australian data breaches. *MALR*, 15, 149–164.
- Laudan, L. (1978). *Progress and its problems: towards a theory of scientific growth*. Berkeley, CA: University of California Press.
- Lavrakas, P. (2008). *Encyclopedia of Survey Research Methods* (Online). London; Los Angeles, [Calif.]; SAGE.
- Layton, R., & Watters, P. A. (2014). A methodology for estimating the tangible cost of data breaches. *Journal of Information Security and Applications*, 19(6), 321–330.
- Lazanski, T. J., & Kljajić, M. (2006). Systems approach to complex systems modelling with special regards to tourism. *Kybernetes*, 35(7/8), 1048–1058.
- Lee, J. S., Pries-Heje, J., & Baskerville, R. (2011). *Theorizing in design science research* (Vol. 6629 LNCS).
- Lepmets, M., Mesquida, A. L., Cater-Steel, A., Mas, A., & Ras, E. (2014). The Evaluation of the IT Service Quality Measurement Framework in Industry. *Global Journal of Flexible Systems Management*, 15(1), 39–57.
- Leyden, J. (2017). *Last year's ICO fines would be 79 times higher under GDPR* (Security). The Register. https://www.theregister.co.uk/2017/04/28/ico_fines_post_gdpr_analysis/ [Accessed 15-September-2018]
- Li, L. (2010). An Integrated Visual Approach for Business Process Modelling. University of Auckland, New Zealand.
- Light, B., Burgess, J., & Duguay, S. (2016). The walkthrough method: An approach to the study of apps. *New Media & Society*, 20(3), 881–900.
- Littman, L., Swaney, M., & Williams, A. (2014). The New Frontiers of Privacy Harm. Presented at the Silicon Flatirons, University of Colorado Law School. <https://siliconflatirons.org/events/the-new-frontiers-of-privacy-harm/> [Accessed 31-December-2018].
- Liu, K., & Terzi, E. (2010). A Framework for Computing the Privacy Scores of Users in Online Social Networks. *ACM Trans. Knowl. Discov. Data*, 5(1), 6:1–6:30.
- Liu, K., & Li, W. (2015). *Organisational semiotics for business informatics*. Abingdon, Oxon: Routledge, Taylor & Francis Group
- Looney, G. L., Roy, A., Anderson, G. V., & Scharf, R. F. (1980). Research algorithms for emergency medicine. *Annals of Emergency Medicine*, 9(1), 12–17.
- Lorenz, C. (2011). History and Theory. In D. Woolf & A. Schneider (Eds.), *The Oxford History of Historical Writing* (pp. 13–35). Oxford: Oxford University Press.
- Lottridge, D., & Mackay, W. E. (2009). Generative Walkthroughs: To Support Creative Redesign. In *Proceedings of the Seventh ACM Conference on Creativity and Cognition* (pp. 175–184). New York, NY, USA: ACM.
- Lowman, S., & Ferguson, I. (2010). Web history visualisation for forensic investigations. *Msc Forensic Informatics Dissertation, Department of Computer and Information Sciences, University of Strathclyde*.
- Maier, H. R., Guillaume, J. H. A., van Delden, H., Riddell, G. A., Haasnoot, M., & Kwakkel, J. H. (2016). An uncertain future, deep uncertainty, scenarios, robustness and adaptation: How do they fit together? *Environmental Modelling & Software*, 81, 154–164.
- March, S. T., & Storey, V. C. (2008). Design Science in the Information Systems Discipline: An Introduction to the Special Issue on Design Science Research. *MIS Quarterly*, 32(4), 725–730.
- Markus, M. L., Majchrzak, A., & Gasser, L. (2002). A design theory for systems that support emergent knowledge processes. *MIS Quarterly*, 179–212.
- Martins, R. de J., Knob, L. A. D., da Silva, E. G., Wickboldt, J. A., Schaeffer-Filho, A., & Granville, L. Z. (2019). Specialized CSIRT for Incident Response Management in Smart Grids. *Journal of Network and Systems Management*, 27(1), 269–285.
- Marx, G. T. (1998). Ethics for the new surveillance. *Information Society*, 14(3), 171–185.
- Massey, A. K., & Antón, A. I. (2008). A requirements-based comparison of privacy taxonomies. Presented at the 2008 Requirements Engineering and Law, RELAW'08.
- Matwyshyn, A. M., Cui, A., Keromytis, A. D., & Stolfo, S. J. (2010). Ethics in security vulnerability research. *IEEE Security & Privacy*, 8(2), 67–72.
- Maurushat, A. (2009). Data breach notification law across the world from California to Australia. *Privacy Law and Business International*.
- McCullagh, K. (2007). Data sensitivity: Proposals for resolving the conundrum. *J. Int'l Com. L. & Tech.*, 2, 190.

- McDermott, R. (2011). Internal and External Validity. In A. Lupia, D. P. Green, J. H. Kuklinski, & J. N. Druckman (Eds.), *Cambridge Handbook of Experimental Political Science* (pp. 27–40). Cambridge: Cambridge University Press
- McGinn, J. J., & Chang, A. R. (2013). RITE+ Krug: A combination of usability test methods for Agile design. *Journal of Usability Studies*, 8(3), 61–68.
- McLaren, T., & Buijs, P. (2011). A design science approach for developing information systems research instruments. Retrieved from <https://pdfs.semanticscholar.org/153c/b6dd9c5d042b2ecdf076e2be7f8964a47e3a.pdf>. [Accessed 20-July-2018].
- Medlock, M. C., Wixon, D., Terrano, M., & Romero, R. L. (2002). Using the RITE method to improve products; a definition and a case study. In Usability Professionals Association (Vol. 51).
- Medlock, M. C., Wixon, D., McGee, M., & Welsh, D. (2005). The Rapid Iterative Test and Evaluation Method: Better Products in Less Time. In R. G. Bias & D. J. Mayhew (Eds.), *Cost-Justifying Usability (Second Edition)* (pp. 489–517). San Francisco: Morgan Kaufmann.
- Mell, P., Scarfone, K., & Romanosky, S. (2006). Common Vulnerability Scoring System. *IEEE Security & Privacy*, 4(6), 85–89.
- Miles, M. B., & Huberman, A. M. (1994). Qualitative data analysis: An expanded sourcebook. Sage.
- Mingers, J., & Willcocks, L. (2014). An integrative semiotic framework for information systems: The social, personal and material worlds. *Information and Organization*, 24(1), 48–70.
- Mislan, R. P., Casey, E., & Kessler, G. C. (2010). The growing need for on-scene triage of mobile devices. *Embedded Systems Forensics: Smart Phones, GPS Devices, and Gaming Consoles*, 6(3–4), 112–124
- Mocas, S. (2004). Building theoretical underpinnings for digital forensics research. *Digital Investigation*, 1(1), 61–68.
- Mohammad Ghafari, Mortaza Saleh, & Touraj Ebrahimi. (2012). A Federated Search Approach to Facilitate Systematic Literature Review in Software Engineering. *International Journal of Software Engineering & Applications (Chennai, India)*, 3(2), 13–24.
- Molitor, G. T. (2009). Scenarios: worth the effort? *Journal of Futures Studies*, 13(3), 81–92.
- Moll, H. A. (2010). Challenges in the validation of triage systems at emergency departments. *Journal of Clinical Epidemiology*, 63(4), 384–388.
- Monika, D. Srinivasan, & T. Reindl. (2017). Demand side management in residential areas using geographical information system. In 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2) (pp. 1–6).
- Montasari, R., Peltola, P., & Evans, D. (2015). Integrated Computer Forensics Investigation Process Model (ICFIPM) for Computer Crime Investigations. In H. Jahankhani, A. Carlile, B. Akhgar, A. Taal, A. G. Hessami, & A. Hosseinian-Far (Eds.), *Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security: 10th International Conference, ICGS3 2015, London, UK, September 15-17, 2015. Proceedings* (pp. 83–95). Cham: Springer International Publishing
- Moore, E., & Likarish, D. (2015). A cyber security multi agency collaboration for rapid response that uses AGILE methods on an education infrastructure. In *IFIP World Conference on Information Security Education* (pp. 41–50). Springer.
- Moon, J. (2010). Using story: In higher education and professional development. Routledge.
- Moriarty, S. (1994a). VISEMICS: A Proposal for a marriage between semiotics and visual communication. In *Visual Communication 94*. Feather River Inn, Blairsden, California.
- Moriarty, S. (1994b). Visual communication as a primary system. *Journal of Visual Literacy*, 14(2), 11–12.
- Moriarty, S. (1995). Visual Communication Theory: A search for roots. In *Visual Communication Conference*. Flagstaff AZ. https://docuri.com/download/visual-communication-theory_59c1cb86f581710b2861195a_pdf. [Accessed 31-December-2018].
- Moriarty, S. (2005). Visual Semiotics theory. *Handbook of Visual Communication: Theory, Methods, and Media*, 8, 227–241.
- Moriarty, S., & Sayre, S. (2005). An Intended-Perceived Study Using Visual Semiotics. *Handbook of Visual Communication: Theory, Methods, and Media*, 8, 243–255.
- Moser, A., & Cohen, M. I. (2013). Hunting in the enterprise: Forensic triage and incident response. *Triage in Digital Forensics*, 10(2), 89–98.
- Moskop, J. C., & Iserson, K. V. (2007). Triage in Medicine, Part II: Underlying Values and Principles. *Annals of Emergency Medicine*, 49(3), 282–287.
- Mourouzis, A., Antona, M., & Stephendis, C. (2011). A diversity-sensitive evaluation method. *Universal Access in the Information Society*, 10(3), 337–356.
- Mulligan, D., Koopman, C., & Doty, N. (2016). Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A-Mathematical Physical and Engineering Sciences*, 374(2083), 20160118.
- Mundie, D., Ruefle, R., Dorofee, A., McCloud, J., Perl, S., & Collins, M. (2014). An Incident Management Ontology. Presented at the Incident Management, Software Engineering Institute | Carnegie Mellon University 4500 Fifth Ave., Pittsburgh, PA, United States of America: Software Engineering Institute. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=426836> [Accessed 31-December-2018].
- Muntermann, J., & Roßnagel, H. (2009). On the Effectiveness of Privacy Breach Disclosure Legislation in Europe: Empirical Evidence from the US Stock Market. In A. Jøsang, T. Maseng, & S. J. Knapkog (Eds.), *Identity and Privacy in the Internet Age* (pp. 1–14). Springer Berlin Heidelberg.

- Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization*, 17(1), 2–26.
- Myers, M. D., & Venable, J. R. (2014). A set of ethical principles for design science research in information systems. *Information & Management*, 51(6), 801–809.
- Naumann, J. D., & Jenkins, A. M. (1982). Prototyping: The New Paradigm for Systems Development. *MIS Quarterly*, 6(3), 29–44.
- Nenonen, S., Brodie, R. J., Storbacka, K., & Peters, L. D. (2017). Theorizing with managers: how to achieve both academic rigor and practical relevance? *European Journal of Marketing*, 51(7/8), 1130–1152.
- Newton, J. H. (2004). Visual Ethics Theory. *Handbook of Visual Communication*, 429–43.
- Newton, J. H., & Williams, R. (2010). Visual Ethics: An Integrative Approach to Ethical Practice in Visual Journalism. In *Journalism Ethics*.
- Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, 79(119).
- Noblett, M. G., Pollitt, M. M., & Presley, L. A. (2000). *Recovering and examining computer forensic evidence* (Vol. 2).
- Nunamaker, J. F., Chen, M., & Purdin, T. D. M. (1990). Systems Development in Information Systems Research. *Journal of Management Information Systems*, 7(3), 89–106.
- Nunamaker, J. F., Jr., & Briggs, R. O. (2012). Toward a Broader Vision for Information Systems. *ACM Trans. Manage. Inf. Syst.*, 2(4), 20:1–20:12.
- Oetzel, M. C., & Spiekermann, S. (2012). Privacy-by-design through systematic privacy impact assessment - A design science approach. Presented at the ECIS 2012 - Proceedings of the 20th European Conference on Information Systems.
- Oetzel, M. C., & Spiekermann, S. (2014). A systematic methodology for privacy impact assessments: A design science approach. *European Journal of Information Systems*, 23(2), 126–150.
- Offermann, P., Levina, O., Schönherr, M., & Bub, U. (2009). Outline of a Design Science Research Process. In *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology* (pp. 7:1-7:11). Philadelphia, Pennsylvania: ACM.
- Offermann, P., Blom, S., Levina, O., & Bub, U. (2010). Proposal for components of method design theories. *Business & Information Systems Engineering*, 2(5), 295–304.
- O’Keefe, C., Otorepec, S., Elliot, M., Mackey, E., & O’Hara, K. (2017). *The De-Identification DecisionMaking Framework* (CSIRO Reports No. EP173122 and EP175702).
- O’Keefe, R. (2014). Design Science, the design of systems and Operational Research: back to the future? *Journal of the Operational Research Society*, 65(5), 673–684.
- O’Laughlin DT, & Hick JL. (2008). Ethical issues in resource triage...includes discussion. *Respiratory Care*, 53(2), 190-200 11p.
- Oliveira, E. S. de, & Loula, A. (2015). Symbolic associations in neural network activations: Representations in the emergence of communication. In *2015 International Joint Conference on Neural Networks (IJCNN)* (pp. 1–8).
- Olsson, J., & Boldt, M. (2009). Computer forensic timeline visualization tool. *The Proceedings of the Ninth Annual DFRWS Conference*, 6, Supplement, S78–S87.
- Omar, M. S. H. (2014). A Novel Workflow Management System for Handling Dynamic Process Adaptation and Compliance. Loughborough University.
- O’Meara, M., Porter, K., & Greaves, I. (2007). Triage. *Trauma*, 9(2), 111–118.
- Open Security Foundation. (2014). DataLossDB. <https://blog.datalossdb.org/>. [Accessed 31-December-2018].
- Ose, S. O. (2016). Using Excel and Word to Structure Qualitative Data. *Journal of Applied Social Science*, 10(2), 147–162.
- Paavola, S. (2005). Peircean abduction: Instinct or inference? *Semiotica*, 2005(153-1/4), 131–154.
- Pace, A., & Buttigieg, S. C. (2017). Can hospital dashboards provide visibility of information from bedside to board? A case study approach. *Journal of Health Organization and Management*, 31(2), 142–161.
- Paradice, D. B. (2007). A Program of Study of the Use of Stories in DSS. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on* (pp. 253a-253a).
- Parkin, S., & Epili, S. (2015). A Technique for Using Employee Perception of Security to Support Usability Diagnostics (pp. 1–8). Presented at the Proceedings - 5th Workshop on Socio-Technical Aspects in Security and Trust, STAST 2015.
- Parsonage, H. (2009). Computer forensics case assessment and triage. <http://computerforensics.parsonage.co.uk/triage/ComputerForensicsCaseAssessmentAndTriageDiscussionPaper.pdf>. [Accessed 31-December-2018].
- Patton, J. (2008). Getting Software RITE. *IEEE Softw.*, 25(3), 20–21.
- Payne, S. L. B. (1951). *The art of asking questions*. Oxford;Princeton, N.J; Princeton University Press.
- Pearlgood, A. (2012). The impact of mandatory data infringement reporting. *Computer Fraud & Security*, 2012(5), 11–13.
- Pearson, C. (2008). Beyond Peirce: The New Science of Semiotics and the Semiotics of Law. *International Journal for the Semiotics of Law - Revue Internationale de Sémiotique Juridique*, 21(3), 247–296.
- Pearson, S., & Allison, D. (2009). A model-based privacy compliance checker. *International Journal of E-Business Research*, 5(2), 63–83.
- Pearson, S., & Watson, R. (2010). *Digital Triage Forensics: Processing the Digital Crime Scene*. Syngress Publishing.
- Peppers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, 24(3), 45–77.

- Peffers, K., Rothenberger, M., Tuunanen, T., & Vaezi, R. (2012). Design Science Research Evaluation. In K. Peffers, M. Rothenberger, & B. Kuechler (Eds.), *Design Science Research in Information Systems. Advances in Theory and Practice* (pp. 398–410). Springer Berlin Heidelberg.
- Peirce, C. S. 1839-1914. (1953). *Letters to Lady Welby*. New Haven: Published by Whitlock for the Graduate Peirce, C. S. 1839-1914. (1953). *Letters to Lady Welby*. United States: Published by Whitlock for the Graduate Philosophy Club of Yale University.
- Peirce, C. S. (1997). *Pragmatism as a principle and method of right thinking: the 1903 Harvard lectures on pragmatism*. Albany: State University of New York Press.
- Petersen, K., Feldt, R., Mujtaba, S., & Mattsson, M. (2008). Systematic Mapping Studies in Software Engineering. In *Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering* (pp. 68–77). Italy: British Computer Society.
- Petersen, K., Vakkalanka, S., & Kuzniarz, L. (2015). Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and Software Technology*, 64, 1–18.
- Phua, C. (2009). Protecting organisations from personal data breaches. *Computer Fraud & Security*, 2009(1), 13–18.
- Pieterse, T. (2011). The corporate incident response framework (CIRF). In *IST-Africa Conference Proceedings, 2011* (pp. 1–13).
- Piirainen, K., Gonzalez, R. A., & Kolfschoten, G. (2010). Quo Vadis, Design Science? – A Survey of Literature. In R. Winter, J. L. Zhao, & S. Aier (Eds.), *Global Perspectives on Design Science Research* (pp. 93–108). Springer Berlin Heidelberg.
- Plowright, D. (2016). Charles Sanders Peirce: pragmatism and education. Dordrecht: Springer.
- Pollak, E., Falash, M., Ingraham, L., & Gottesman, V. (2004). Operational analysis framework for emergency operations center preparedness training. In *Simulation Conference, 2004. Proceedings of the 2004 Winter* (Vol. 1). IEEE.
- Poller, A., Türpe, S., & Kinder-Kurlanda, K. (2014). An Asset to Security Modeling?: Analyzing Stakeholder Collaborations Instead of Threats to Assets. In *Proceedings of the 2014 New Security Paradigms Workshop* (pp. 69–82). Victoria, British Columbia, Canada: ACM.
- Pollitt, M. (2007). An ad hoc review of digital forensic models (pp. 43–52). Presented at the Proceedings - SADFE 2007: Second International Workshop on Systematic Approaches to Digital Forensic Engineering.
- Pollitt, M. (2010). A History of Digital Forensics. In K.-P. Chow & S. Shenoi (Eds.), *Advances in Digital Forensics VI: Sixth IFIP WG 11.9 International Conference on Digital Forensics, Hong Kong, China, January 4-6, 2010, Revised Selected Papers* (pp. 3–15). Berlin, Heidelberg: Springer Berlin Heidelberg.
- Pollitt, M. (2013). Triage: A practical solution or admission of failure. *Triage in Digital Forensics*, 10(2), 87–88.
- Ponemon Institute. (2014). Consumer Study on Aftermath of a Breach FINAL 2 - experian-consumer-study-on-aftermath-of-a-data-breach.pdf. <http://www.experian.com/assets/p/data-breach/experian-consumer-study-on-aftermath-of-a-data-breach.pdf> [Accessed 31-December-2018].
- Privitera, M. B. (2016). *Collaborative Medical Device Design*. Loughborough University.
- Rabionet, S. E. (2011). How I Learned to Design and Conduct Semi-structured Interviews: An Ongoing and Continuous Journey. *The Qualitative Report*, 16(2), 563–566.
- Raghavan, S. (2013). Digital forensic research: current state of the art. *CSI Transactions on ICT*, 1(1), pp 91-114.
- Rasmussen, N., Chen, C. Y., & Bansal, M. (2009). *Business dashboards: a visual catalog for design and deployment*. Chichester; Hoboken, N.J.: Wiley.
- Reddy, K., & Venter, H. (2009). A Forensic Framework for Handling Information Privacy Incidents. In G. Peterson & S. Shenoi (Eds.), *Advances in Digital Forensics V* (pp. 143–155). Springer Berlin Heidelberg.
- Reidenberg, J. R., Russell, N. C., Callen, A. J., Qasir, S., & Norton, T. B. (2015). Privacy harms and the effectiveness of the notice and choice framework. *ISJLP*, 11, 485.
- Reijers, H. A., Leopold, H., & Recker, J. (2017). Towards a science of checklists. In *Proceedings of the 50th Hawaii International Conference on System Sciences*.
- Ring, T. (2013). A breach too far? *Computer Fraud & Security*, 2013(6), 5–9.
- Ritchie, J., Lewis, J., McNaughton Nicholls, C., & Ormston, R. (2014). *Qualitative research practice: a guide for social science students and researchers* (Second). Los Angeles: SAGE.
- Rogers, M. K., Goldman, J., Mislán, R., Wedge, T., & Debrota, S. (2006). Computer forensics field triage process model. In *Proceedings of the conference on Digital Forensics, Security and Law* (p. 27). Association of Digital Forensics, Security and Law.
- Rossi, M., Henfridsson, O., Lyytinen, K., & Siau, K. (2013). Design Science Research: The Road Traveled and the Road That Lies Ahead. *Journal of Database Management (JDM)*, 24(3), 1–8.
- Rotenberg, M., & Jacobs, D. (2013). Updating the Law of Information Privacy: The New Framework of the European Union Privacy, Security, and Human Dignity in the Digital Age. *Harvard Journal of Law & Public Policy*, 36(2), 605–652.
- Rounsevell, M. D. A., & Metzger, M. J. (2010). Developing qualitative scenario storylines for environmental change assessment. *Wiley Interdisciplinary Reviews: Climate Change*, 1(4), 606–619.
- Roussev, V., Quates, C., & Martell, R. (2013). Real-time digital forensics and triage. *Triage in Digital Forensics*, 10(2), 158–167.
- Rowell, M. D. (2017). Cyber indicators of compromise: a domain ontology for security information and event management (Master Dissertation). Naval Postgraduate School Monterey United States.
- Rowley, J. (2007). The wisdom hierarchy: representations of the DIKW hierarchy. *Journal of Information Science*, 33(2), 163–180.

- Ryan, G. W., & Bernard, H. R. (2003). Techniques to Identify Themes. *Field Methods*, 15(1), 85–109.
- Salomon, J. M., & Elsa, P. (2004). Computer security incident response grows up. *Computer Fraud & Security*, 2004(11), 5–7.
- Sandelowski, M. (1986). The problem of rigor in qualitative research. *Advances in Nursing Science*, 8(3), 27–37.
- Sandner, T., Kehlenbeck, M., & Breitner, M. H. (2010). Visualization of automated compliance monitoring and reporting (pp. 364–368). Presented at the Proceedings - 21st International Workshop on Database and Expert Systems Applications, DEXA 2010.
- Santiago Rivera, D., & Shanks, G. (2015). A Dashboard to Support Management of Business Analytics Capabilities. *Journal of Decision Systems*, 24(1), 73–86.
- Santillan, L. (2014). An i* based approach for conceptual modeling of business process technology (Vol. 1157). Presented at the CEUR Workshop Proceedings.
- Savage, S. R. (2017). Characterizing the Risks and Harms of Linking Genomic Information to Individuals. *IEEE Security & Privacy*, 15(5), 14–19.
- Schneier, B. (2014). The future of incident response. *IEEE Security and Privacy*, 12(5), 96–97.
- Schönfelder, W. (2011). CAQDAS and qualitative syllogism logic-NVivo 8 and MAXQDA 10 compared. In *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research* (Vol. 12).
- Schwartz, P. M., & Janger, E. J. (2007). Notification of Data Security Breaches. *Michigan Law Review*, 105(5), 913–984.
- Schwartz, P. M., & Peifer, K.-N. (2017). Transatlantic Data Privacy Law. *Georgetown Law Journal*, 106(1), 115–180.
- Seefeld, A. W. (2008). Triage. *Journal of Emergency Nursing*, 34(1), 9–10.
- Shacklett, M. (2014). A former CIO's take on Target CIO resigning after massive data breach. <https://www.techrepublic.com/article/a-former-cios-take-on-target-cio-resigning-after-massive-data-breach/> [Accessed 13-November-2014].
- Shamala, P., Ahmad, R., & Yusoff, M. (2013). A conceptual framework of info structure for information security risk assessment (ISRA). *SETOP'2012 and FPS'2012 Special Issue*, 18(1), 45–52.
- Sharifi, H., & Zhang, Z. (1999). A methodology for achieving agility in manufacturing organisations: An introduction. *International Journal of Production Economics*, 62(1–2), 7–22.
- Sherehiy, B., Karwowski, W., & Layer, J. K. (2007). A review of enterprise agility: Concepts, frameworks, and attributes. *International Journal of Industrial Ergonomics*, 37(5), 445–460.
- Shiaeles, S., Chryssanthou, A., & Katos, V. (2013). On-scene triage open source forensic tool chests: Are they effective? *Triage in Digital Forensics*, 10(2), 99–115.
- Shirey, J., Charng, A., & Nguyen, Q. (2013). The RITE Way to Prototype. *UX Magazine*, (Article No :980). <https://uxmag.com/articles/the-rite-way-to-prototype> [Accessed 31-December-2018].
- Stalla-Bourdillon, S., & Knight, A. (2016). Anonymous Data v. Personal Data - False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data. *Wisconsin International Law Journal*, 34(2), 284–322.
- Stufflebeam, D. L. (2000). Guidelines for developing evaluation checklists: the checklists development checklist (CDC). *Kalamazoo, MI: The Evaluation Center*. http://www.wmich.edu/sites/default/files/attachments/u350/2014/guidelines_cdc.pdf [Accessed 5-July-2018].
- Shukor, N. S. A., Iahad, N. A., & Rahman, A. A. (2017). Summative evaluation for design science artifact using structured walkthrough. In *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 1–6).
- Silic, M., & Back, A. (2014). Information security: Critical review and future directions for research. *Information Management & Computer Security*, 22(3), 279–308.
- Silverman, D. (2013). *Doing qualitative research: A practical handbook*. SAGE Publications Limited.
- Simmons, C., & Dasgupta, D. (2014). AVOIDIT: A cyber attack taxonomy. In *9th Annual Symposium on Information Assurance (ASIA'14)*. ALBANY, NY. <http://www.albany.edu/iasymposium/proceedings/2014/6-SimmonsEtAl.pdf> [Accessed 31-December-2018].
- Sisense. (2017). *How to Build a Better Dashboard: Behind the Scenes Design Workshop*. <https://ps.sisense.com/dashboard-design-video.html?alild=45737750> [Accessed 5-June-2018].
- Smith, L. D. (1985). Problems and Progress in the Philosophy of Science: An Essay Review (Larry Laudan, 'Progress and Its Problems: Towards a Theory of Scientific Growth'). *Journal of the History of the Behavioral Sciences*, 21(3), 208.
- Smith, D. M. (2003). The Cost of Lost Data - Graziadio Business Review | Graziadio Business Review | Graziadio School of Business and Management | Pepperdine University. *Graziadio Business Review*, 6(3). <http://gbr.pepperdine.edu/2010/08/the-cost-of-lost-data/> [Accessed 31-December-2018].
- Snedaker, S., & Rima, C. (2014). Chapter 8 - Emergency Response and Recovery. In *Business Continuity and Disaster Recovery Planning for IT Professionals (Second Edition)* (pp. 427–449). Boston: Syngress.
- Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3), 477–564.
- Solove, D. J. (2008). The New Vulnerability: Data Security and Personal Information. In *Securing Privacy in the Internet Age* (A. Chander, L. Gelman, and M. J. Radin). Stanford University Press. <http://ssrn.com/abstract=583483> [Accessed 5-May-2017].
- Solove, D. J., & Citron, D. K. (2016). Risk and Anxiety: A Theory of Data Breach Harms. GWU Law School Public Law Research Paper No. 2017-2; GWU Legal Studies Research Paper No. 2017-2. <https://ssrn.com/abstract=2885638> [Accessed 5-June-2018].

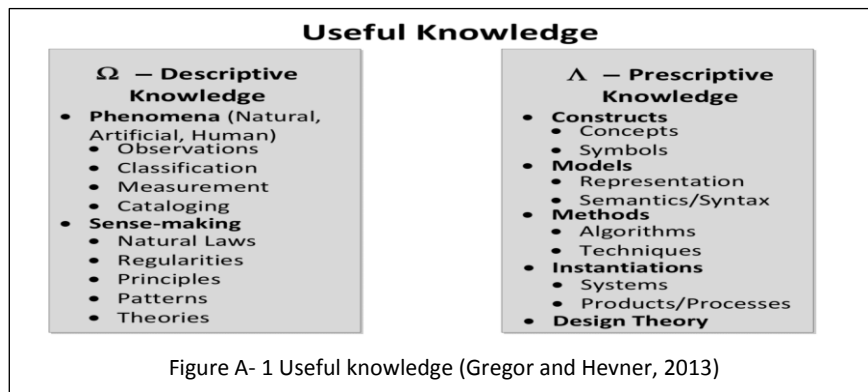
- Song, Y. J., Park, K. Y., & Kang, J. M. (2011). The Method of Protecting Privacy Capable of Distributing and Storing of Data Efficiently for Cloud Computing Environment. In *Computers, Networks, Systems and Industrial Engineering (CNSI), 2011 First ACIS/JNU International Conference on* (pp. 258–262).
- Souza De Souza, D. V. (2015). A Conceptual Framework and Best Practices for Designing and Improving Construction Supply Chains. University of Salford.
- Sophos Limited. (2013). Sophos Threatsaurus: The A-Z of Computer and Data Security Threats. <http://www.sophos.com/en-us/medialibrary/PDFs/other/sophosthreatsaurusaz.pdf>. [Accessed 31-December-2018].
- Spafford, E. H. (1989). The Internet Worm Program: An Analysis. *SIGCOMM Comput. Commun. Rev.*, 19(1), 17–57.
- Spiekermann, S., Böhme, R., Acquisti, A., & Hui, K.-L. (2015). Personal data markets. *Electronic Markets*, 25(2), 91–93.
- Spiekermann, S., Böhme, R., Acquisti, A., & Hui, K.-L. (2015). Personal data markets. *Electronic Markets*, 25(2), 91–93.
- Swan, M., & Brunswicker, S. (2018). Blockchain Economic Networks and Algorithmic Trust. In *Emergent Research Forum (ERF)*. New Orleans.
- Tan, J. H., Luan, S., & Katsikopoulos, K. (2017). A signal-detection approach to modeling forgiveness decisions. *Evolution and Human Behavior*, 38(1), 27–38.
- Tanaka-Ishii, K. (2015). Semiotics of Computing: Filling the Gap Between Humanity and Mechanical Inhumanity. In P. Trifonas (Ed.), *International Handbook of Semiotics* (pp. 981–1002). Dordrecht: Springer Netherlands.
- TED.com. (2009). *The next Web of open, linked data: Sir Tim Berners-Lee on TED.com | TED Blog* [TEDTalk Video]. Retrieved from http://www.ted.com/talks/tim_berniers_lee_on_the_next_web?language=en [Accessed 31-December-2018].
- Teelink, S., & Erbacher, R. F. (2006). Improving the Computer Forensic Analysis Process Through Visualization. *Commun. ACM*, 49(2), 71–75.
- Theoharidou, M., & Gritazalis, D. (2007). Common Body of Knowledge for Information Security. *IEEE Security & Privacy*, 5(2), 64–67.
- Tøndel, I. A., Line, M. B., & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. *Computers & Security*, 45, 42–57.
- Trope, R. L. (2019). When Incident Response Goes Awry: Cybersecurity Developments. *The Business Lawyer*, 74(1), 229–241.
- Turn, R. (1976). Classification of Personal Information for Privacy Protection Purposes. In *Proceedings of the June 7-10, 1976, National Computer Conference and Exposition* (pp. 301–307). New York, New York: ACM.
- Uma, M., & Padmavathi, G. (2013). A survey on various cyber attacks and their classification. *International Journal of Network Security*, 15(5), 390–396.
- Unger, R., & Nunnally, B. (2013). *Designing the Conversation: Techniques for Successful Facilitation*. New Riders.
- UC Berkeley. (2010). Even theories change. The Understanding Science site, UC Museum of Paleontology, University of California at Berkeley in collaboration with a diverse group of scientists and teachers, funded by National Science Foundation. [http://undsci.berkeley.edu/article/%3C?%20echo%20\\$baseUrl:%20?%3E_0/howscienceworks_20](http://undsci.berkeley.edu/article/%3C?%20echo%20$baseUrl:%20?%3E_0/howscienceworks_20) [Accessed 31-December-2018].
- Vaidya, R. (2019). Cyber Security Breaches Survey 2019: Statistical Release. DCMS: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/791940/Cyber_Security_Breaches_Survey_2019_-_Main_Report.PDF [Accessed 29-April-2019].
- Vaishnavi, V., & Kuechler, W. (2007). *Design Science Research methods and Patterns: Innovating Information and Communication Technology* (1st ed.). Boca Raton, FL, New York: Taylor & Francis Group.
- Vaishnavi, V., & Kuechler, W. (2015). *Design science research methods and patterns: innovating information and communication technology* (Second). Boca Raton: CRC Press, Taylor & Francis Group.
- Vaishnavi, V., Kuechler, W., & Petter, S. (2017). *Design Science Research in Information Systems*. Retrieved from <http://www.desrist.org/design-research-in-information-systems/>. [Accessed 5-June-2018].
- Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & Health Sciences*, 15(3), 398–405.
- Van der Merwe, A., Gerber, A., & Smuts, H. (2017). Mapping a Design Science Research Cycle to the Postgraduate Research Report. In *Annual Conference of the Southern African Computer Lecturers' Association* (pp. 293–308). Springer.
- van Deursen, N. (2013). HI-Risk: a socio-technical method for the identification and monitoring of healthcare information security risks in the information society. Napier University, Edinburgh.
- Vassell, M., Apperson, O., Calyam, P., Gillis, J., & Ahmad, S. (2016). Intelligent Dashboard for augmented reality based incident command response co-ordination. In *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)* (pp. 976–979).
- Vayer, J. S., Ten Eyck, R. P., & Cowan, M. L. (1986). New concepts in triage. *Annals of Emergency Medicine*, 15(8), 927–930..
- Venable, J. (2006). A framework for design science research activities. In *Emerging Trends and Challenges in Information Technology Management: Proceedings of the 2006 Information Resource Management Association Conference* (pp. 184–187). Idea Group Publishing.
- Venable, J., Pries-Heje, J., & Baskerville, R. (2012). A Comprehensive Framework for Evaluation in Design Science Research. In K. Peffers, M. Rothenberger, & B. Kuechler (Eds.), *Design Science Research in Information Systems. Advances in Theory and Practice* (pp. 423–438). Springer Berlin Heidelberg.

- Venkatraman, S., Sundarraj, R. P., & Mukherjee, A. (2016). Prototype Design of a Healthcare-Analytics Pre-adoption Readiness Assessment (HAPRA) Instrument. In J. Parsons, T. Tuunanen, J. Venable, B. Donnellan, M. Helfert, & J. Keneally (Eds.), *Tackling Society's Grand Challenges with Design Science* (pp. 158–174). Springer International Publishing.
- Vlastos, E., & Patel, A. (2007). An open source forensic tool to visualize digital evidence. *Computer Standards & Interfaces*, 29(6), 614–625.
- Vogt, W. P., Gardner, D. C., & Haeffele, L. M. (2012). *When to use what research design*. London; New York, N.Y.; Guilford Press.
- Vogt, W. P., Gardner, D. C., Haeffele, L. M., & Vogt, E. R. (2014). *Selecting the right analyses for your data: quantitative, qualitative, and mixed methods*. Guilford Publications.
- Wang, Y., & Nepali, R. K. (2015). Privacy impact assessment for online social networks. In *2015 International Conference on Collaboration Technologies and Systems (CTS)* (pp. 370–375).
- Wang, M., & Jiang, Z. (2017). The Defining Approaches and Practical Paradox of Sensitive Data: An Investigation of Data Protection Laws in 92 Countries and Regions and 200 Data Breaches in the World. *International Journal of Communication* (19328036), 11, 3286–3305.
- Ware, C. (2012). *Information visualization: perception for design* (3rd Edition). Boston: Morgan Kaufmann.
- Werlinger, R., Botta, D., & Beznosov, K. (2007). Detecting, analyzing and responding to security incidents: a qualitative analysis. In *Proceedings of the 3rd symposium on Usable privacy and security* (pp. 149–150). ACM.
- White & Black Ltd. (2016). Civil damages for distress in data protection cases after Vidal-Hall [Blog]. <https://www.wablegal.com/civil-damages-distress-data-protection-cases-vidal-hall/> [Accessed 31-August-2018].
- Wilkinson, A., & Eidinow, E. (2008). Evolving practices in environmental scenarios: a new scenario typology. *Environmental Research Letters*, 3(4), 045017.
- Willig, C. (2013). *Introducing qualitative research in psychology*. McGraw-Hill Education (UK).
- Williams, M., Axon, L., Nurse, J. R. C., & Creese, S. (2016). Future scenarios and challenges for security and privacy. In *2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI)* (pp. 1–6).
- Williams, R., McMahon, E., Samtani, S., Patton, M., & Chen, H. (2017). Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach. In *Intelligence and Security Informatics (ISI), 2017 IEEE International Conference on* (pp. 179–181). IEEE.
- Wilson, L. O., Wilson, F. P., & Wheeler, M. (1981). Computerized triage of pediatric patients: Automated triage algorithms. *Annals of Emergency Medicine*, 10(12), 636–640.
- Wilson, J. M. (2013). *Cybersecurity Protection: Design Science Research toward an Intercloud Transparent Bridge Architecture (ICTOBRA)*. Capella University.
- Wohlin, C., Runeson, P., da Mota Silveira Neto, P. A., Engström, E., do Carmo Machado, I., & de Almeida, E. S. (2013). On the reliability of mapping studies in software engineering. *Journal of Systems and Software*, 86(10), 2594–2610.
- Woods, L. (2017). United Kingdom: Heading towards Brexit but with a Data Protection Bill Implementing GDPR Reports: GDPR Implementation Series. *European Data Protection Law Review (EDPL)*, 3(4), 500–506.
- Woskov, S. M., Grimaila, M. R., Mills, R. F., & Haas, M. W. (2011). Design considerations for a case-based reasoning engine for scenario-based cyber incident notification. In *2011 IEEE Symposium on Computational Intelligence in Cyber Security (CICS)* (pp. 84–91).
- World Economic Forum. (2011). *Personal Data: The Emergence of a New Asset Class*. http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf. [Accessed 10-October-2016].
- World Economic Forum. (2012). *Partnering for Cyber Resilience*. http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf [Accessed 18-October-2018].
- World Economic Forum. (2014). *Global Risks 2014 Ninth Edition*. World Economic Forum. http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf. [Accessed 23-July-2015].
- Wright, C. S., & Zia, T. A. (2011). Using checklists to make better best (pp. 245–251). Presented at the Proceedings of the 9th Australian Information Security Management Conference.
- Wright, D. (2011). Should Privacy Impact Assessments Be Mandatory? *Commun. ACM*, 54(8), 121–131.
- Wright, D., Finn, R., & Rodrigues, R. (2013a). A comparative analysis of privacy impact assessment in six countries. *Journal of Contemporary European Research*, 9(1), 160–180.
- Wright, D., Gellert, R., Gutwirth, S., & Friedewald, M. (2011). Minimizing Technology Ricks with PIAs, Precaution, and Participation. *IEEE Technology and Society Magazine*, 30(4), 47–54.
- Wright, D., & Raab, C. (2014). Privacy principles, risks and harms. *International Review of Law, Computers and Technology*, 28(3), 277–298.
- Wright, D., Wadhwa, K., Lagazio, M., Raab, C., & Charikane, E. (2013). *Privacy impact assessment and risk management* (Report for the Information Commissioner's Office). Trilateral Research & Consulting.
- Xu, D., & Ning, P. (2005). Privacy-preserving alert correlation: a concept hierarchy based approach. In *21st Annual Computer Security Applications Conference (ACSAC'05)* (pp. 10 pp. – 546).
- Yigitbasiglu, O. M., & Velcu, O. (2012). A review of dashboards in performance management: Implications for design and research. *International Journal of Accounting Information Systems*, 13(1), 41–59.

- Yu, E. (2011). Modelling strategic relationships for process reengineering. *Social Modeling for Requirements Engineering*, 11, 2011.
- Zhang, H., & Ali Babar, M. (2013). Systematic reviews in software engineering: An empirical investigation. *Information and Software Technology*, 55(7), 1341–1354.
- Zhang, H., Babar, M. A., & Tell, P. (2011). Identifying relevant studies in software engineering. *Special Section: Best Papers from the APSECBest Papers from the APSEC*, 53(6), 625–637.
- Zhou, L., Vasconcelos, A., & Nunes, M. (2008). Supporting decision making in risk management through an evidence-based information systems project risk checklist. *Information Management & Computer Security*, 16(2), 166–186.
- Zhu, Z., Wang, G., & Du, W. (2009). Deriving Private Information from Association Rule Mining Results. In *2009 IEEE 25th International Conference on Data Engineering* (pp. 18–29).

Appendices

Appendix A: DSR knowledge



Knowledge form	Research Study
Classify knowledge based on its materialism, i.e. where it exists and in which shape.	
Explicit knowledge, that is, knowledge articulated, expressed, and recorded in media such as text, numbers, codes, formula, musical notations, and video tracks.	Interview study; User Evaluation Study
Embodied knowledge, that is, knowledge situated in the minds of people and often difficult to express in an explicit way	Interview study
Embedded knowledge, that is, knowledge that resides not in humans but in entities, such as physical objects, processes, routines, or structures	User Evaluation Study

Figure A- 2 DSR knowledge form (Johannesson and Perjons, 2014, p 21-28)

Knowledge types	Triage Playbook
Classify knowledge based on its different purposes.	
Definitional knowledge, which includes concepts, constructs, terminologies, definitions, vocabularies, classifications, and taxonomies.	Definition of privacy harm in terms of data harm assessment matrix. The data harm matrix uses scoring and classification of entities of data harm i.e. types and sensitivities of personal data, categories of individuals and security protection measures.
Descriptive knowledge, which describes and analyses an existing or past reality.	Description of triage in terms of a sequence of steps and using Peirce ternary of Firstness, Secondness and Thirdness to structure and explain the sequence.
Predictive knowledge, which offers black-box predictions, i.e. it predicts outcomes based on underlying factors but without explaining causal or other relationships between them.	Dashboard
Prescriptive knowledge, which consists of prescriptive models and methods that help to solve practical problems.	Checklists for PHA; Designing and constructing a triage playbook to address the problems associated with data harm assessment and breach notifications during initial DBI response.

Figure A- 3 DSR knowledge types (Johannesson and Perjons, 2014, p 21-28)

Appendix B: This research referenced by sources

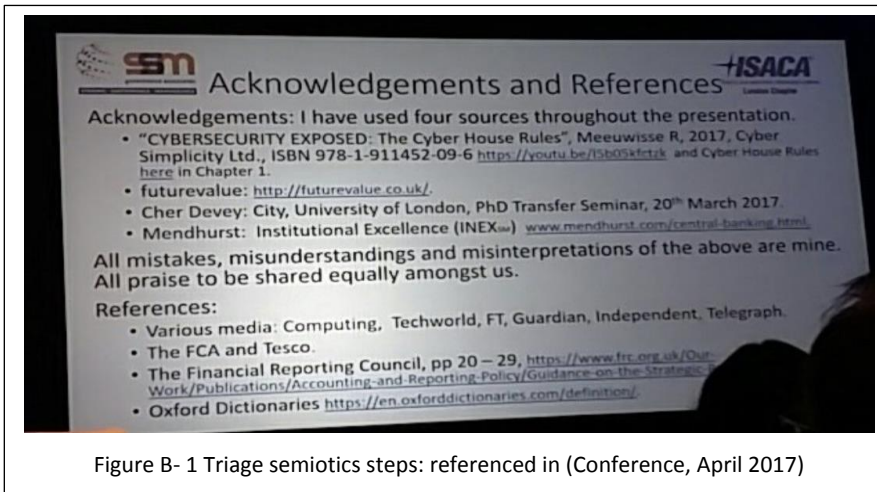


Figure B- 1 Triage semiotics steps: referenced in (Conference, April 2017)

This email was also forwarded to supervisors on 9 February 2018.

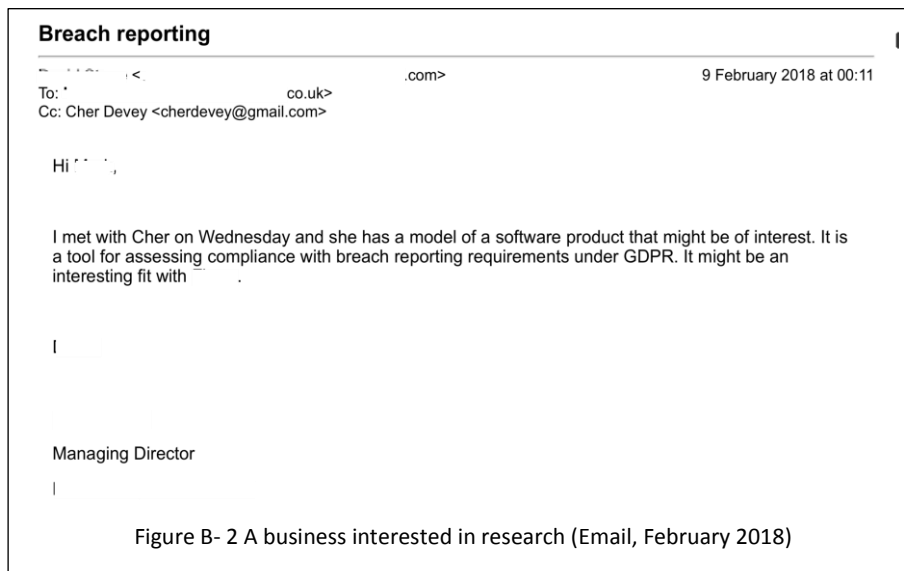


Figure B- 2 A business interested in research (Email, February 2018)

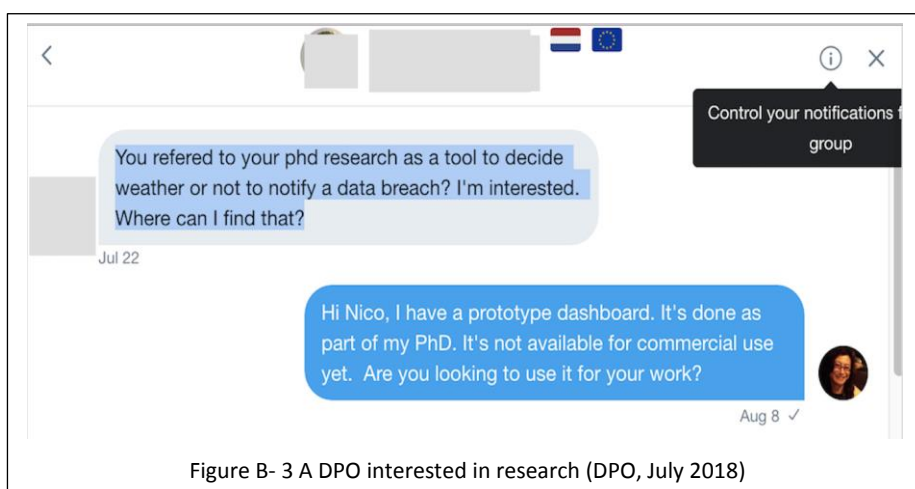
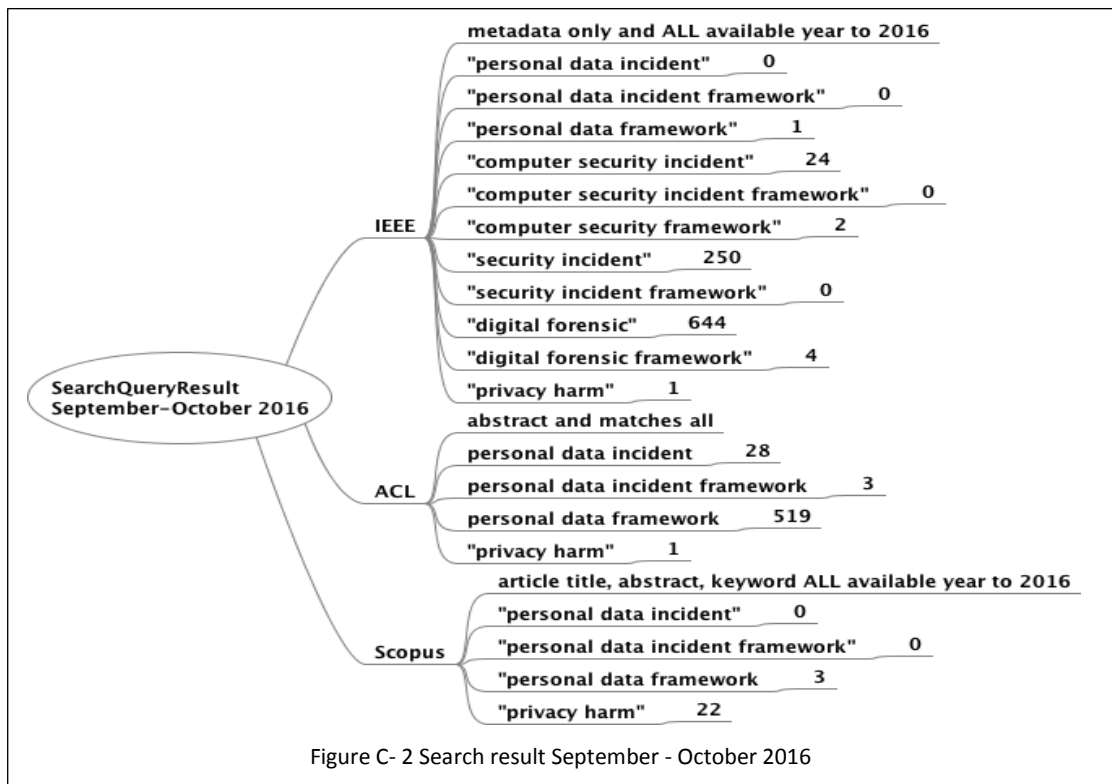
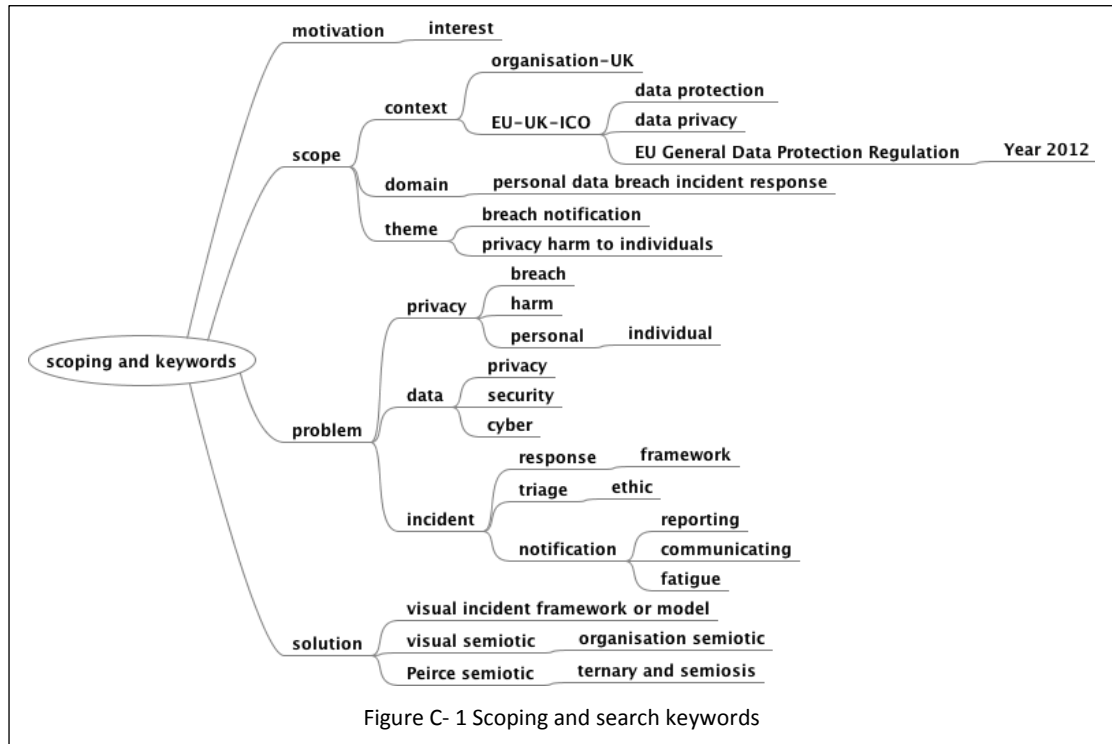
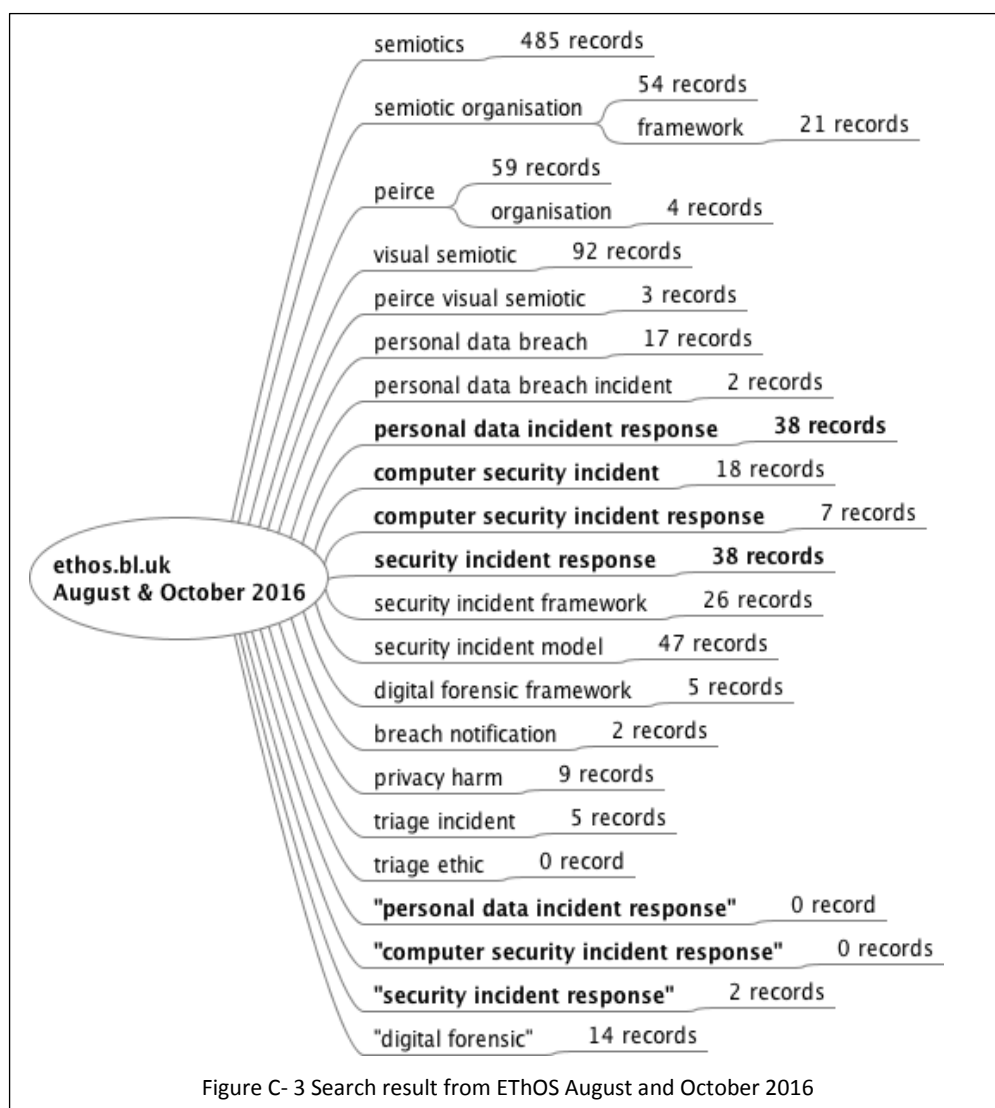


Figure B- 3 A DPO interested in research (DPO, July 2018)

Appendix C: SSM search scope and results





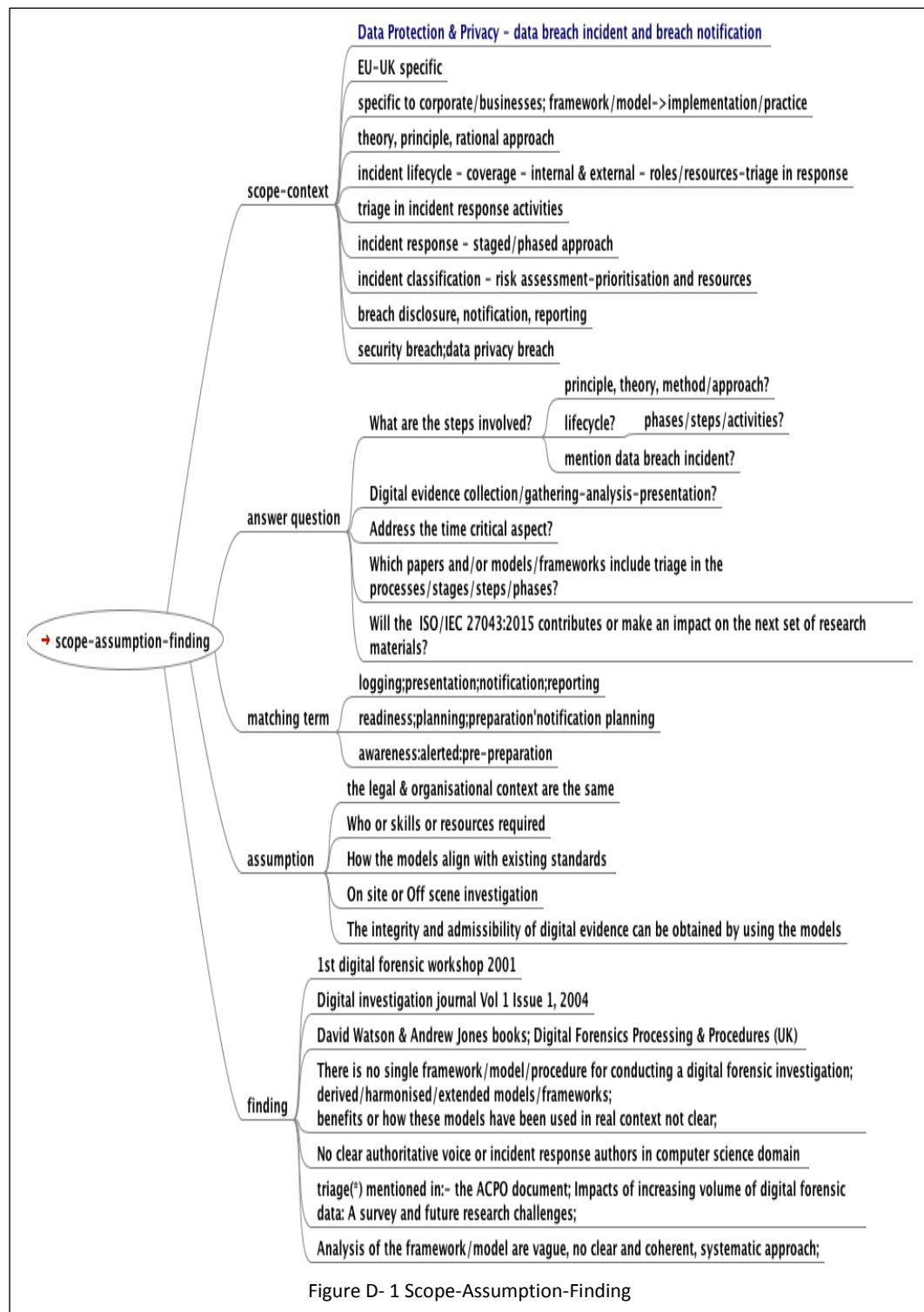


Figure D- 1 Scope-Assumption-Finding

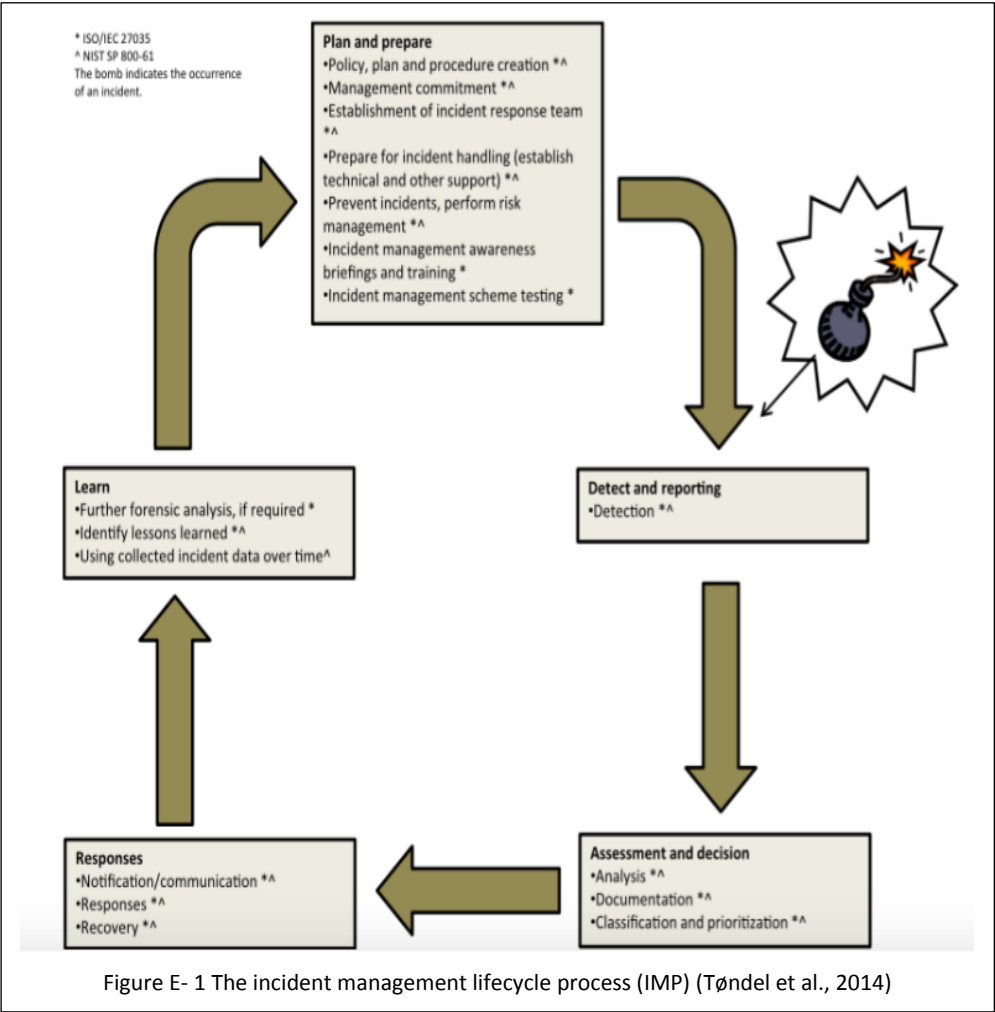
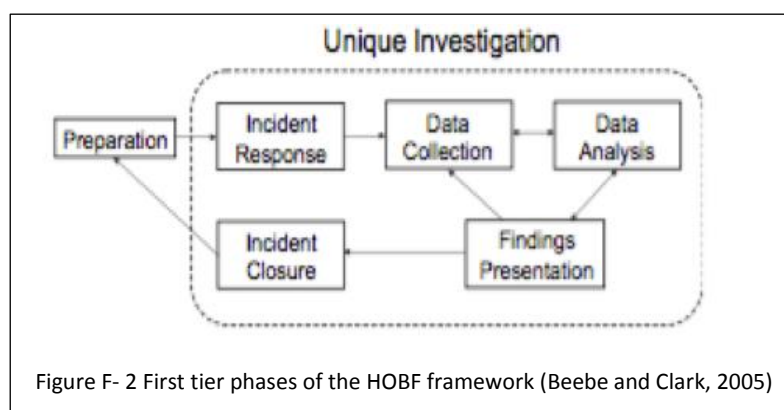
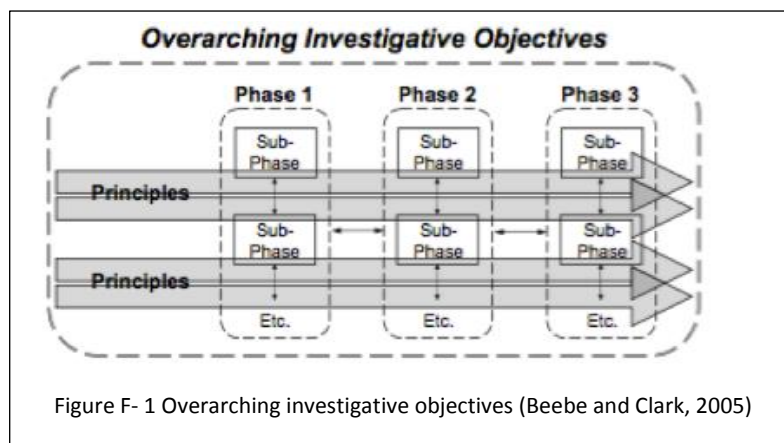


Figure E- 1 The incident management lifecycle process (IMP) (Tøndel et al., 2014)



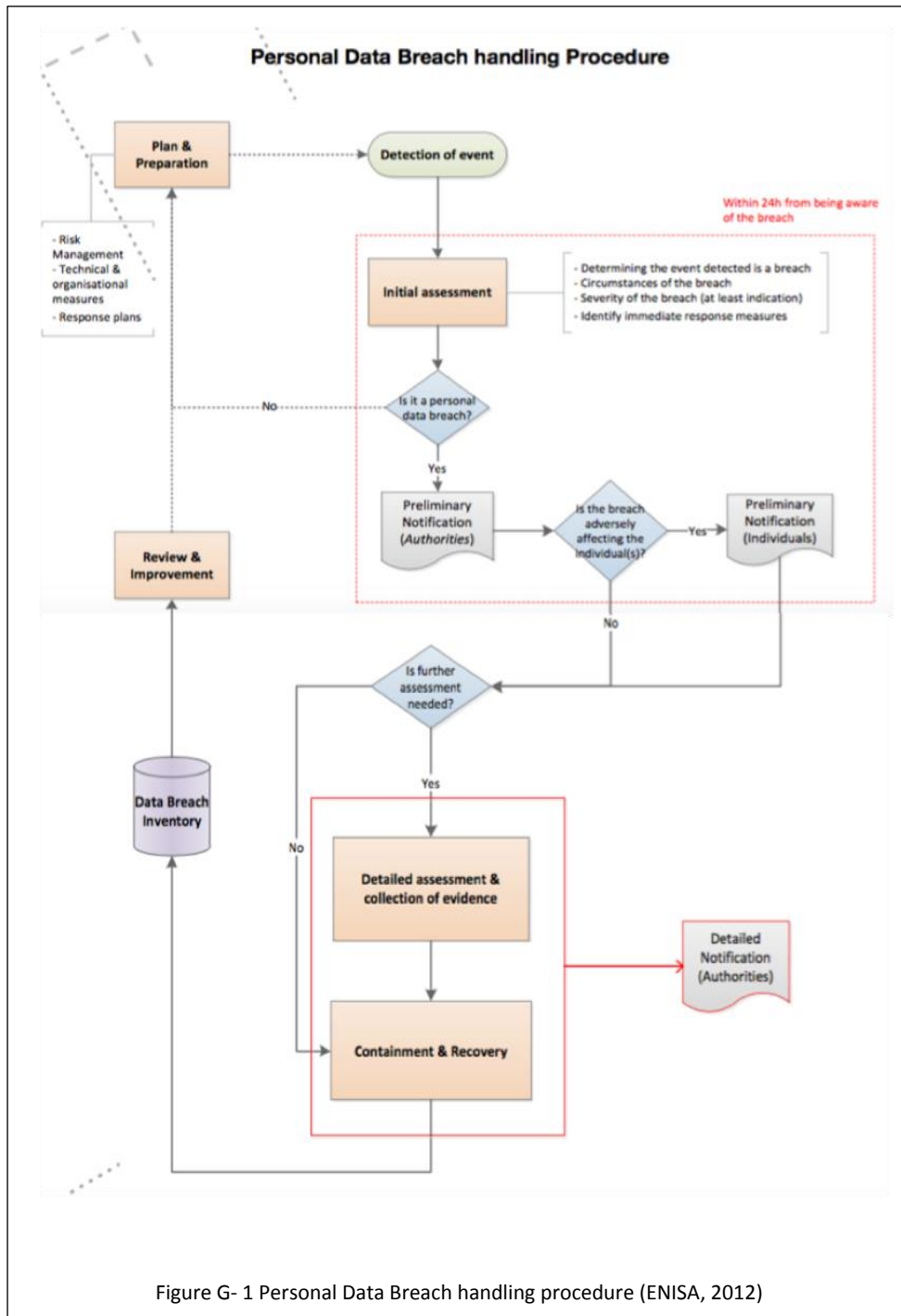


Figure G- 1 Personal Data Breach handling procedure (ENISA, 2012)

Appendix H: Interview Study: planning, designing and conducting

H-1: Elicitation and dialogue

To achieve the overall aims of the interview study, the interview questions¹⁸⁸ were also such that they both provide a guiding process or dialogue for conducting the interview, as well as enabling the elicitation of interviewees' needs and/or problems surrounding the research topics of interest. With this in mind, Berger (2016, p 199) viewed the structure of interviews and conversations as a stream of: Q&A, Q&A, Q&A, Q&A. These resemble an ordinary conversation or dialogue. But in an ordinary dialogue, the answers are usually longer than the question. Hence interviews potentially allow more detailed information to be elicited (Berger 2016, p 200). Burns (2000, p 425) declared that the interviewee has equal status to the researcher in the dialogue rather than being a guinea pig.

In a study on requirements elicitation by Goguen and Linde (1993), the researchers revealed that although interviews and questionnaires are widely used, in fact conversation, interaction, and discourse analysis are more detailed and precise, and hence more likely to be accurate. However, in pointing out that there is absolutely no agreement among experts on how best to elicit information or knowledge, Davis et al. (2006) argued that interviews which are preferentially structured appear to be one of the most effective elicitation techniques in a wide range of domains and situations.

In the social science literature interviewing as an instrument for dialogue allows the researcher to frame questions for a good conversation (Kvale, 2007) with the interviewee to elicit information around the research themes. These are unlike other forms of methods, such as a survey, which lacks the medium for personal interaction to elicit with probing and follow-up type questions as the stories unfold with new insights during an interview (Kvale, 2007). Gillham (2000, p 48), suggested that semi-structured interviews are suited for sensitive or subtle topics. This is so as semi-structured interviews usually have a set of questions that guide the interview rather than dictate its direction. This is unlike structured interviews, where the questions are fixed, or unstructured interviews with no set agenda (Bryman and Bell, 2015, p 480-483).

Gillham (2000a, p 9) suggested that face-to-face interviews are suitable when the material is sensitive in character, confidentiality may be an issue, depth of meaning is central, and the research aims require insight and understanding. Face-to-face interviews provide direct access to experts in the subject matter. Such interactive face-to-face dialogue, through open and semi-structured questions, provides the researcher with descriptions, narratives and texts, to interpret and report according to the topic of interests or research (Kvale, 2007) and (Gubrium and Holstein, 2001).

To enhance and improve the overall quality of this semi-structured, organised and yet informal dialogue style interviews, interviewees were treated as being contributing interviewees in the research, rather than objects only answering pre-defined question. This study followed the approach by Hove and Tårnes (2013), informal in the sense that this researcher adopted an open mind to be prepared for twists and surprises and by being present and showing interest in the interviewee's responses. This is so, as no matter how thorough in planning and preparation, there will be challenges during the execution of the interviews. Being a powerful data gathering technique, conducting an interview also has potential pitfalls (Myers and Newman, 2007). However advanced planning was done to address or mitigate pitfalls.

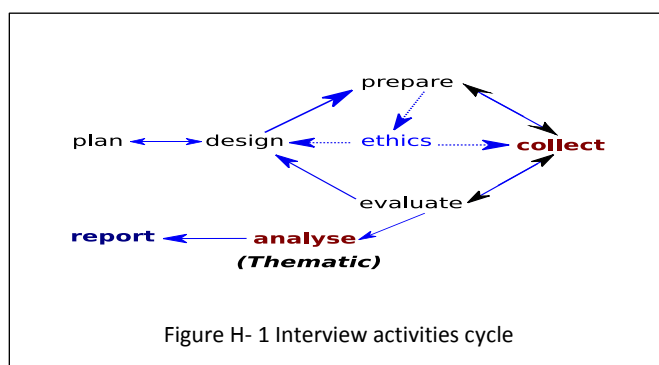
H-2: Planning the interview

To begin with, like any other data collection methods, pre-planning and preparation are essential to ensure that the overall aims of the interviews are achieved. Accordingly, a six stage semi-structured interview guideline as given by Rabionet (2011) was aimed at: (a) selecting the type of interview; (b) establishing ethical guidelines, (c) crafting the interview protocol; (d) conducting and recording the interview; (e) analysing and summarising the interview; and (f) reporting the findings.

Willig (2013, p 29) in stating that semi-structured interviewing requires careful preparation and planning, suggested these questions to think through: who to interview (and why), how to recruit interviewees, how to record and transcribe the interview, what style of interviewing to use, and what to ask interviewees. Rabionet (2011) and Willig (2013, p 29) guidelines and suggestions were adopted for this study as outlined in *designing the interview questions, selecting participants and conducting the interview*. The overall activities of the research interviews cycle¹⁸⁹ are shown in Figure H- 1 p 218.

¹⁸⁸ These were the questions in the interview scripts which were framed from the interview study questions.

¹⁸⁹ The activities followed those outlined in Hove and Tårnes (2013) with alteration for this research.



The evaluate step was to check that the overall interview design, the preparation, and the collected (recorded) interview data were all working according to plan. Ethics (including privacy concerns) as shown in the interviews cycle - with the paths indicating the steps before the start of the interviews with interviewees (collect data) - to remind of the need to be mindful throughout the interview processes.

Planning of the interviews started in late June 2016. On 9th May 2016, CSREC approved the research interviews. The CSREC ethics application¹⁹⁰ included: approval for contacting interviewees, the recruiting process (i.e. *who I am interviewing?*), the nature of the interviews and questions (*what data I am collecting? what are the questions?*), the participant (interviewee) notes and ethics consent form for the participants.

H-3: Designing the interview questions

In interviews, involving people as participants; in hearing their voices, recording, interpreting and analysing the data, conflicts of interest may arise (Bold 2012, p 61). Building trust in the overall interview cycle is key for ensuring that such conflicts are avoided. Hove and Tårnes (2013) suggested to build trust with interviewees to overcome the issues of withholding of information that could be of value to the study. The authors recommended proper planning with well-designed interview questions to guide the process, and most importantly, informing interviewees that confidentiality and anonymity will be maintained. Myers and Newman (2007) provided some pointers for preparing the interview script which should involve at a minimum: 1) *Preparing the opening – introducing yourself etc.* 2) *Preparing the introduction – explaining the purpose of the interview. Preparing the key questions.* 3) *Preparing the close – if needed, asking permission to follow-up, or asking who else the interviewee recommends might be interviewed.*

As part of crafting the interview questions, Payne (1951) was invoked to help with designing the questions. In framing the interview scripts, the overall aim of the study drove the designing of the interview questions (as shown in the interview scripts). The outcome was the interview scripts¹⁹¹ shown in Appendix I p 221 which followed the suggestion by Myers and Newman (2007). As discussed in Section H-6, the interview scripts were subsequently revised (Appendix J p 223) after five interviews. The interview scripts were discussed with supervisors, and also with an experienced security consultant. The interview scripts were altered/modified to enhance the elicitation of interviewee's experience of DBI by prompting for hypothetical cases or incidents. The hypothetical question needs to be framed such that the personal data breach incident may not have occurred, or the interviewee has no direct exposure or interaction with the incidents when it occurred. This is another case of improvisation. It is the nature of interview research that researchers need to improvise or make adjustment either to the questions to align with the sample population or change the sample size. This was raised by Vogt et al. (2012, p 155), who stated: whatever your plan for finding potential interviewees and selecting among them, you will execute it imperfectly. Vogt et al. (2014, p 45) in suggesting that one should have a general (interview dialogue) in mind, but when faced with the unexpected, improvisation is needed; this is one of the strengths of a good interviewer.

H-4: Selecting interviewees

Originally only a minimum of five and maximum of seven interviewees were planned for. However, after five interviews, the collected data did not have the breadth of coverage for exploring the extent and nature of DBI across the industry sectors i.e. the sampling frame was too small for the intended population. As the nature of the study was exploratory, and the scope was to gather data across industry sectors, the population under study also needed to match the requirements for breath of knowledge and information.

It is important to stress here again that the number of voluntary interviewees was limited because of their company understandable wishes not to disclose inside information. Vogt et al. (2012, p 156) also remarked that several good texts on interview research focused on how to conduct interview research but little guidance was given on whom to interview or on sampling and recruitment methods. Although, Vogt et al. (2012, p 156) provided interview sampling guidance as listed in a table on p 157-158, *the number of sample size was not stated*, just text description for what to prepare for when questions are exploratory.

¹⁹⁰ The guiding questions for the ethics application were suggested by Prof. Stephanie Wilson.

¹⁹¹ Dr. David Haynes provided helpful notes, interview templates and suggestions on the designing of the interview questions.

This researcher's approach on participant sampling was intuitive and ad hoc. After only five interviews, a need was found to make adjustments to the sample size and also the interview questions (as described in Section H-6). More candidates were recruited following the discovery that more than seven interviewees were needed. This is the spontaneous nature of the qualitative inquiry. Sandelowski (1986), in referencing other sources, added that sample sizes in qualitative research are frequently small because of the large volume of verbal data that must be analysed. As sampling is often theoretical rather than statistical, the size is not predetermined as it is dependent on the nature of the data collected and where those data take the investigator (Sandelowski, 1986). Such theoretical sampling is described by Ritchie et al. (2014, p 117) under the general heading of purposive sampling in qualitative research. The term purposive refers to the use of prescribed selection criteria where samples are usually small in size - *if the data are properly analysed, there will come a point where very little new evidence is obtained from each additional fieldwork unit* (Ritchie et al., 2014, p 117). Ritchie et al. (2014, p 116) further introduced the principle of qualitative sampling as the requirement for *symbolic representation*; because a unit is chosen both to *represent* and *symbolise* features of relevance to the investigation.

Although the sample size was small, the sampling was as diverse as possible within the defined population, and the units (candidates) were chosen because they typified a circumstance or hold a characteristic that was expected or known to have salience to the subject matter under study. These constituted the two requirements for using the prescribed selection criteria (Ritchie et al., 2014, p 116). Hence candidates with diverse roles and responsibilities associated with the subject matter under study, and across the industry sectors were targeted for interviews.

Senior professional managers and individuals with the relevant job titles, roles or responsibilities in organisations/businesses around/in London locations were recruited or invited via professional networks and at conferences/seminars across industry sectors. Also, interviewees were asked to help encourage colleagues to participate or introduce their contacts (referred to as snowballing). Initial screening of suitable candidates was conducted via emails or Skype chats. Only candidates that meet the roles and/or job titles with the relevant responsibilities - held in senior positions were invited. Specifically, the following key people/roles were targeted: Data Compliance Officers; Data Protection Officers; Security Incident Responders; Data Governance Managers; Cybersecurity Incident Responders; IT or Information Security auditors; Digital Forensics Investigators; or those in any roles or responsibilities for managing or planning their organisation's personal data breach, information security or cybersecurity incidents.

Invitation emails confirming the date, venue of the meeting and notes about the interview (participant notes) with the consent form were sent out during May, June and July 2016¹⁹². Interviewees were also informed about the audio-recording, face-to-face or Skype, and the one hour for the interview.

Candidates were also reassured that their confidentiality and privacy are important and fully respected, and all interview materials would be kept confidential. This was to enhance or build trust with the potential interviewees. Furthermore, when candidates asked for clarification about the nature of the research topics, further supporting information was given. This kind of information exchange also helped to allay fear, making the recruitment process more effective.

H-5: Pseudonymisation of data

Each interviewee was uniquely identified by: a) the industry sector code and b) a number (the interview sequence number). The recorded interviews themselves were uniquely identified by a) the date of the interview and b) a number (the interview sequence number). For example, the first interview with an interviewee from the finance sector on 15-June-2016 has the following coding and data files:

- Interviewee profile: F1
- transcribed file: 15june2016-1
- recorded file: 15june2016-1 (if more than one recording, numbering with -1a, -1b etc. Only one transcribed file for multiple recordings. Multiple recordings were needed for five interviewees due to interruptions during the interview sessions.

The above coding schemes also ensured that the individuals and companies were not identifiable, and all such identifiable data and information were replaced with pseudonyms in the transcribed files and in all results and report files. All audio files were transcribed line-by-line (mostly verbatim).

In this report pseudomisation means that any information that indirectly or directly identifies individuals and individual organisations is deleted or changed. In a face-to-face interview, as the interviewees' identities (anonymity) are known to the researcher, and the promise not to disclose (maintain confidentiality) are taken into consideration when conducting and analysing the data. Privacy covers anonymity and confidentiality. During the study the data is only available to this researcher and the supervisors. All recordings and any sensitive files will be deleted at the end of this study.

H-6: Conducting the interview

Myers and Newman (2007) and Rabionet (2011) guidelines provided the overall interview approach. Gillham (2000a, p 47) was also referenced to further guide the framing, reflecting and probing of questions during

¹⁹² One interview was in August and another in November 2016. Interviewees were unable to do interviews during the planned months.

the interviews. For example, supplementary questions (probes) to clarify or extend the response; or remind respondents of points that they have/have not raised (framing and prompts). The interviewer's control is of direction, topics covered, and their order; the actual content is determined (induced) by the interviewee (Gillham 2000a, p 47).

Gillham (2000a, p 53) and Bryman and Bell (2015, p 272), also suggested piloting the interview to check that the research instrument as a whole functions well. One pilot was conducted with a non-subject matter expert primarily to test the duration required for raising all the questions, and to set up and test Skype calls and the recording function. However, one Skype interview went disastrously wrong in that the recording had no sound track even though the file size and recorded duration indicated the conversation was properly recorded. Prior to this incident, other Skype conversations went smoothly. The rest of the interviews were face-to-face and conducted in interviewees' offices, except two interviews at City, University of London, and two interviews in public spaces (the British Library and in a café).

After the first interview, two diagrams were introduced to help show the nature of incident responses, especially in relation to the overall incident management lifecycle. This was done as the first interviewee suggested that more information about the study was needed. However, one diagram i.e. Appendix E, Figure E- 1 p 214, was deemed as suitable for use following discussions with the supervisors.

Prior to conducting the interviews, the duration of the interviews was planned for maximum of one hour. As pointed out by Burns (2000, p 426) with semi-structured interviews, the verbosity of the interviewees, their willingness to talk, and the value of what they are saying meant that the length (and the number of interview sessions) cannot be fixed rigidly.

The revised interview scripts were listed Appendix J p 223. As five interviewees were already completed, based on the initial sets of questions, further recruitment of interviewees, again based on the purposive sampling approach as described in Section H-4 p 218, were conducted to collect more data. The original interviews plan and schedule were changed to accommodate more interviews.

Appendix I: Interview scripts (original)

Preliminaries

Consent form signed?

Interview with [Name] of [Organisation] on [Date]

Interviewee [Job title] and [Role/Responsibility]

A. Background questions

- Current job title, role/responsibility or position.

- 1) What is your job title?
- 2) How long have you been with your organisation?
- 3) What is your role/responsibility?
- 4) Have you been in your current role for long?

For business owners/consultants: What kind of business is it? How long have you been in this business?

B. Views and experiences on personal data incident response

- Use of the terms 'personal data' and 'personal data breach'.

- 1) What do you regard as 'personal data'?
- 2) When you hear the term 'personal data breach', what comes to your mind?

- Personal data incident response experiences in your career.

- 3) What kinds of response activities do you think of for personal data breach incidents?
- 4) Please share some of your experiences or stories of responses to personal data breach incidents, that you are legally allowed to disclose, without naming companies or individuals.

C. Your organisation's personal data breach incident response plan

- Personal data breach incident response guidelines, procedures or frameworks.

- 1) How does your organisation respond to personal data breach incidents?
 - a) Can you please give an example?
 - b) Why did you pick that example?
 - 2) What guideline, procedure or framework does your organisation use for responding to a personal data breach incident, if any?
 - a) How efficiently does it function?
 - b) How effective is it, operationally?
 - c) Is it possible to have a copy, if you have access to it?
 - d) If you cannot authorise it, who can I ask, please?
 - 3) If none are in use, what are the reasons or issues?
 - 4) If you do not use any guideline, procedure or framework now, will you be looking to adopt and implement one?
- Prioritisation approaches for a personal data incident response.
- 5) How do you distinguish a personal data breach incident from a security breach incident?
 - 6) It has been suggested by an incident response research authority/agency that personal data breach incident response should be done in phases;
 - a) Do you respond in phases?
 - b) What are these?
 - c) What are your overall view?

- 7) What are the criteria for prioritising your personal data incident responses?
- D. Views and concerns on the EU General Data Protection Regulation
 - Potential effects on your organisation's personal data breach incidents response posture.
- 1) Regarding the new EU General Data Protection Regulation (GDPR) that is due for implementation in 2018, please describe your views and concerns as to how this legislation will affect your organisation's personal data breach incident response posture? [Supplementary notes on the EU GDPR].
- Notification, privacy harm and principles.
- 2) Although under Principle 6 on the rights of the individuals as stated in the UK DPA 1998, there is no obligations to notify affected individuals when there is a personal data breach;

What are your views on notification to individuals whose data has been compromised due to accidental or unintentional security breaches?

- 3) According to the Information Commissioner Office (ICO), organisations should review the personal data they hold, and assess how valuable, sensitive or confidential it is, and what damage or distress could be caused to individuals if there were a security breach. These consequences are referred to as privacy harm, i.e. the physical, moral and financial harms associated with the personal data breach incidents.

What types of privacy harm have you encountered or dealt with i.e. physical, moral, financial or otherwise?

- 4) Would you consider other data processing principles such as those that include ethics for addressing privacy harm when responding to personal data breach incidents?
- E. Your closing remarks about this interview
- 1) Is there anything else that you would like to add?
- 2) Can you please also suggest other people or organisations that you think should be consulted as part of this study? Can I mention your name?

Appendix J: Interview scripts (revised)

Preliminaries

Consent form signed?

Interview with [Name] of [Organisation] on [Date]

Interviewee [Job title] and [Role/Responsibility]

Switch recorders ON

Brief description of research studies; focusing on the response phase - show the generic Incident Lifecycle/Management diagram.

A. Background questions

- Current job title, role/responsibility or position.

- 1) What is your job title?
- 2) How long have you been with your organisation?
- 3) What is your role/responsibility?
- 4) Have you been in your current role for long?

For business owners/consultants:

What kind of business is it?

How long have you been in this business?

B. Views and experiences on personal data incident response

- Use of the term 'personal data'.

- 1) What do you regard as 'personal data'?

- Personal data incident response experiences in your career.

- 2) What kinds of response activities do you think of for personal data breach incidents?

- Hypothetical case of how your organisation respond to a personal data incident

- 3) What if (or when) your organisation has a personal data breach incident, how would your organisation respond? or Imagine you have a personal data breach incident in your organisation, how would your organisation respond?

C. Your organisation's personal data breach incident response plan

- Personal data breach incident response guidelines, procedures or frameworks.

- 1) What guideline, procedure or framework does your organisation use for responding to a personal data breach incident, if any?

- a) How efficiently does it function?

- b) How effective is it, operationally?

- c) Is it possible to have a copy, if you have access to it?

- d) If you cannot authorise it, who can I ask, please?

- 2) If none are in use, what are the reasons or issues?

- 3) If you do not use any guideline, procedure or framework now, will you be looking to adopt and implement one?

- Prioritisation approaches for a personal data incident response.

- 4) How do you distinguish a personal data breach incident from a security breach incident?

- 5) It has been suggested by an incident response research authority/agency that personal data breach incident response should be done in phases;

- a) Do you respond in phases?

- b) What are these?

c) What are your overall view?

6) What are the criteria for prioritising your personal data incident responses?

D. Views and concerns on the EU General Data Protection Regulation

- Potential effects on your organisation's personal data breach incidents response posture.
- 1) Regarding the new EU General Data Protection Regulation (GDPR) that is due for implementation in 2018, please describe your views and concerns as to how this legislation will affect your organisation's personal data breach incident response posture?
- Notification, privacy harm and principles.
- 2) Although under Principle 6 on the rights of the individuals as stated in the UK DPA 1998, there is no obligations to notify affected individuals when there is a personal data breach;

What are you views on notification to individuals whose data has been compromised due to accidental or unintentional security breaches?

Under the GDPR, organisations have an obligation to notify affected individuals of a personal data breach.

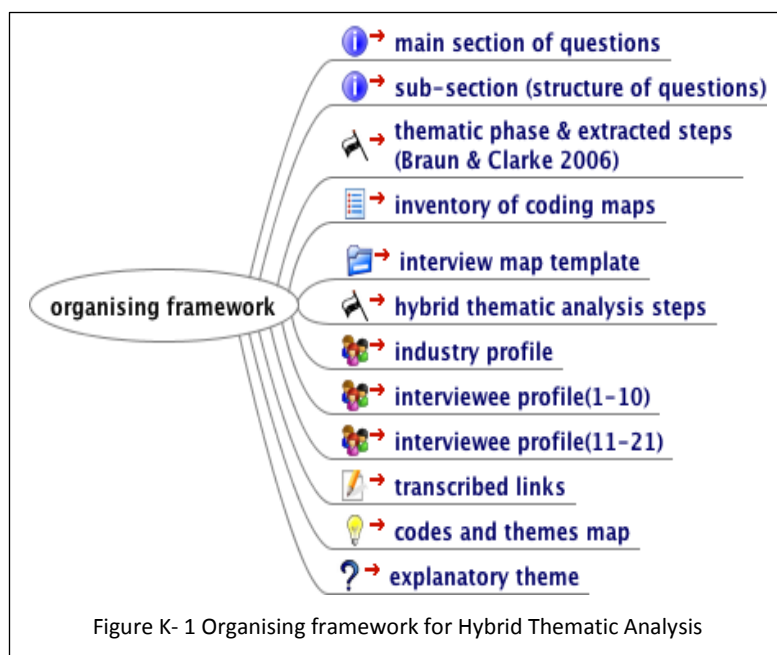
- 3) According to the Information Commissioner Office (ICO), organisations should review the personal data they hold, and assess how valuable, sensitive or confidential it is, and what damage or distress could be caused to individuals if there were a security breach. These consequences are referred to as privacy harm, i.e. the physical, moral and financial harms associated with the personal data breach incidents.

What types of privacy harm have you encountered or dealt with i.e. physical, moral, financial or otherwise?

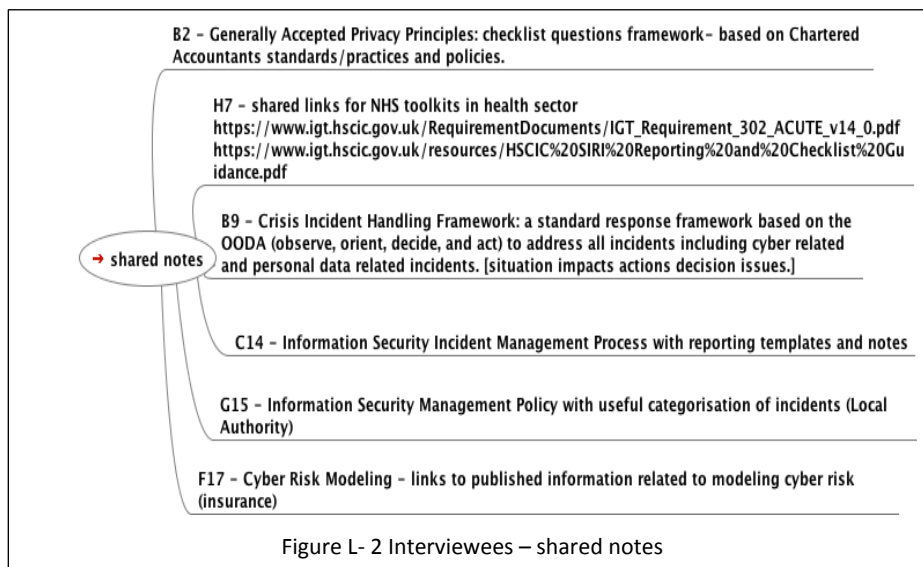
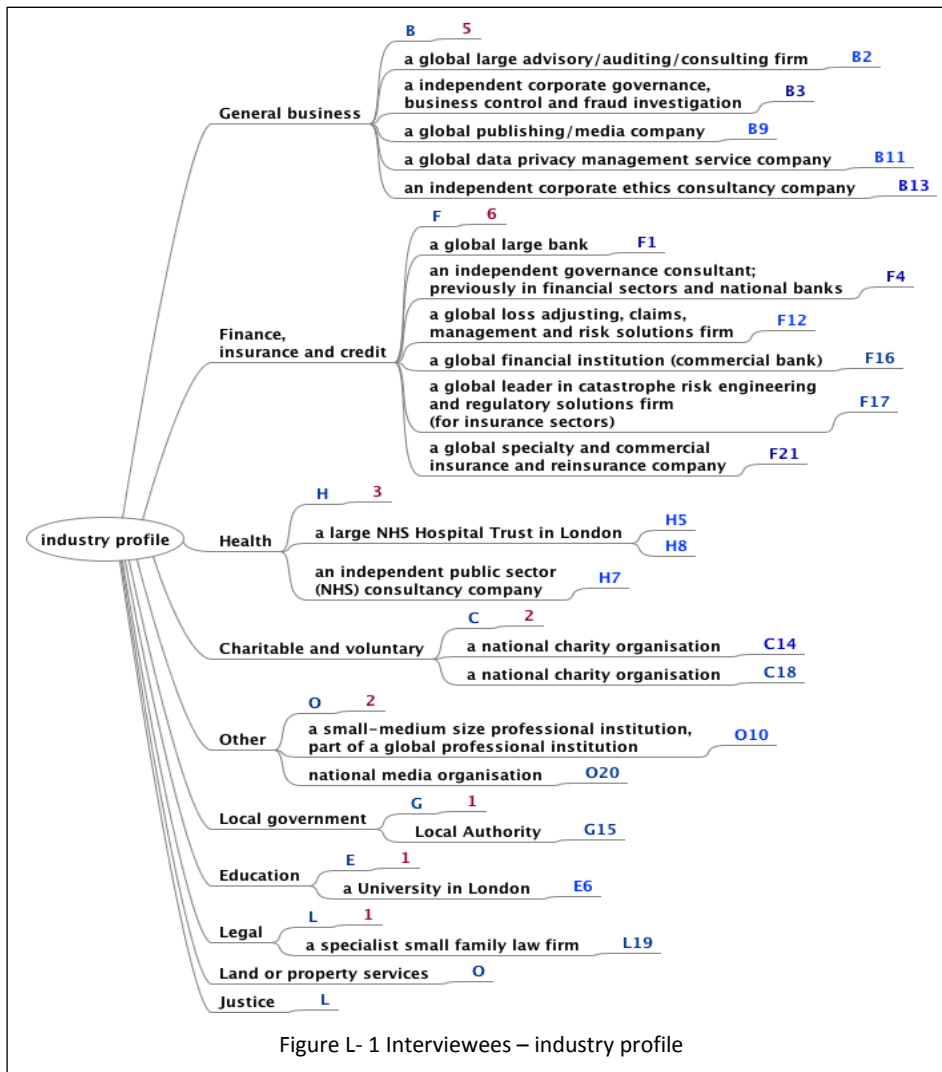
- 4) Would you consider other data processing principles such as those that include ethics for addressing privacy harm when responding to personal data breach incidents?

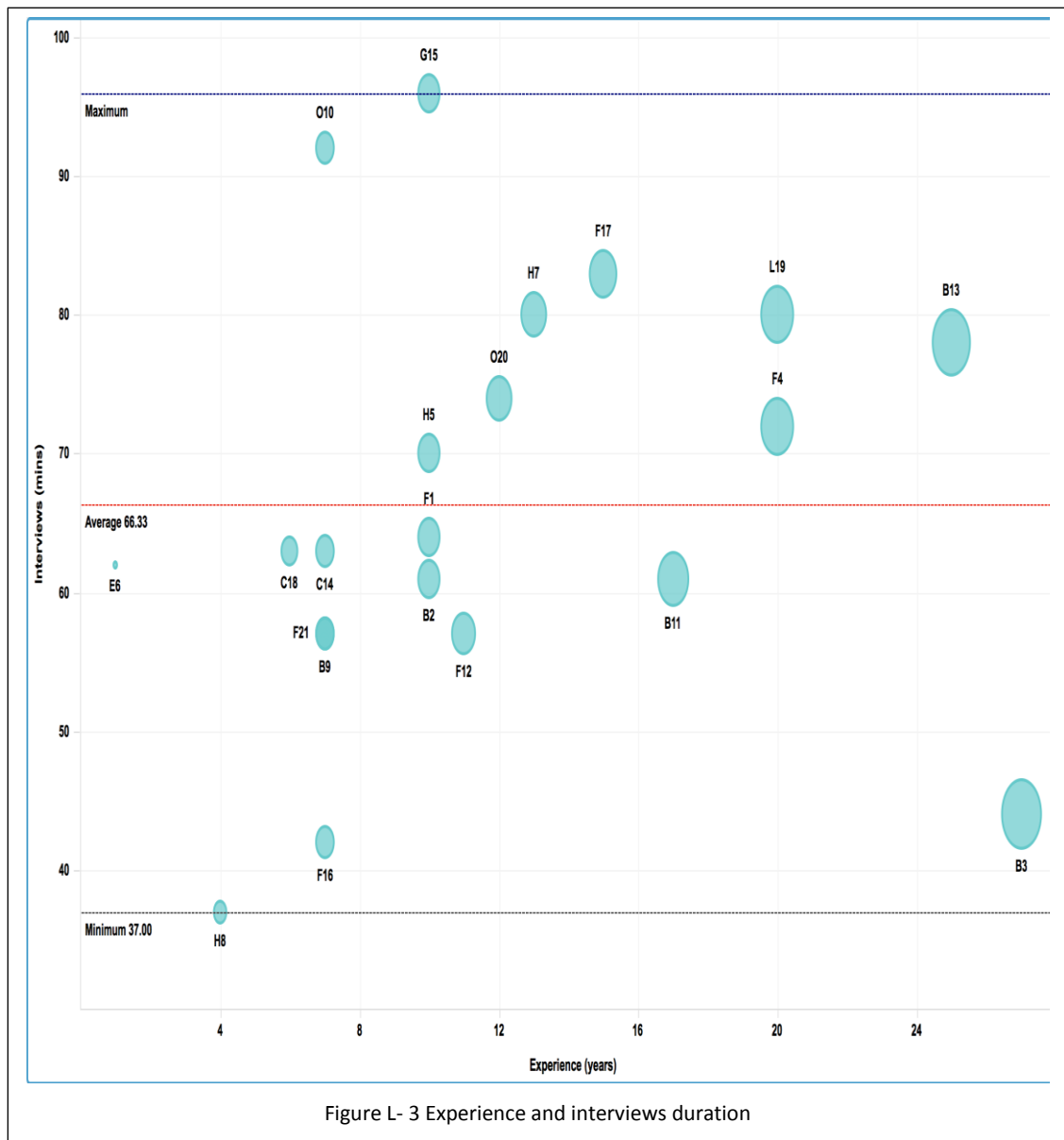
E. Your closing remarks about this interview

- 1) Is there anything else that you would like to add?
- 2) Can you please also suggest other people or organisations that you think should be consulted as part of this study? Can I mention your name?



Appendix L: Interviews maps and results





The interviewees were represented using the coded scheme (Section 4.4) and also described in Appendix H-5 p 219. Figure L- 1 p 226 shows the profile of the interviewees. Figure L- 3 p 227 shows the interviewee's years of experience in industry i.e. the bigger the ball the more experience, plotted against the length of the interview i.e. interview duration. Balls that overlapped i.e. have the same interview durations and year experience, shared the same balls. E.g. F21 and B9 shared same 7 years experience and 57 mins interview. As shown by the dotted red Average (66.33 mins) lines, most of the interviews took over 60 minutes. Also, most of the experienced interviewees took more than 60 minutes.

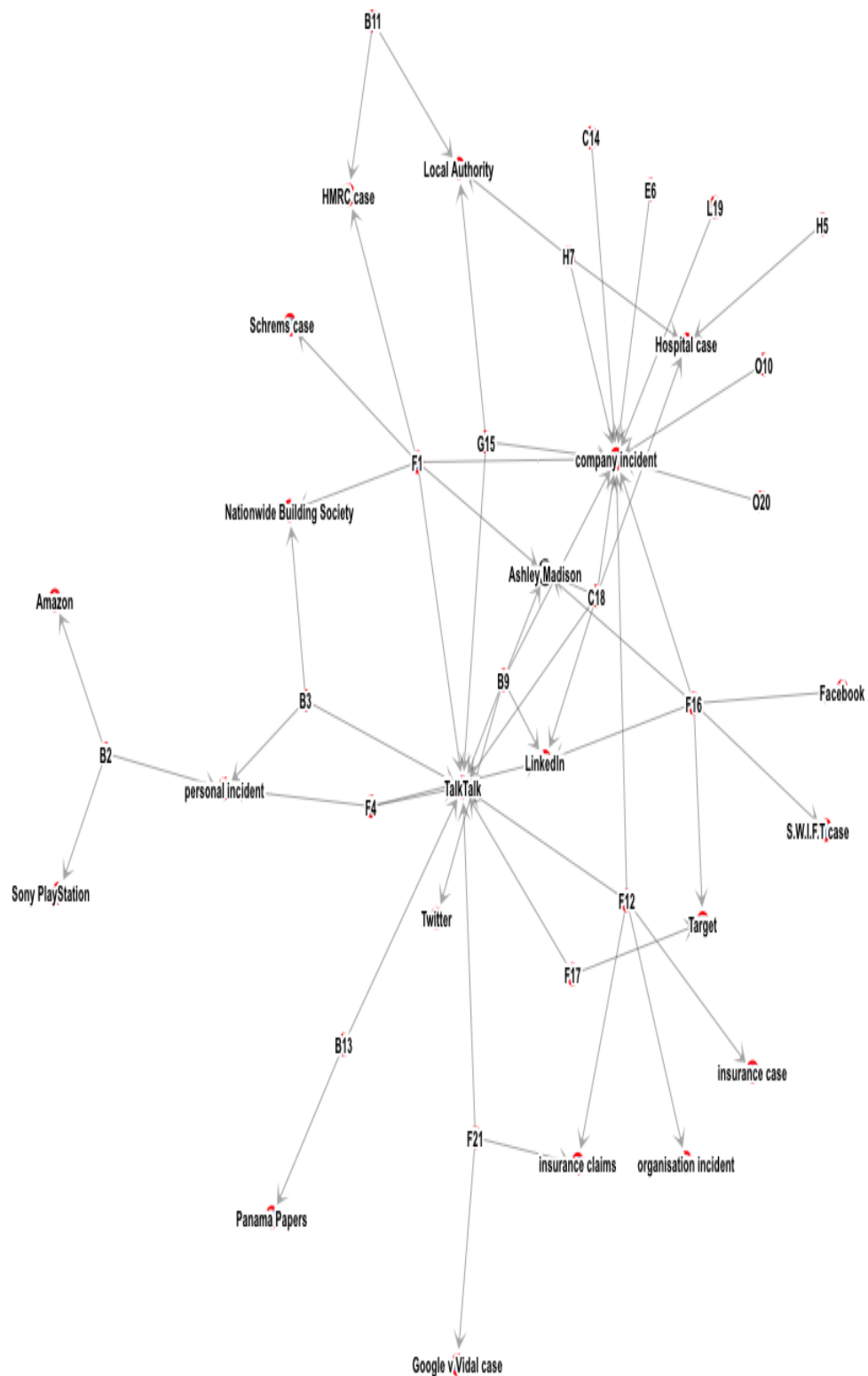
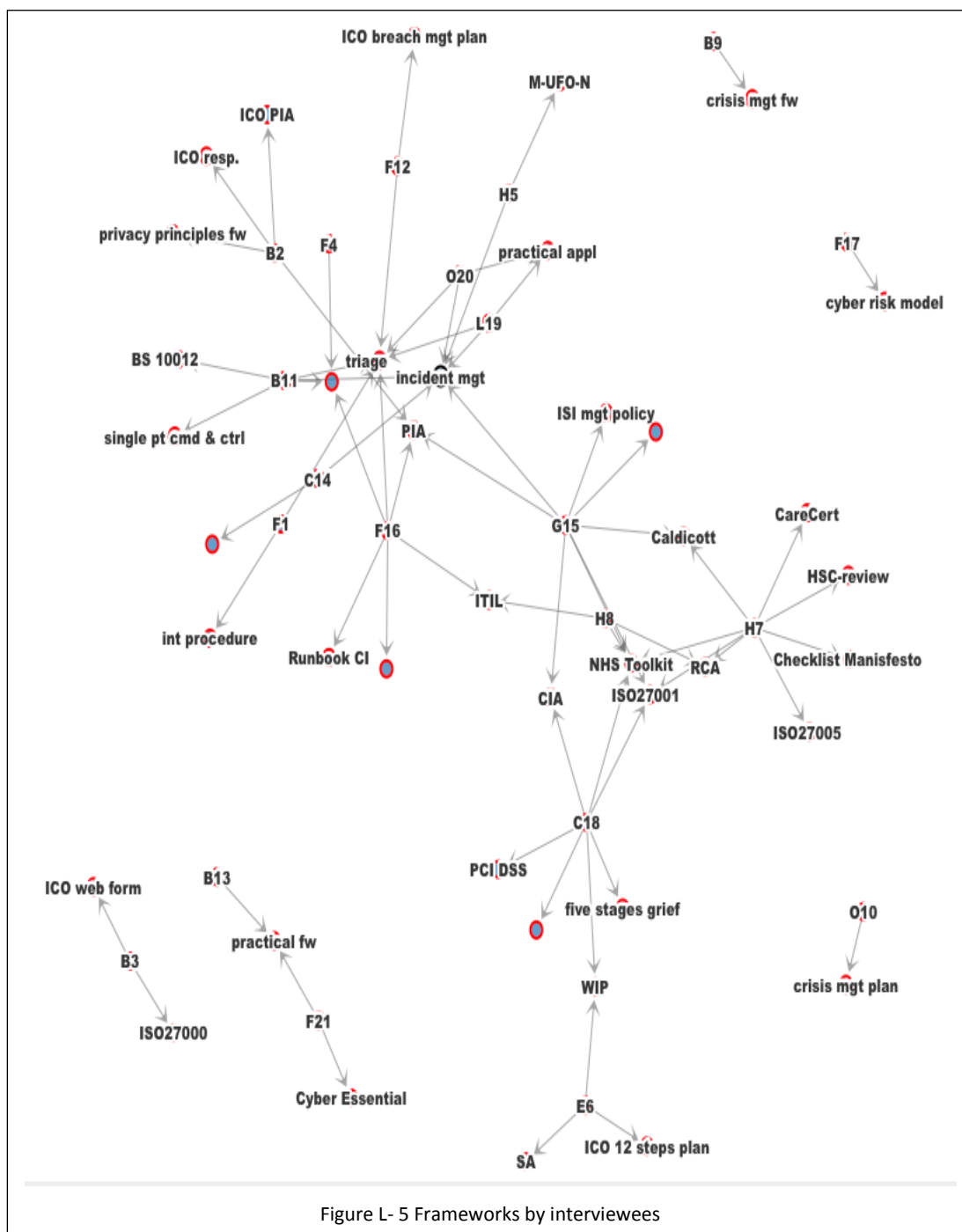


Figure L- 4 Incidents reported by interviewees



Appendix M: Dashboard requirements

Functional requirements

Functions/features	ReqID	Iteration #
Users provide the DBI scenarios (hypothetical/actual/future).	1.1	1
The dashboard will enable the user to save the DBI response sessions.	1.2	1
The dashboard will enable the incident scenario to be deleted.	1.3	1
The dashboard will enable the user to stop and restart at any point before the completion of the triage.	1.4	1
The dashboard will support user during the triage with relevant help messages.	1.5	2
The dashboard will provide an export of all the scenarios to a file.	1.6	1
The dashboard will enable the user to collect relevant breach data in a timely fashion using the sequence of steps - verify, assess and prioritise (VAP) .	1.7	1
The dashboard will assist in timely tracking of the gathering of information using 'call-do-response' checklists (checklist-questions).	1.8	1
The dashboard will provide checklist-questions on personal data and security measures (breach-checklists)	1.9	1
The dashboard will provide a range of answers for the breach checklists (checklist-answers).	2.0	1
The dashboard will enable the user to step through the breach-checklists .	2.1	1
The dashboard will support user during the VAP with relevant help messages for the breach-checklists .	2.2	2
The dashboard will perform a data privacy harm assessment (PHA) using a pre-set data harm matrix .	2.3	1
The dashboard will use the pre-set data-breach-security entities (data harm entities).	2.4	1
The dashboard will drive the PHA using the data harm entities for initial assessment of the data impact levels and impact levels on individuals.	2.5	1
The dashboard will display the alerts for the level of impact (high, medium, low) to individuals and provide the notification reasons (why?) as specified in the GDPR on breach notification.	2.6	1
The dashboard will provide alerts for the level of harm, impact of the harm so that appropriate breach notification can be prioritised.	2.7	1
The dashboard will display the triage duration (from when the incident is logged (started) until completion of the triage (i.e. to the final prioritisation screen)	2.8	1 & 2
The dashboard will keep track of the triage duration and show the triage clock whenever the user stops/exists at any point before completion of the triage.	2.9	1 & 2
The dashboard will display the countdown to 72 hours from when the incident was first made aware (72 hr notification alert).	3.0	1 & 2
The dashboard will keep track of the 72 hrs notification duration and show the notification alert clock whenever the user stops/exists at any point before completion of the triage.	3.1	1 & 2
The dashboard will use appropriate color schemes for alerting the level of impact: low- green; medium - yellow; high - red.	3.2	1
The dashboard will provide confidence level checklists on user's checklist-answers for: individuals suffered distress; personal data compromised; volume of data compromised; and personal data protected.	3.3	2
The dashboard will show all the confidence level checklists results.	3.4	2

Other Requirements

Help text
supporting help information
User details
user name and role
User Interface
The user interacts using a visual dashboard via a web browser.
The visual dashboard interface is clean, intuitive and easy to navigate.
The navigation are supported by appropriate use of visual clues, icons and color schemes.
Use triage color schemes for displaying the PHA risk levels and alerts
green - no harm; red - high harm; yellow - harm;
User event
user event logging/recording
logging the user events/activities from opening to closing an incident
user create/log incidents
user retrieval of active incidents
user amend active incidents
user amend incident indicators and alerts
user closing active incidents
Incident information
pre-set answers to checklist of questions
time to respond
pre-set response duration e.g. 72 hours from creation to closure
actual time to respond
incident timestamp
incident status (active, closed)
display time to respond
display actual time to respond
display of incident status
display of incident duration
alert amendment/changes timestamp
display incident and alerts using the triage color schemes
actionable information from the verify-assess-prioritise checklists
PHA information
entities and alerts
privacy harm matrix

Appendix N: Verify-Assess-Prioritise with Checklists

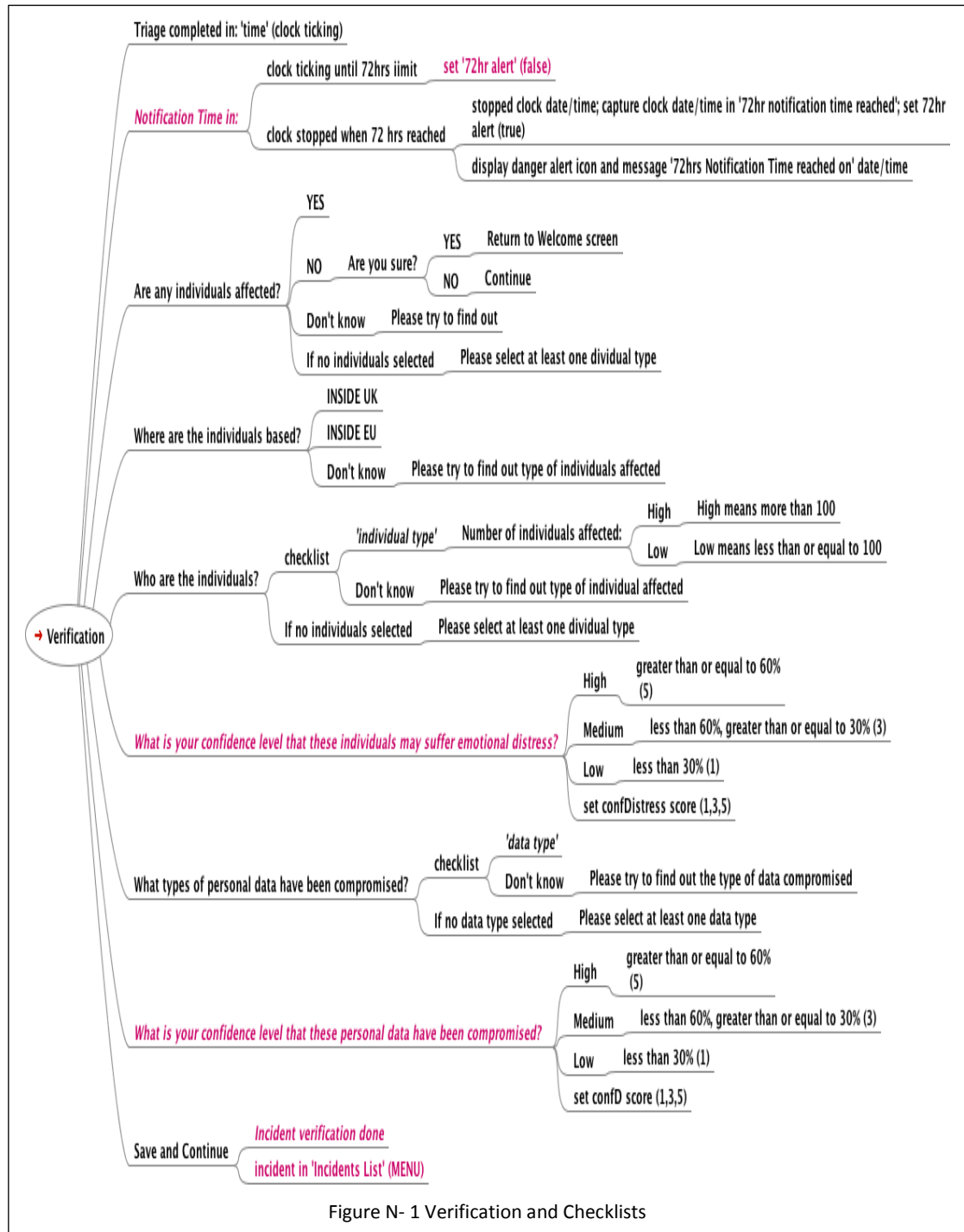


Figure N- 1 Verification and Checklists

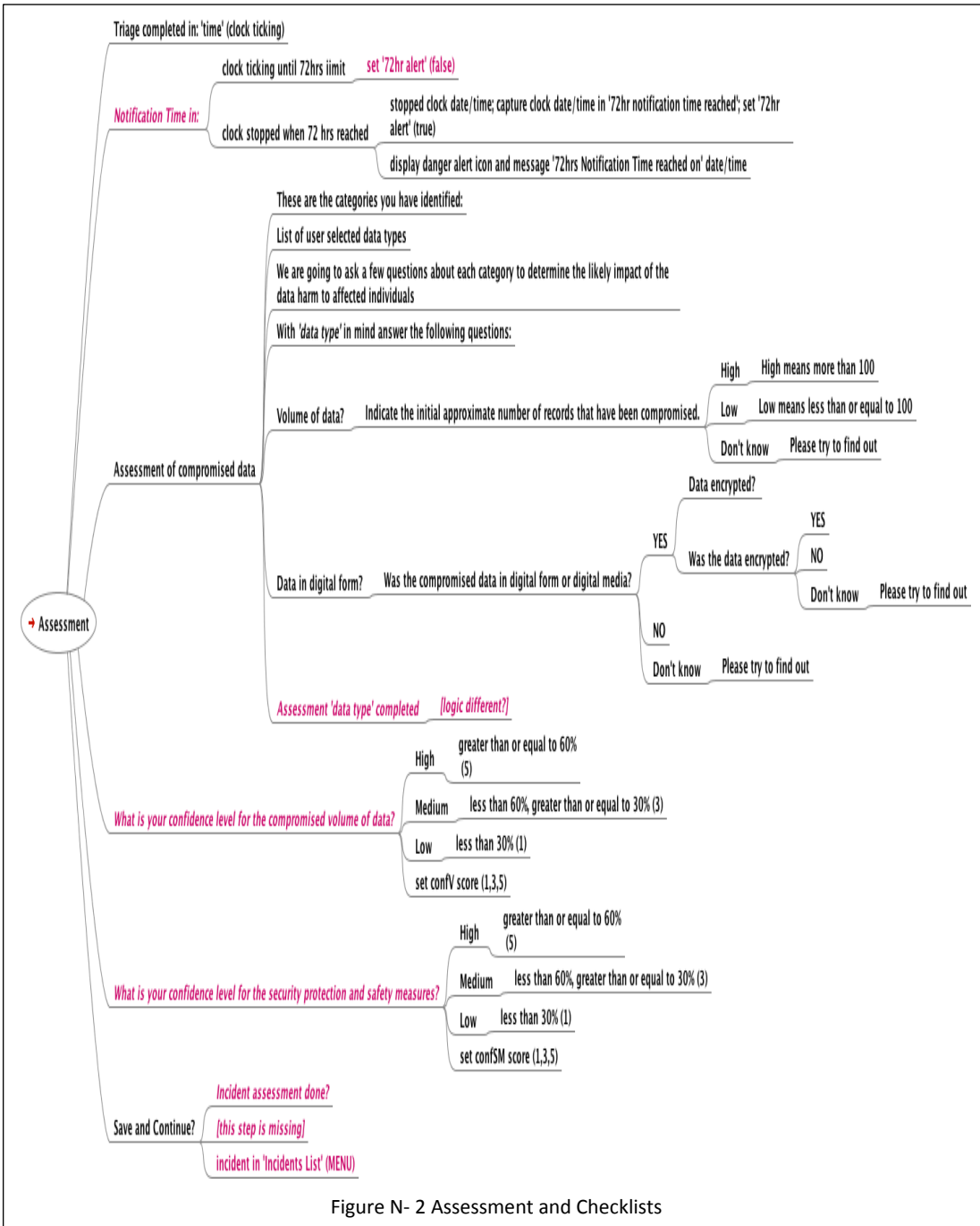


Figure N- 2 Assessment and Checklists

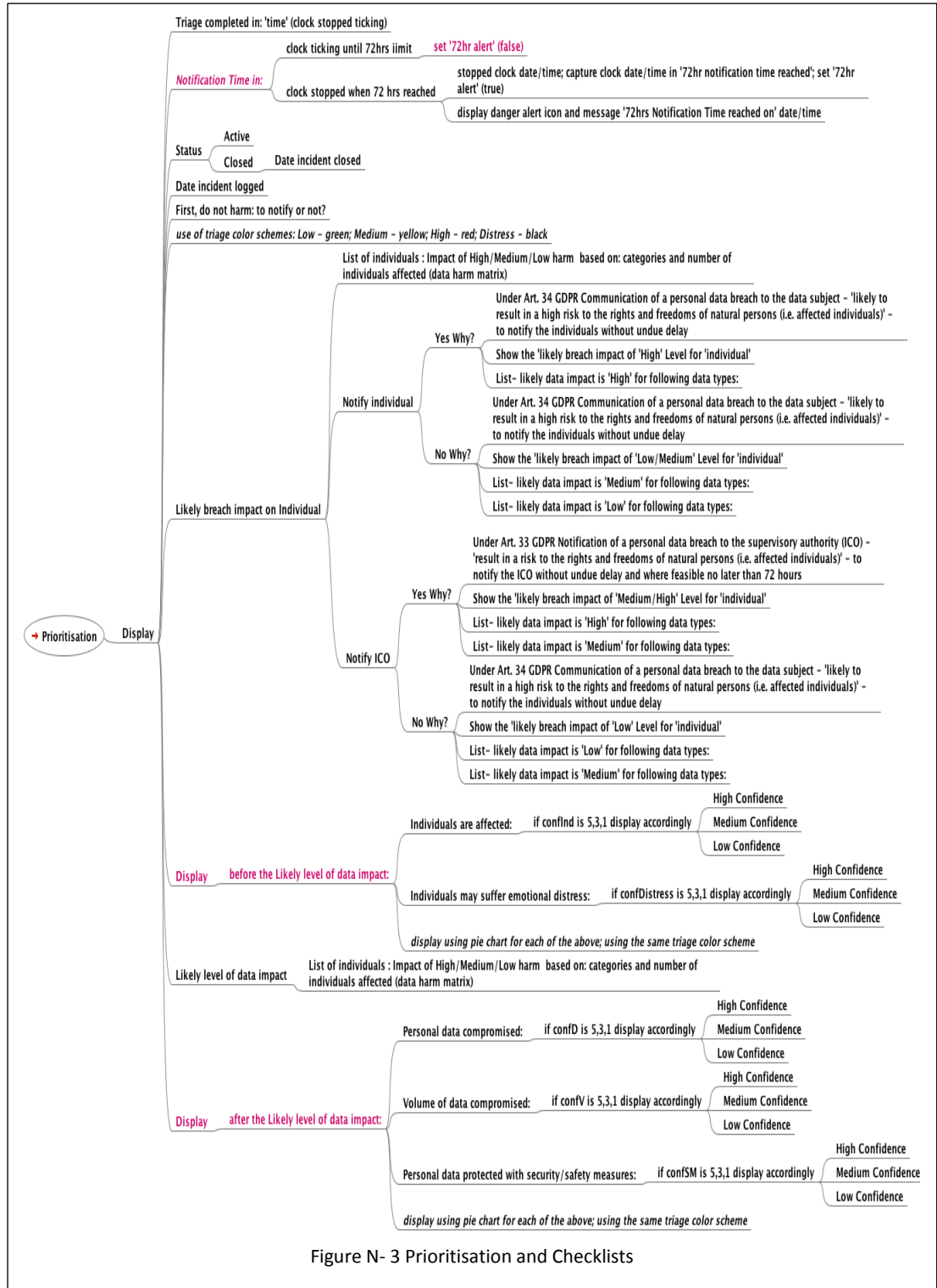


Figure N- 3 Prioritisation and Checklists

Appendix O: Data Matrix

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
personal data	sensitivity	security	score = sensitivity+security	data impact				notify					breach impact			individuals	breach
				low(1-2)	medium(3-6)	high (7-10)		individuals		ICO			low(1)	medium(3)	high (5)		
genetic	5	3,5	8,10						patient	Yes						patient	5
health	5	3,5	8,10						child	Yes						child	5
biometric	5	3,5	8,10						criminal/suspect	Yes						criminal/suspect*	5
sex life or sexual orientation	5	3,5	8,10					customer/client	customer/client	No	Yes					customer/client	1,3
political opinions	5	3,5	8,10					employee	employee	No	Yes					employee	1,3
racial or ethnic origin	5	3,5	8,10					subscriber/member	subscriber/member	No	Yes					subscriber/member	1,3
religious beliefs	5	3,5	8,10					student/researcher	student/researcher	No	Yes					student/researcher	1,3
trade union membership	5	3,5	8,10					donor	donor	No	Yes					donor	1,3
economic/financial	5	3,5	8,10														
social(metadata)	5	3,5	8,10														
name	1,3	1,3	2,4,6														
identification number (ID)	1,3	1,3	2,4,6														
online identifier	1,3	1,3	2,4,6														
location data	1,3	1,3	2,4,6														
picture/image/videos	1,3	1,3	2,4,6														
social(not-metadata)*	1,3	1,3	2,4,6														
cultural	1,3	1,3	2,4,6														

Figure O- 1 Data Matrix

The numerical values assigned to 'sensitivity' and 'security' (columns B and C) are to enable coding and logic of the scoring to be done.

The 'score=sensitivity+security' provided the numerical values for the labels i.e. 'low', 'medium' or 'high' as shown under the 'data impact' columns.

Similarly, on column R, 'breach' the numerical values are set to enable the scoring of the 'breach impact' as shown by the columns N, O and P.

The pre-set parameters i.e. as listed under 'personal data' and 'individuals' and the numerical values could be enhanced and tailored to meet organisational specific schemas.

Also, the 'notify' decision-making criteria can be refined to meet other notification rules and other stakeholders.

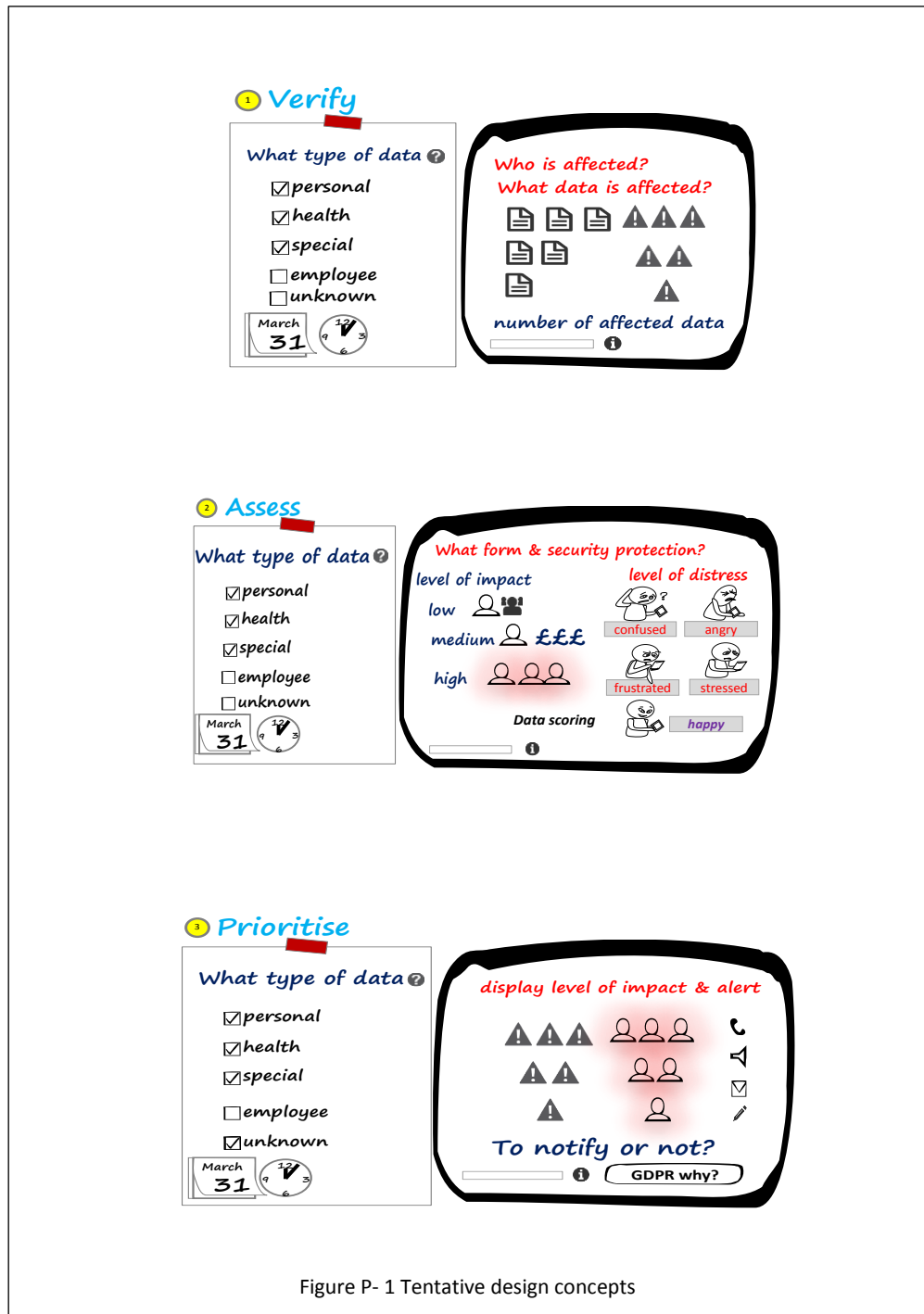
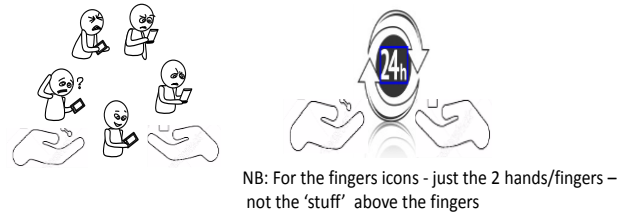


Figure P- 1 Tentative design concepts

These were shared with Dr Ludi Price.



These two icons were taken with permission from the DMA site (many thanks):
<http://www.dmcommission.com/the-dma-code/>



Simplify the icons

NB: Reliability without the expansion/zoom icon

Change TRUST to [Accountability]

See some samples for simple icons:

<https://depositphotos.com/133637200/stock-illustration-business-ethics-solid-icon-set.html>

<https://www.shutterstock.com/image-vector/business-ethics-solid-icon-set-isolated-532292002?src=ejB9JuKc49JwFIZlc849mA-1-10>

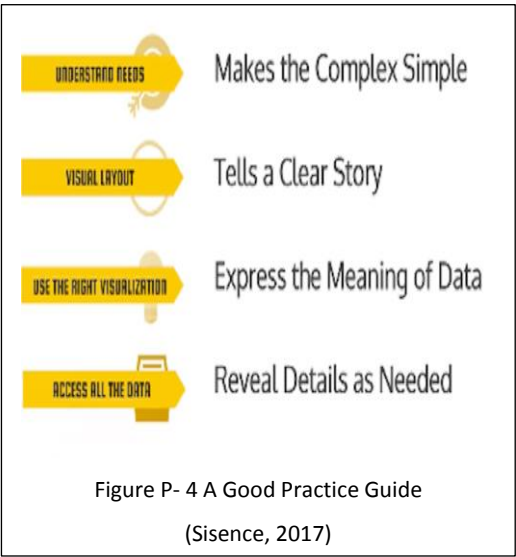
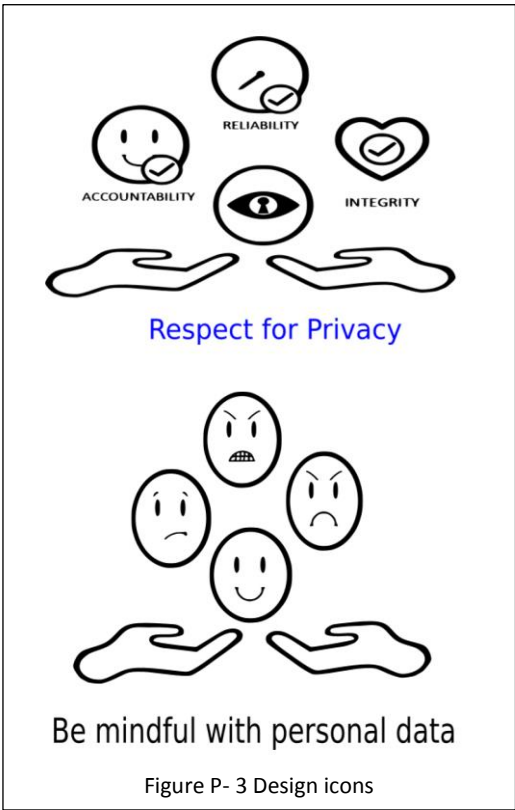
<https://www.shutterstock.com/image-vector/business-ethics-icon-set-social-responsibility-510864925?src=ejB9JuKc49JwFIZlc849mA-1-22>

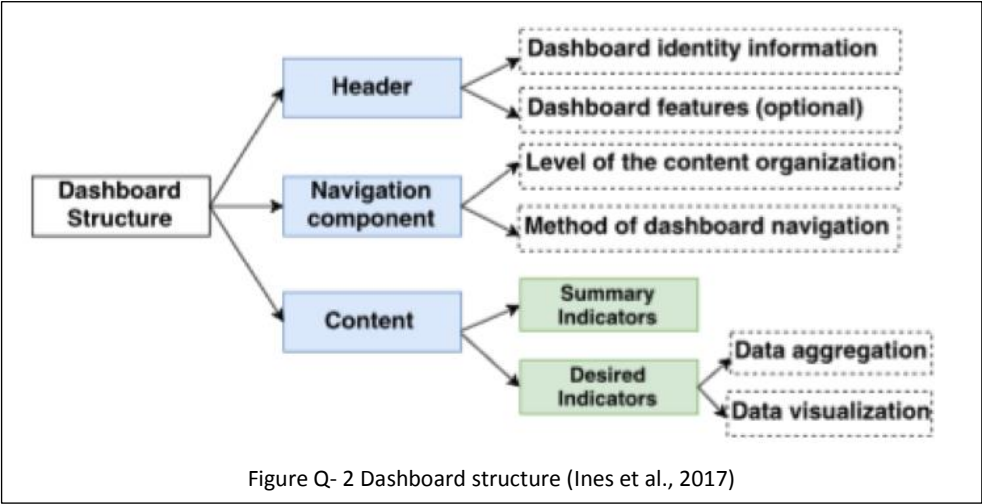
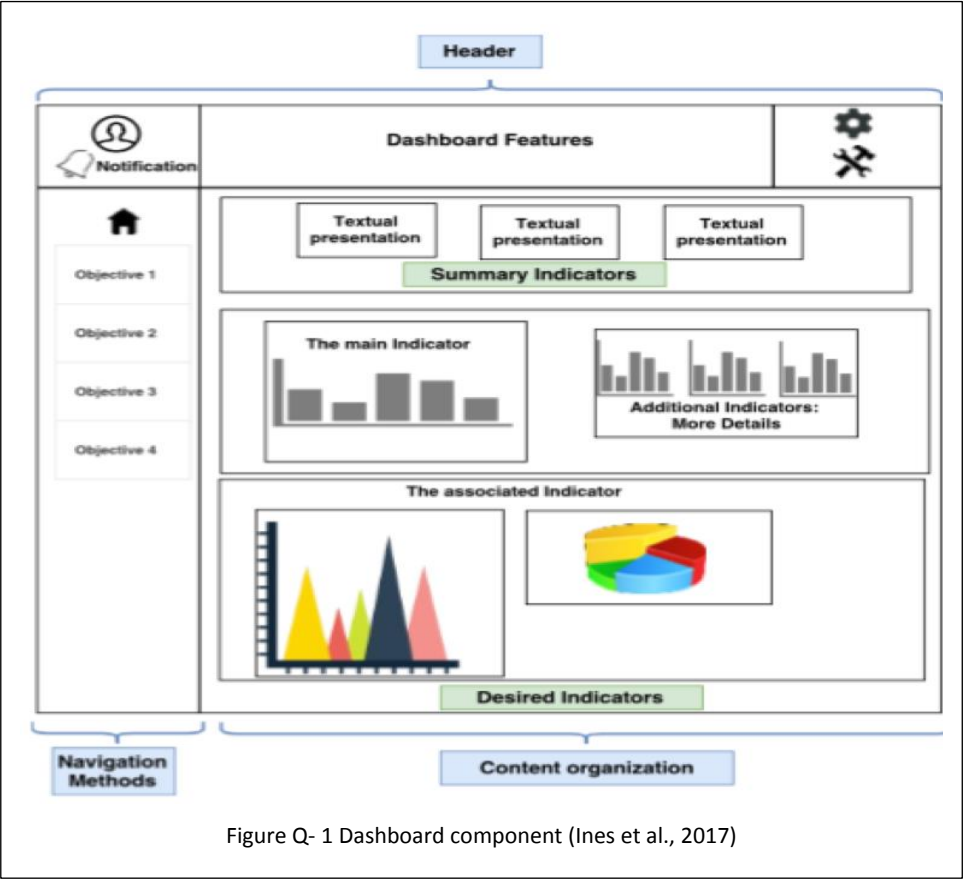
<https://www.bigstockphoto.com/search/ethics/>

<https://www.shutterstock.com/search/ethics>

Figure P- 2 Tentative design icons

The individual icons were produced by Dr Ludi Price and merged by this researcher to produce these two pictures for use by Developer2.





Appendix R: Samples of mockup screens



Appendix S: Notes and Job Post

18th August 2017 meeting with NT at E's Office, Newbury. Summary of the meeting by Cher D.

- I walkthrough my triage diagrams in my draft writeup on Triage for Privacy Harm Assessment (PHA);
- I mentioned the use of Peirce ternary for my triage - Verify, Assess & Prioritise;
- I showed and explained the checklists of questions for the PHA (mindmap diagrams); Described a bit about checklists;
- I highlighted the findings from my interview study;
- I explained the context and scope of my research and my research questions;
- NT shared his 'user-experienced' principles - learnability, usability, aesthetics & the question, is it useful? for dashboard design;
- NT described his approach starting with user stories and the need to ask the question 'who am I solving the problem for?';
- We discussed the various potential users or stakeholders (i.e. DPO, senior decision makers (C-Suite) and also by CISRTs of my triage playbook;
- We also discussed the prototyping steps as shown in a diagram in my draft writeup;
- NT reminded me that the prototype dashboard is for proof of concept of my research aims and my triage; Evaluation of the prototype dashboard will need to be conducted with users. The evaluation will be directed not on the visual design aspects of the prototype dashboard but on the appropriateness or applicability or usefulness (the utility) of the dashboard, namely answering my overall research aim and questions;
- I highlighted the benefits of having electronic checklists and how the triage can be used not only by privacy researchers & practitioners (for PHA) but also potentially for bridging the gaps between security (primarily focusing on Threat/Cyber Intelligence) and privacy. I mentioned the various information sharing initiatives and standards for Threat Intelligence and the concept of 'indicator of compromise';
- We discussed briefly my plan to submit my abstract for the Oasis-FIRST conference in December. Hopefully I can show work done on the dashboard and mention E's collaboration and contribution for the dashboard design and prototype.
- We closed the discussion meeting with next steps;

Next steps:

- NT to email me the signed NDA (by E's CEO) for me to sign;
- NT to provide his 'ToDo list';
- NT to provide his summary of our discussion - together with the scribbled discussion notes;
- For the fortnightly Friday meeting (starting from this Friday), we may use Skype. For doing mockups (using Balsamiq) and activities related to designing of the dashboard, we will aim for face-to-face meetings.

Overall, I find the meeting today productive and it was good that NT shared his views/experiences on dashboard design and reinforced what Steph W said during our meeting on 17th July at City namely, the need to clearly distinguish my PhD work (my triage playbook, and my conceptual model for the triage-PHA) from the prototype

Figure S- 1 First email with Developer1

<https://www.upwork.com/jobs/~019703291409e37712>



Closed - This post is no longer open to applicants.

[View proposals](#)

[Reuse posting](#)

[View hires](#)

iterative design & building a prototype (no back-ends) dashboard on desktop (Windows10)

Desktop Software Development

Posted 9 months ago

The project requires commitment for max 3 months and/or until completion of the project which is for a PhD software project.
Mock-ups already done using balsamiq with another developer.
A set of code and a 1st cut prototype dashboard has been delivered by the developer. Due to changes in circumstances, the developer is unable to commit to the tight schedule.
I now need someone dedicated and can work with me to finish the project. The prototype dashboard will be used for evaluation with users, and need to be 'professional' in design. Plan for 3 iterations (agile development) in total.

The code is based on Electron & React framework - using a boilerplate from github. I am happy to consider other tools/environments for the dashboard design & build as long as it achieved the desired outcomes.
Welcome further dialogue

\$500
Fixed-price

Intermediate level
I am looking for a mix of
experience and value

Project Type: One-time project

Skills and expertise

CSS Graphic Design HTML JavaScript Node.js React.js
Responsive Web Design User Experience Design Web Design Website Development
Wireframing

About the client

Payment method verified

☆☆☆☆ 0.00 of 0 reviews

United Kingdom
London 02:55 pm

1 job posted
100% hire rate, 1 open job

\$200 total spent
1 hire, 0 active

Member since Nov 28, 2017

Figure S- 2 Job details on upwork.com

Email dated 1st December 2017 to MS (Developer2)

Hi MS,

Thanks for the chat.

As discussed, please find attached an NDA for both of us to sign and a witness.

The NDA was done with the other developer at a company and it has been checked by my University. I've changed it to reflect your name in the NDA.

Once you have seen the code and run the EXE (for Windows) & my Excel sheet which has the logic for processing the answers to the questions, let's discuss further.

As discussed briefly, I am working on a very tight timescale and must finish the whole project by end February. The 1st cut of the prototype dashboard is done but now need further improvement. The current plan:

1) Sort out the typos for 'biometric' (not biometetric) and 'category' (not cateogry) (see the attached screenshots).

2) Design a 'nicer and better' User Interface for all the screens; use the concept of checklists and icons to show the items - I will provide examples of the icons.

3) Re-work the logic in the code to reflect what is in the Excel sheet (harmdistressdataV2.0.xlsx)- will need to walkthrough with you.

4) The final screen - prioritisation screen - needs a better display and more text - will provide the additional text for this screen.

5) Allow user to save and re-start (select their opened, active case) the incident case.

6) Allow a free text field in the final screen for user to add comment/description before they close the case.

7) Show the figures for the volume of record associated with High and Low i.e. High is >100; Low is <= 100).

8) Provide a better start screen - change current start screen - A triage playbook for privacy harm assessment: To Notify or Not?

9) Change 'Hello Electron React!' to 'Welcome to PrototypeDashboardV1.0'. (versioning for iteration)

10) As part of the project, code must be available and release to me.

11) Also to conduct walkthrough of the code and any instructions so that I can verify/validate the code and also do minor changes and rebuild.

12) No back-ends to database but all user inputs must be written to an Excel/csv file for further analysis.

13) Be able to do iterative design and implementation - see picture in slide 11 in Script.pdf - max. 3 major iterations. Script.pdf provides some information for my user evaluation with users. Planning to start this on 11th Dec but schedule has slipped.

14) Improve/enhance the logic in the Excel to include scoring for the indicators - the source of scoring in the ENISA paper.

15) Allow simple -user-friendly UI e.g. to move backward and change the results (before closure of the case) - for further discussion

16) Show the time indicator - start of the case to final closure. See attached pdf map of 'other requirements' - for further discussion (not all need to be implemented- nice to have stuff).

I need a working 1st prototype (not all the 'other requirements' implemented) ready by 14th Dec. If this can be delivered earlier - even better!

Attaching the 3 articles - the ENISA (office in Egypt!) paper, one on Checklist and the other on privacy harm- which I will be using for my research.

As mentioned I am using the concept of triage (as used in medical domain) and want to use the colors scheme: the triage color schemes - those used by medical people to color code the injured - will be used for the data privacy harm indicators in the dashboard:

green - no harm; red - high harm; yellow - harm; black - distress (bold/thick strokes of black).

Link to the code in Dropbox (*link unshared after project completion*):

<https://www.dropbox.com/sh/synri8y8jm8zmf1/AAAHgIBYsYbTluFY4G3ypISSa?dl=0>

Link to the EXE file (Windows)

<https://www.dropbox.com/s/wp47ufiyoeji8vh/dashboard-windows%2864bit%29.exe?dl=0>

I am free this evening after 9pm and also tomorrow anytime before 4pm. I am free all day on Sunday.

Figure S- 3 First email with Developer2

Appendix T: Iteration 1 DashboardV1 screenshots

Welcome screen and Dashboard Menu

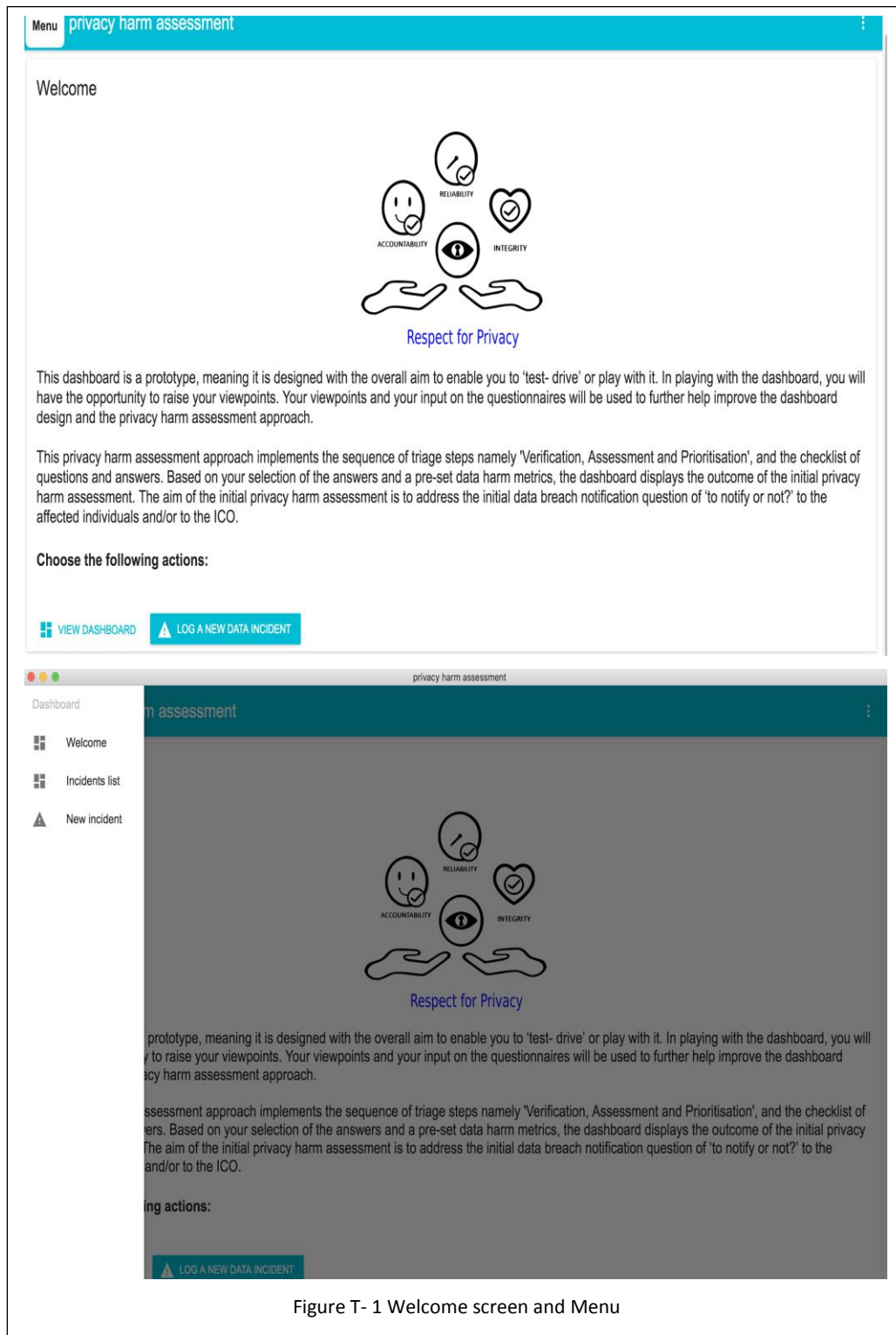


Figure T- 1 Welcome screen and Menu

Log a new incident or New Incident

privacy harm assessment

Initial triage of the data incident

Triage time
00:01:40

1 Verification

2 Assessment

3 Prioritisation

Reporter Name

Cher

Briefly describe the nature or type of the data incident

Test

Date incident logged (when organisation became aware)

Date

2018-09-11

Time

12 am

SAVE AND CONTINUE

Figure T- 2 Log a new incident

Calendar for selecting the date and time of the incident

privacy harm assessment

Initial triage of the data incident

Triage time
00:01:17

1 Verification

2 Assessment

3 Prioritisation

Reporter Name

Cher

Briefly describe the nature or type of the data incident

Test

Date incident logged (when organisation became aware)

Date

Time

SAVE AND CONTINUE

2018

Tue, Sep 11

<

September 2018

>

M	T	W	T	F	S	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

CLOSE

Figure T- 3 Calendar for selecting the date and time

Verify individuals are affected and where are they located

Location: Inside UK or Inside EU

privacy harm assessment

Menu

Initial triage of the data incident

Triage time 00:02:33

Notification due in 55:10:58

1 Verification 2 Assessment 3 Prioritisation

Status: Active

Verification of the nature of the data incident

To the best of your knowledge, when you first 'became aware' of the incident, start gathering information and determining with the following initial questions:

- 1 Are any individuals affected?
- 2 Where are the individuals based?
- 3 Who are the individuals?
- 4 What types of personal data have been compromised?

Figure T- 4 Verification of individuals

privacy harm assessment

Menu

Initial triage of the data incident

Triage time 00:03:55

Notification due in 55:09:35

1 Verification 2 Assessment 3 Prioritisation

Status: Active

Verification of the nature of the data incident

To the best of your knowledge, when you first 'became aware' of the incident, start gathering information and determining with the following initial questions:

- 1 ☒ Are any individuals affected?
- 2 Where are the individuals based?
- 3 Who are the individuals?
- 4 What types of personal data have been compromised?

Figure T- 5 Verification of individuals: location

Verify who are the individuals.

Status: Active

Verification of the nature of the data incident

To the best of your knowledge, when you first 'became aware' of the incident, start gathering information and determining with the following initial questions:

✓ Are any individuals affected?

✓ Where are the individuals based?

3 Who are the individuals?

☐ Employees

☐ Customer/Client

☐ Patient

☐ Child

☐ Criminal

☐ Subscriber/Member

☐ Student/Researcher

☐ Donor

☐ Don't Know

SAVE AND CONTINUE

Figure T- 6 Verification of individuals: types

Verify number of affected individuals

Verification of the nature of the data incident

To the best of your knowledge, when you first 'became aware' of the incident, start gathering information and determining with the following initial questions:

✓ Are any individuals affected?

✓ Where are the individuals based?

Number of individuals affected

Number of individuals affected ▾

High means greater than 100
Low means less than or equal to 100

CLOSE

☐ Subscriber/Member

☐ Student/Researcher

☐ Donor

☐ Don't Know

SAVE AND CONTINUE

Figure T- 7 Verification of individuals: number

Verify the types of data compromised

privacy harm assessment

4 What types of personal data have been compromised?

- ☐ Genetic
- ☐ Health
- ☐ Biometric
- ☐ Sex life or sexual orientation
- ☐ Political views
- ☐ Racial or ethnic origin
- ☐ Religious or philosophical beliefs
- ☐ Trade union membership
- ☐ Economic/Financial
- ☐ Name
- ☐ Identification number
- ☐ Online identifier
- ☐ Location Data
- ☐ Picture/Image/Video
- ☐ Social (Not metadata)
- ☐ Cultural
- ☐ Don't Know

SAVE AND CONTINUE

Figure T- 8 Verification of data: types

Assess the volume of the compromised data for each of the identified data

privacy harm assessment

Menu

Initial triage of the data incident

Triage time 00:09:07

Notification due in 55:04:24

1 Verification 2 Assessment 3 Prioritisation

Assessment of compromised data

These are the categories you have identified:

1 Economic/Financial 2 Name

We are going to ask a few questions about each category to determine the likely impact of data harm to affected individuals

With Economic/Financial data in mind answer the following questions:

1 Volume of data? 2 Data in digital form? 3 ???

Indicate the initial approximate number of records that have been compromised:

HIGH LOW DONT KNOW

High means more than 100

Figure T- 9 Assessment of data: volume

Assess the data form i.e. digital or non-digital for each of the identified data

Menu privacy harm assessment

Initial triage of the data incident

Triage time 00:10:24

Notification due in 55:03:07

1 Verification 2 Assessment 3 Prioritisation

Assessment of compromised data

These are the categories you have identified:

1 Economic/Financial 2 Name

We are going to ask a few questions about each category to determine the likely impact of data harm to affected individuals

With Economic/Financial data in mind answer the following questions:

1 Volume of data? 2 Data in digital form? 3 ???

Was the compromised data in digital form or digital media?

YES NO DONT KNOW

Figure T- 10 Assessment of data: form

Assess the data security protection for each of the identified data

If digital data, was it encrypted?

Menu privacy harm assessment

Initial triage of the data incident

Triage time 00:11:08

Notification due in 55:02:23

1 Verification 2 Assessment 3 Prioritisation

Assessment of compromised data

These are the categories you have identified:

1 Economic/Financial 2 Name

We are going to ask a few questions about each category to determine the likely impact of data harm to affected individuals

With Economic/Financial data in mind answer the following questions:

1 Volume of data? 2 Data in digital form? 3 Data encrypted?

Was the data encrypted?

YES NO DONT KNOW

Figure T- 11 Assessment of data: security

Assess the data security protection for each of the identified data

If non-digital data, where there any safety measures in place?

Menu privacy harm assessment

Initial triage of the data incident

Triage time 00:12:59

Notification due in 55:00:32

1 Verification 2 Assessment 3 Prioritisation

Assessment of compromised data

These are the categories you have identified:

1 Economic/Financial 2 Name

We are going to ask a few questions about each category to determine the likely impact of data harm to affected individuals

With Name data in mind answer the following questions:

1 Volume of data? 2 Data in digital form? 3 Non-digital data protected?

Were there safety measures in place for the non-digital data/media (e.g. paper or physical media)?

YES NO DON'T KNOW

Figure T- 12 Assessment of data: security measures (non-digital)

Final prioritisation screen: *Triage completed in* and *Notification due in*

Menu privacy harm assessment

Initial triage of the data incident

Triage completed in 00:13:50

Notification due in 54:58:31

1 Verification 2 Assessment 3 Prioritisation

Status: Active
Date incident logged: 11 September 2018 12:00 AM

First, do no harm : To notify or not?

Individual	Impact	Notify individual	Notify ICO
Employees	Medium	Yes why?	Yes why?

Do please notify the individuals as a matter of good business practice. Minimising distress to the affected individuals must be your first priority

Likely level of data impact

Type of data	Impact
Economic/Financial (digital)	High
Name (non-digital)	Low

Figure T- 13 Prioritisation screen: triage and notification results

Final prioritisation screen: The individuals impacted and the impact levels;
The types of data and impact levels

Verification Assessment Prioritisation

Status: Active
Date incident logged: 11 September 2018 12:00 AM

First, do no harm : To notify or not?

Individual	Impact	Notify individual	Notify ICO
Employees	Medium	Yes why?	Yes why?

Do please notify the individuals as a matter of good business practice. Minimising distress to the affected individuals must be your first priority

Likely level of data impact

Type of data	Impact
Economic/Financial (digital)	High
Name (non-digital)	Low

Be mindful with personal data

Figure T- 14 Prioritisation screen: impact levels

Why notify individuals?

Menu privacy harm assessment

Initial triage of the data incident Triage completed in 00:13:50 Notification due in 54:10:05

Verification Assessment Prioritisation

First, do no harm : To notify or not?

Individual

Employee

Do please notify the individuals as a matter of good business practice. Minimising distress to the affected individuals must be your first priority

Likely level of data impact

Type of data Impact

Economic/Financial (digital) High

Name (non-digital) Low

Under Art. 34 GDPR Communication of a personal data breach to the data subject - 'likely to result in a high risk to the rights and freedoms of natural persons (i.e. affected individuals)' - to notify the individuals without undue delay.

Likely data impact is High for following data types:
Economic/Financial: High

CLOSE

Figure T- 15 Prioritisation screen: why notify individuals?

Why notify the ICO?

Menu privacy harm assessment

Initial triage of the data incident Triage completed in 00:13:50 Notification due in 54:09:54

Verification Assessment Prioritisation

First, do no harm : To notify or not?

Individual

Employee

Do please notify the individuals as a matter of good business practice. Minimising distress to the affected individuals must be your first priority

Likely level of data impact

Type of data Impact

Economic/Financial (digital) High

Name (non-digital) Low

Under Art 33 GDPR Notification of a personal data breach to the supervisory authority (ICO) - 'result in a risk to the rights and freedoms of natural persons(i.e. affected individuals)' - to notify the ICO without undue delay and where feasible no later than 72 hours.

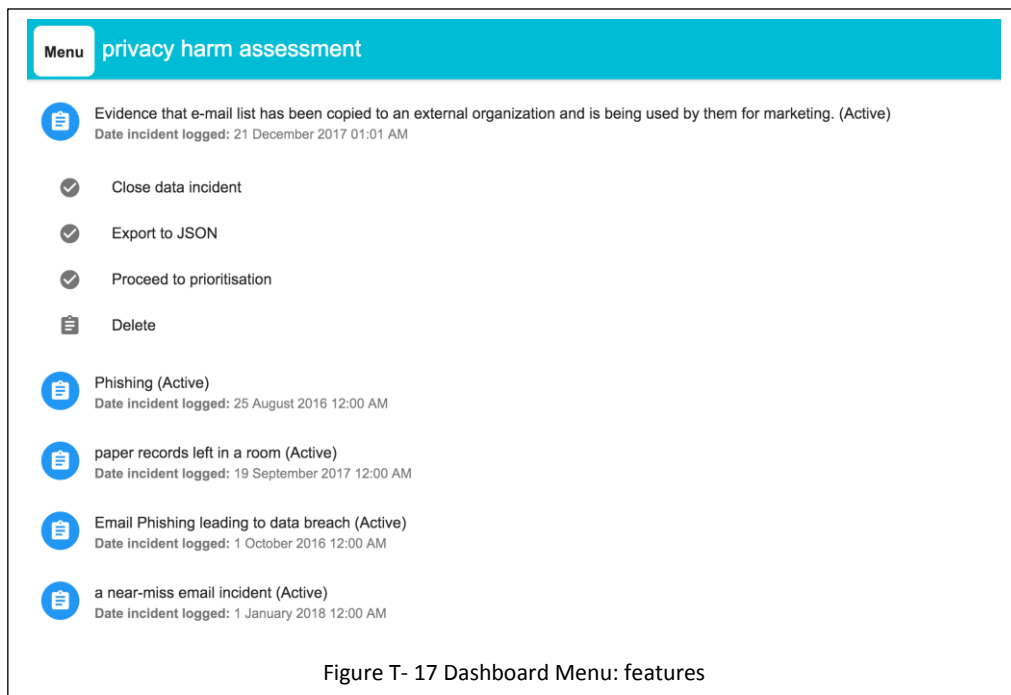
Likely breach impact of Medium Level for Employees

Likely data impact is High for following data types:
Economic/Financial: High

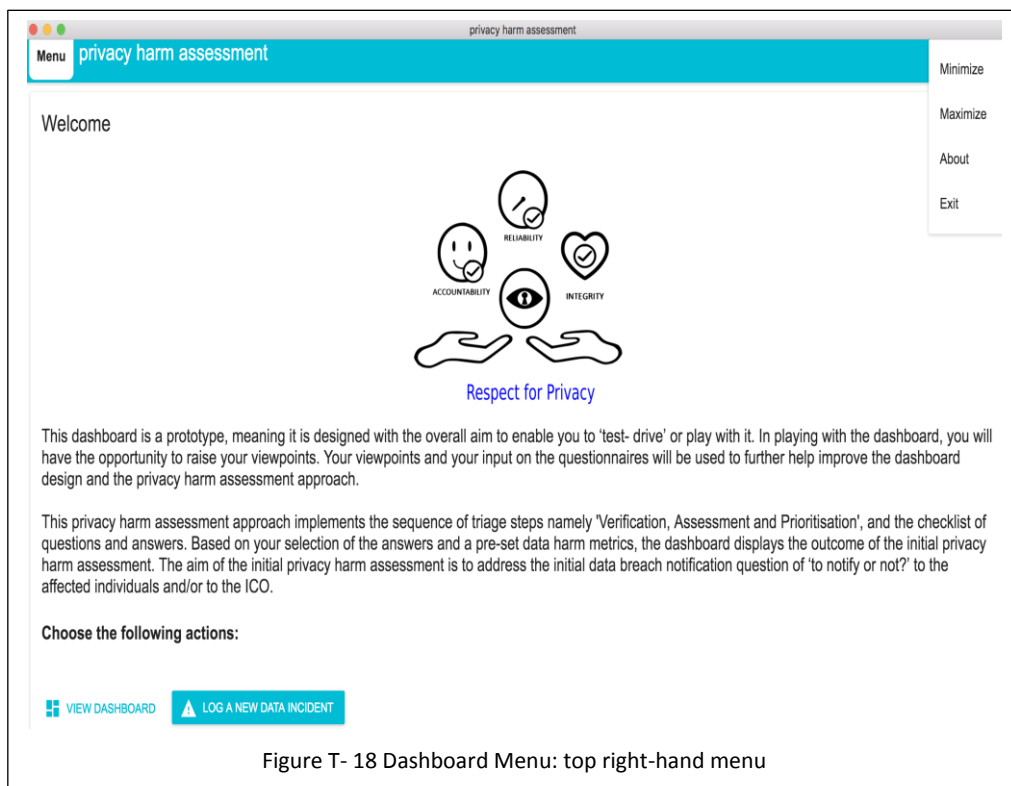
CLOSE

Figure T- 16 Prioritisation screen: why notify the ICO?

Dashboard Menu features



Dashboard screen menu (on the top-right hand side)



Appendix U: Iteration 2 DashboardV2 screenshots

Welcome screen, Dashboard Menu, Log a New Incident, Calendar selections are the same as in DashboardV1. Verify individuals affected, where are they located and number of individuals screens are the same as in DashboardV1. Changes in DashboardV2 are shown below:

Verify who are the individuals.

New *suspect* added to *criminal*

privacy harm assessment

✓ Are any individuals affected?

✓ Where are the individuals based?

3 Who are the individuals?

- ☐ Employees
- ☐ Customer/Client
- ☐ Patient
- ☐ Child
- ☐ Criminal/Suspect
- ☐ Subscriber/Member
- ☐ Student/Researcher
- ☐ Donor
- ☐ Don't Know

SAVE AND CONTINUE

You can stop and continue (via Menu)

Figure U- 1 Verification of individuals: new type

Confidence level: individuals suffer distress

Menu privacy harm assessment

Initial triage of the data incident

Triage time 00:05:00

Notification due in 53:41:23

1 Verification 2 Assessment 3 Prioritisation

Verification of the nature of the data incident

To the best of your knowledge, when you first 'became aware' of the incident, start gathering information and determining with the following initial questions:

✓ Are any individuals affected?

✓ Where are the individuals based?

✓ Who are the individuals?

4 What is your confidence level that these individuals may suffer emotional distress?

HIGH MEDIUM LOW

5 What types of personal data have been compromised?

6 What is your confidence level that these personal data have been compromised?

Figure U- 2 Confidence level: individuals suffer distress

Verify the types of data compromised

New 'social (sensitive)'

privacy harm assessment

5 What types of personal data have been compromised?

- ☐ Genetic
- ☐ Health
- ☐ Biometric
- ☐ Sex life or sexual orientation
- ☐ Political views
- ☐ Racial or ethnic origin
- ☐ Religious or philosophical beliefs
- ☐ Trade union membership
- ☐ Economic/Financial
- ☐ Name
- ☐ Identification number
- ☐ Online identifier
- ☐ Location Data
- ☐ Picture/Image/Video
- ☐ Social (Not metadata)
- ☒ Social (Sensitive)
- ☐ Cultural
- ☐ Don't Know

SAVE AND CONTINUE

Figure U- 3 Verification of data: new types

Confidence level: data compromised

Menu privacy harm assessment You can stop and continue (via Menu)

Initial triage of the data incident Triage time 00:07:00 Notification due in 53:39:22

1 Verification 2 Assessment 3 Prioritisation

Verification of the nature of the data incident

To the best of your knowledge, when you first 'became aware' of the incident, start gathering information and determining with the following initial questions:

- ✓ Are any individuals affected?
- ✓ Where are the individuals based?
- ✓ Who are the individuals?
- ✓ What is your confidence level that these individuals may suffer emotional distress?
- ✓ What types of personal data have been compromised?
- 1 What is your confidence level that these personal data have been compromised?

HIGH MEDIUM LOW

Figure U- 4 Confidence level: personal data compromised

Assess the volume of the compromised data for each of the identified data (same as in DashboardV1).

Confidence level: data volume compromised

The screenshot displays a web application titled "privacy harm assessment". At the top, there is a teal header bar with a "Menu" button on the left and a "You can stop and continue (via Menu)" button on the right. Below the header, a progress bar shows three steps: "1 Verification" (completed with a checkmark), "2 Assessment" (active with a blue circle), and "3 Prioritisation" (disabled with a grey circle). The main content area is titled "Assessment of compromised data". It states, "These are the categories you have identified:" followed by two items: "Health" and "Name", each with a blue checkmark icon. Below this, it says, "We are going to ask a few questions about each category to determine the likely impact of data harm to affected individuals". The next section asks, "What is your confidence level for the compromised volume of data?". At the bottom of this section are three buttons: "HIGH" (teal), "MEDIUM" (light blue), and "LOW" (light blue). The entire interface is enclosed in a thin black border.

Figure U- 5 Confidence level: compromised volume of data

Assess the data form i.e. digital or non-digital for each of the identified data (same as in DashboardV1).

Assess the data security protection for each of the identified data. If digital data, was it encrypted? (same as in DashboardV1).

Assess the data security protection for each of the identified data. If non-digital data, where there any safety measures in place? (same as in DashboardV1).

Confidence level: data protected

The screenshot displays a web application for 'privacy harm assessment'. At the top, a blue header bar contains a 'Menu' button, the title 'privacy harm assessment', and a link 'You can stop and continue (via Menu)'. Below the header, a status bar shows 'Initial triage of the data incident', 'Triage time 00:10:27', and 'Notification due in 53:35:55'. A progress bar indicates three steps: '1 Verification' (completed), '2 Assessment' (current), and '3 Prioritisation'. The main content area is titled 'Assessment of compromised data' and includes the text 'These are the categories you have identified:' followed by 'Health' and 'Name' (both with checkmarks). Below this, it states 'We are going to ask a few questions about each category to determine the likely impact of data harm to affected individuals'. A question 'What is your confidence level for the security protection and safety measures?' is followed by three buttons: 'HIGH', 'MEDIUM', and 'LOW'. The 'LOW' button is selected, and a tooltip 'Less than 30%' is visible. At the bottom, the caption 'Figure U- 6 Confidence level: security protection' is present.

Menu privacy harm assessment You can stop and continue (via Menu)

Initial triage of the data incident Triage time 00:10:27 Notification due in 53:35:55

1 Verification 2 Assessment 3 Prioritisation

Assessment of compromised data

These are the categories you have identified:

Health Name

We are going to ask a few questions about each category to determine the likely impact of data harm to affected individuals

What is your confidence level for the security protection and safety measures?

HIGH MEDIUM LOW

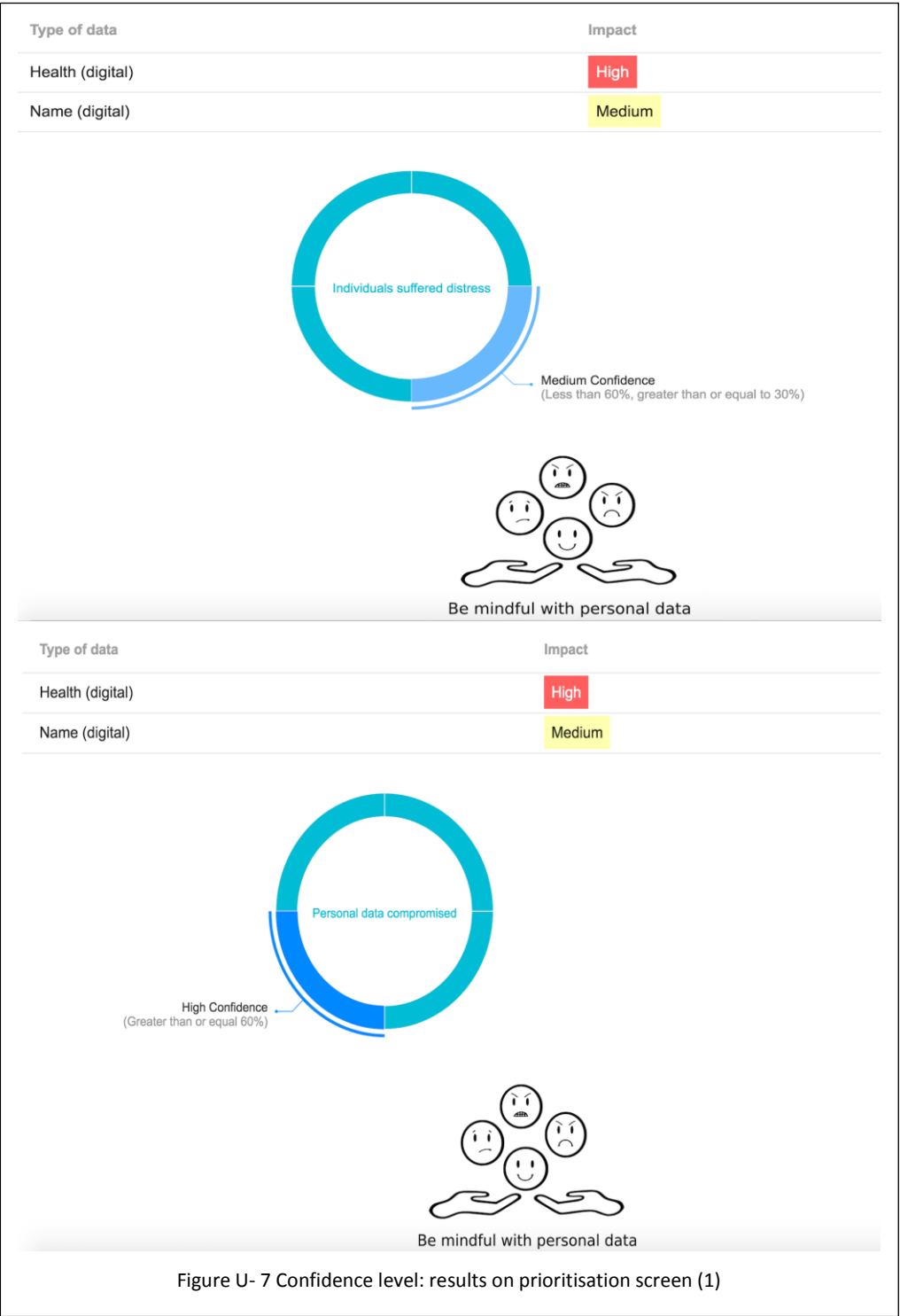
Less than 30%

Figure U- 6 Confidence level: security protection

Final prioritisation screen: 'Triage completed in' and 'Notification due in' (same as in DashboardV1).

Why notify individuals? and Why notify the ICO? screens are the same as in DashboardV1.

Confidence levels on prioritisation screen:



Type of data	Impact
Health (digital)	High
Name (digital)	Medium



Type of data	Impact
Health (digital)	High
Name (digital)	Medium



Appendix V: UES Questionnaire

	Question	Answer option/free form text field
Pre-dashboard		
Background	Q1 What is your role or title? Q2 How long have you been in this role or title? Q3 What are the responsibilities of your role or title?	
experience: PIA, PHA, & views on beach information, harm	Q4 Have you been involved with personal data breach (data breach) incident response?	☐ Yes, with previous organisations ☐ Yes, with current organisation ☐ No direct involvement but have responsibility for data breach notification to relevant data authority or law enforcement bodies ☐ No direct involvement but have responsibility for managing or responding to data breach incident ☐ Other. Please comment:
	A privacy impact assessment (PIA) is a systematic process for evaluating the potential effects on privacy of a project, initiative, or proposed system or scheme (Extracted from 'Should Privacy Impact Assessments Be Mandatory?' by Wright (2011)). Q5 Have you ever conducted privacy impact assessment?	☐ Yes ☐ No ☐ Other. Please comment:
	In this study, privacy harm assessment (PHA) addresses the impact of the data incident in terms of privacy harm on individuals whose data have been compromised by the data incident. An example of a privacy harm (harm) is the distress that an individual may suffer as a consequence of the personal data being compromised. Q6 Have you ever conducted privacy harm assessment during data incident response?	☐ Yes ☐ No ☐ Other. Please comment:
	Q7 During the initial stage namely before a thorough investigation (e.g. digital forensics) of data incident, there is minimal available breach information	☐ Strongly agree ☐ Somewhat agree ☐ Neither agree nor disagree ☐ Somewhat disagree ☐ Strongly disagree
	Q8 Data breaches increase a person's risk of identity theft or fraud and cause emotional distress as a result of that risk (Extracted from 'Risk and Anxiety: A Theory of Data Breach Harms' by Solove and Citron (2016)).	☐ Strongly agree ☐ Somewhat agree ☐ Neither agree nor disagree ☐ Somewhat disagree ☐ Strongly disagree
	Q9 To prevent notification fatigue to individuals, only in cases where a data breach is likely to adversely affect the privacy of the individual, for example in cases of identity theft or fraud, financial loss, physical harm, significant humiliation or damage to reputation, should the individual be notified (Extracted from 'Draft Report on the General Data Protection Regulation' by Albrecht 2012).	☐ Strongly agree ☐ Somewhat agree ☐ Neither agree nor disagree ☐ Somewhat disagree ☐ Strongly disagree

	Question	Answer option/free form text field
	Q10 A data breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage (Extracted from 'Guide to the General Data Protection Regulation (GDPR)' by ICO (ICO, 2018)).	☐ Strongly agree ☐ Somewhat agree ☐ Neither agree nor disagree ☐ Somewhat disagree ☐ Strongly disagree
Scenario selection	Q11 Please select a UK-based data incident scenario for the remaining questionnaires, and for the dashboard walkthrough	☐ To respond to a hypothetical data incident, or ☐ To respond to a data incident that you have had experience in, or ☐ To conduct a data incident response as part of a pre-incident response planning exercise (e.g. for a tabletop exercise).
	Q12 Please describe briefly the nature or type of your chosen data incident:	
views on harm and distress	Q13 Based on your chosen data incident, please indicate the overall level of the actual, likely or could have impact of the privacy harm (harm) to the individuals whose personal data have been or may have been compromised.	☐ Low level of impact ☐ Medium level of impact ☐ High level of impact ☐ Don't know
	Q14 Based on your chosen data incident, please indicate the overall actual, likely or could have level of distress (for example, anxiety) that the individuals have or may have suffered as a consequence of the data incident:	☐ Low level of distress ☐ Medium level of distress ☐ High level of distress ☐ Don't know
breach notification	Q15 Were the individuals whose personal data have been or may be compromised, initially notified of the data incident? If yes, please select 'Next' to continue. [Next to Q16] If no, please comment:	
	Q16 If the individuals were initially notified, how soon were they notified?	☐ As soon as possible, without undue delay (no thorough investigation) of being aware of the incident. ☐ Within 72 hours (no thorough investigation) of being aware of the incident ☐ After more thorough investigation, and within 72 hours of being aware of the incident ☐ After more thorough investigation, and outside 72 hours of being aware of the incident ☐ Other. Please comment:
	Q17 Was the Information Commissioner's Office (ICO) initially notified of the data incident? If yes, please select 'Next' to continue. [Next to Q18] If no, please comment:	

	Question	Answer option/free form text field
	Q18 If the ICO was initially notified, how soon was the ICO notified?	☐ As soon as possible, without undue delay (no thorough investigation) of being aware of the incident. ☐ Within 72 hours (no thorough investigation) of being aware of the incident ☐ After more thorough investigation, and within 72 hours of being aware of the incident ☐ After more thorough investigation, and outside 72 hours of being aware of the incident ☐ Other. Please comment:
Post-dashboard	Before continuing with the remaining questions, please walk through the dashboard. When the dashboard walkthrough is completed, select 'Next' to continue.	
Evaluate triage for initial data incident response	Q19 The verification, assessment and prioritisation steps are sufficient for conducting initial data incident response activities.	☐ Strongly agree ☐ Somewhat agree ☐ Neither agree nor disagree ☐ Somewhat disagree ☐ Strongly disagree
	Q20 The sequence of verification, assessment and prioritisation steps is appropriate during initial data incident response	☐ Strongly agree ☐ Somewhat agree ☐ Neither agree nor disagree ☐ Somewhat disagree ☐ Strongly disagree
	Q21 The sequence of verification, assessment and prioritisation steps provides a quick way to conduct privacy harm assessment.	☐ Strongly agree ☐ Somewhat agree ☐ Neither agree nor disagree ☐ Somewhat disagree ☐ Strongly disagree
Evaluate checklists	Q22 The questions and answers in the dashboard are simple to follow.	☐ Strongly agree ☐ Somewhat agree ☐ Neither agree nor disagree ☐ Somewhat disagree ☐ Strongly disagree
	Q23 The questions and answers in the dashboard are useful for quick checking of the necessary breach information.	☐ Strongly agree ☐ Somewhat agree ☐ Neither agree nor disagree ☐ Somewhat disagree ☐ Strongly disagree
	Q24 The questions and answers in the dashboard are useful for tracking of the gathered breach information.	☐ Strongly agree ☐ Somewhat agree ☐ Neither agree nor disagree ☐ Somewhat disagree ☐ Strongly disagree

	Question	Answer option/free form text field
	Q25 The questions and answers in the dashboard are appropriate for assessing privacy harm.	☐ Strongly agree ☐ Somewhat agree ☐ Neither agree nor disagree ☐ Somewhat disagree ☐ Strongly disagree
Evaluate the dashboard	Q26 The dashboard is appropriate for conducting quick privacy harm assessment during initial data incident response where minimal breach information is available.	☐ Strongly agree ☐ Somewhat agree ☐ Neither agree nor disagree ☐ Somewhat disagree ☐ Strongly disagree
	Q27 The dashboard allows breach notification actions to be prioritised in a short timeframe.	☐ Strongly agree ☐ Somewhat agree ☐ Neither agree nor disagree ☐ Somewhat disagree ☐ Strongly disagree
	Q28 The dashboard provides notification alerts which are useful for the prioritisation of breach notification.	☐ Strongly agree ☐ Somewhat agree ☐ Neither agree nor disagree ☐ Somewhat disagree ☐ Strongly disagree
	Q29 The dashboard provides a quick way to address the prioritisation question: 'whether to notify individuals or not?'	☐ Strongly agree ☐ Somewhat agree ☐ Neither agree nor disagree ☐ Somewhat disagree ☐ Strongly disagree
	Q30 What impact would the dashboard have on your initial data incident response?	
	Gathering of information	☐ Extremely ☐ Very effective ☐ Moderately effective ☐ Slightly effective ☐ Not effective at all
	Internal communication during the response	☐ Extremely ☐ Very effective ☐ Moderately effective ☐ Slightly effective ☐ Not effective at all
	Recording the incident response actions	☐ Extremely ☐ Very effective ☐ Moderately effective ☐ Slightly effective ☐ Not effective at all
	Q31 What improvements would you make to the dashboard?	
Closing remark	Q32 In closing this study, what else would you like to add?	

Appendix W: UES user note and consent form

Participant Note (content without the header and City, University of London's Logo)

Introduction

We would like to invite you to take part in a PhD research study (study). You can choose not to participate in part or all of this study, and that you can withdraw at any stage of this study without being penalized or disadvantaged in any way. Any data associated with you and/or your company will be removed from this study, and will not be used for this study if you withdraw at any stage of this study.

Ask us if there is anything that is not clear or if you would like more information. Thank you for your interest and help with this study.

The purpose of this PhD research study is to conduct user evaluation of a prototype version of a visual dashboard (dashboard). The overall aim of the dashboard is to enable organisations in the UK to conduct privacy harm assessment (PHA) for affected individuals during the initial response stage of personal data security incidents (data incidents). There is no doubt that data incidents have become a serious concern in almost every industry. PHA of the data incidents, focusing on the likely risks or high risks to affected individuals should enable organisations to prioritise prior to the actual breach notifications to individuals and also to the data authority.

Your participation in this user evaluation study will be valuable for our research, contributing to the development of a practical solution for privacy harm assessment during initial data incident breach response. This user evaluation study will consist of a facilitated walkthrough session of the dashboard and questionnaires for obtaining your views/comments.

During the facilitated session, you will be briefed on the session, the privacy harm assessment matrix (used in the dashboard), the dashboard and the use of the questions (questionnaire).

You will be briefed on the following available scenarios for using the dashboard:

- 1) To respond to a hypothetical data incident, or
- 2) To respond to a data incident that you have had experience in, or
- 3) To conduct a data incident response as part of a pre-incident response tabletop training exercises.

After the initial briefing, you will use your chosen scenario to answer the pre-dashboard questionnaire, use the dashboard and the final post-dashboard questionnaire and closing remarks. The researcher will walk through the dashboard with you using your chosen scenario.

The user evaluation session is expected to last one hour. The whole session will be recorded (audio recording). The recording is done to enable your responses to be accurately transcribed and analysed. All data input or collected or captured by the dashboard will also be screen recorded/captured. The dashboard will be provided on a laptop. The dashboard is a standalone desktop system. The questionnaire will be conducted using offline survey applications provided by Qualtrics.com (software licensed to City, University of London).

We will make sure that personal identifiable individual information and individual company information will be treated as confidential and not disclosed in the evaluation report or any reports without your written permission.

The identifiable data will not be shared with any other organisation. Only research supervisors and examiners for this study will have access to all data. All personal and commercial sensitive data will be removed and masked by using non-identifying combination of alphabetic and numeric characters. The data will be used only for purposes associated with this study. The data will also be stored and removed securely using the appropriate data management and retention policies set and used by the City, University of London (City). In City, data is retained for ten years.

We will be happy to email you a copy of the summary of the findings of this study.

This study has been approved by the City, University of London, Department of Computer Science Research Ethics Committee (CSREC171129CD). However, if you have any problems, concerns or questions about this study, you should ask to speak to a member of the research team. The research team details:

Cher Devey

M: 07770 953001

E: cher.devey.1@city.ac.uk

Stephanie Wilson

T: 0207 040 8152

E: s.m.wilson@city.ac.uk

Ilir Gashi

T: 0207 040 0273

E: Ilir.gashi.1@city.ac.uk

If you remain unhappy and wish to complain formally, you can do this through City's complaints procedure. To complain about the study, you need to phone 020 7040 3040. You can then ask to speak to the Secretary to Senate Research Ethics Committee and inform them that the name of the project is: User evaluation on privacy harm assessment using questionnaires and a prototype dashboard.

You could also write to the Secretary at:

Anna Ramberg

Research Governance & Integrity Manager

Research & Enterprise
City, University of London
Northampton Square
London
EC1V 0HB

City holds insurance policies which apply to this study. If you feel you have been harmed or injured by taking part in this study you may be eligible to claim compensation. This does not affect your legal rights to seek compensation. If you are harmed due to someone's negligence, then you may have grounds for legal action.

Thank you for taking the time to read this information sheet.

Cher Devey
PhD Research Student
Department of Computer Science
School of Mathematics, Computer Science & Engineering
City, University of London, Northampton Square, London, EC1V 0HB, UK.

Consent Form (content without the header and City, University of London's Logo)

Title of this study: User evaluation of privacy harm assessment using questionnaires and a prototype dashboard.

Please initial box

1.	I agree to take part in the above City University London research project. I have had the project explained to me, and I have read the participant information sheet, which I may keep for my records. I understand this will involve: • a facilitated walkthrough questionnaire session by the researcher; • using a hypothetical data incident or a data incident based on my experience or a pre-incident response for tabletop training exercises; • responding to the pre-dashboard questionnaire; • walking through the dashboard; • responding to the post-dashboard questionnaire; • allowing the whole session to be audiotaped; • allowing the walkthrough of the dashboard to be screen recorded/captured; • making myself available for a further interview should that be required.	
2.	This information will be held and processed for the following purpose(s): Purpose: The purpose of this study is to test the prototype dashboard as part of a PhD study. I understand that any information I provide is confidential, and that no information that could lead to the identification of any individual and/or company will be disclosed in any reports for this study. The identifiable data will not be shared with any other organisation. Only research supervisors and examiners for this study will have access to the identifiable data. All personal and commercial sensitive data will be removed and masked by using non-identifying combination of alphabetic and numeric characters. I consent to the use of the anonymised transcribed audio text files in publications.	
3.	I understand that my participation is voluntary, that I can choose not to participate in part or all of this study, and that I can withdraw at any stage of this study without being penalized or disadvantaged in any way. Any data associated with me and/or my company will be removed from this study, and will not be used for this study if I withdraw at any stage of this study.	
4.	I agree to City, University of London recording and processing this information about me. I understand that this information will be used only for the purpose(s) set out in this statement and my consent is conditional on the University complying with its duties and obligations under the Data Protection Act 1998.	
5.	I agree to take part in the above study.	

When completed, 1 copy for participant; 1 copy for researcher file.

Name of Participant Signature Date

Name of Researcher Signature Date

Appendix X: UES user selection criteria and sample invitation email

Participant Selection Criteria

Candidates with the following criteria were invited to participate:

- Have exposure to or experience in data incident response or;
- Have experience or responsibility for data incident response management or pre-response planning.

Specifically, the following key people/roles were targeted:

- Senior Managers responsible for Data Incident Response Management or Planning;
- Data Protection Officers;
- Data Compliance Officers;
- Data Security Incident Responders;
- Data Governance Managers;
- Cybersecurity Incident Responders;
- or in any roles or responsibilities for managing or planning their organisation's personal data breach or information security or cybersecurity incidents.

Participants who took part in the research study in 2016 and have indicated or expressed willingness to be interviewed were also invited to participate. Other potential candidates were recruited via network of industry professionals at events/seminars/conferences or through introduction by professional colleagues.

Sample Invitation Email

cher devey <cher.devey.1@city.ac.uk> 6 December 2017 at 17:15

To: Kim [REDACTED], Ian. [REDACTED]

Dear Kim and Ian,

I hope both of you are well.

We have exchanged emails last year regarding my research interviews where Ian participated and provided valuable contributions. I am inviting Ian back to contribute to my final PhD study involving a questionnaire and a prototype dashboard.

The purpose of the study is to gather practitioners' viewpoints on privacy harm assessment and the dashboard which implemented the privacy harm assessment approach.

If Ian is willing to participate, could you please let me know which dates on 15th to 26th January 2018 are likely to be convenient. I can also make other dates beyond the 26th January 2018.

I would need no more than an hour of Ian's time. If it is convenient I will come to your offices to conduct the user evaluation study. The study will be audio-recorded.

Attached a participant note. There is also a consent form which I will bring along two copies to be signed before the interview commences. Attached a copy. Please note that I'm emailing these files and the invitation out while waiting for my Ethics approval, which should be completed by early January 2018.

Meanwhile, if you need further information please let me know.

I look forward to hearing from you.

Many thanks,
Cher Devey

On 25 May 2016 at 10:54, cher devey <cher.devey.1@city.ac.uk> wrote:
[Quoted text hidden]
[Quoted text hidden]

2 attachments

Appendix Y: UES Walkthrough briefing snapshots

Group1 - user f8

1Feb2018

Cher (C) : OK, Hi, good afternoon, today is the 1st of Feb 2018, I believe you're Ms SM (S).

S: correct in all those things you stated (laughter – because we have met before in the interview study).C I believe you're also an independent consultant

C: great.

C: Thank you for signing the consent form and for agreeing to participate in my PhD user evaluation. Just want to reassure you we're recording the conversation and the screen. Everything we say here is treated as private and confidential and anything you don't feel comfortable I am happy not to press you on. I am trying to keep it very informal. The drill today is basically, I am here to answer your questions and to guide you to walk through the questionnaire

S: Ok

C:...and the prototype dashboard which we will walk through in a minute.

S: yes

C: Just a brief description of the dashboard, Basically the aim ...I call it a prototype privacy harm assessment dashboard. It's a prototype because it's an initial attempt to gather practitioners' view points on privacy harm assessment during the initial phase of responding to a personal data incident.

S: yes

C: I think I showed you a diagram (incident response) last time. It's looking at response and notification. The idea is to capture your viewpoints on the privacy harm assessment driven by a pre-set data harm matrix, built into dashboard. Preset because fixed at the moment. The idea is to allow me to get your viewpoints with the view to enhance and improve later on. So that is one of the aim. The main question which I am trying to address in the privacy harm assessment dashboard, is to help organisations in the UK, so context is UK driven. In terms of the legal framework, I get that you've heard of GDPR, right?

S: yes, occasionally, like 10 times a day (laughter).

C: so I am touching on specifically breach notification. So you know, there is an incident and the organisation need to respond.

S: yeah

C: So that where I'm coming in. The question is because of part of GDPR, organisation needs to do some sort of initial assessment whether to notify or not to individuals that are affected & also to the ICO. So, this dashboard is to address that initial question whether to notify or not?. So when we walk through that maybe it will become clearer. Right, does that make sense?

S: yes that all makes sense. Thank you very much.

C: you know, like I said I am here to answer any questions because it is a complicated area, I find it complicated. So, the first step is we will do some questionnaire and half way through we will pause.

S: yes

C:...and I will explain how the dashboard is going to be used. Hopefully it won't take more than an hour. Is that OK with you?

S: that's fine.

Group2 - user c10

12Feb2018

C: hi, good afternoon

R: good afternoon

C: today is 12 February 2018. And I believe I am talking to Mr RE (R) chief information security officer with the SC (organisation).

R: yep

C: thank you again for signing the consent form, and for taking time out to do this study,

R: my pleasure

C: quick briefing, the purpose of this study is to gather your view points using a questionnaire and a prototype dashboard. The prototype dashboard implements a sequence of triage steps which you will see in a minute. The overall aim is to help organisations to address the initial breach notification question whether to notify individual or not and to the ICO.

R: ok

C: my role is primarily to guide you through the questionnaire and to answer any questions you have. It shouldn't take more than an hour. Is that ok with you?

R: fine, that's good.

C: thank you, so let's start, ok? The first part will do the questionnaire. Just some background question, you need to do a little bit of typing, if you don't mind?

R: sure

C: because you are with SC, is it alright if I classify you as under charity?

R: yes

C: ok, thank you

R: (mumbling in the background) I can't type

C: don't worry

Appendix Z: UES Group1: a User Walkthrough screenshots

Group1 User (g7)

Qualtrics S: x Questionnaire | Pre and Post x
ps://cityunilondon.eu.qualtrics.com/jfe/form/SV_eEvsq7XX9dXqZvL
Data Chain cPanel Login data research2017 stuff incident ethics crypto privacy Basic Pro

User evaluation of a prototype dashboard for privacy harm assessment during initial personal data incident response - to notify or not?

Q1. What is your role or title?

Compliance and Information Governance Manager

Q2. How long have you been in this role or title?

18 years in local government, 20 months in higher education

Q3. What are the responsibilities of your role or title?

Previously I have been nominated data protection officer at 3 local authorities. I have led on Freedom of Information, Records Management, Data Quality and Information Security Policy. Currently I lead for the College on writing the infr

Figure Z- 1 Pre-Dashboard: Background Q1-3

Qualtrics S: x Questionnaire | Pre and Post x
//cityunilondon.eu.qualtrics.com/jfe/form/SV_eEvsq7XX9dXqZvL
Data Chain cPanel Login data research2017 stuff incident ethics crypto privacy Basic Project v

Q6. In this study, privacy harm assessment (PHA) addresses the impact of the data incident in terms of privacy harm on individuals whose data have been compromised by the data incident. An example of a privacy harm (harm) is the distress that an individual may suffer as a consequence of the personal data being compromised.

Have you ever conducted privacy harm assessment during data incident response?

☐ Yes.

☐ No.

☒ Other. Please comment:

Evaluate impact of loss on data subjects as part of incident management

Q7. During the initial stage namely before a thorough investigation (e.g. digital forensics) of data incident, there is minimal available breach information.

☐ Strongly agree

☐ Somewhat agree

☐ Neither agree nor disagree

Figure Z- 2 Pre-Dashboard: Views on PHA Q6

Initial personal data incident response - to notify or not?

Scenario selection. In this study, the General Data Protection Regulation (GDPR) - effective 25th May 2018 - forms the legal landscape for determining personal data breaches and personal data breach notification requirements in the UK.

Q11.
Please select a UK-based data incident scenario for the remaining questionnaires, and for the dashboard walkthrough.

- ☐ To respond to a hypothetical data incident, or
- ☒ To respond to a data incident that you have had experience in, or
- ☐ To conduct a data incident response as part of a pre-incident response planning exercise (e.g. for a tabletop exercise).

Q12.
Please describe briefly the nature or type of your chosen data incident:

Figure Z- 3 Pre-Dashboard: Scenario selection Q11

Initial personal data incident response - to notify or not?

Q13.
Based on your chosen data incident, please indicate the overall level of the *actual, likely or could have* impact of the privacy harm (harm) to the individuals whose personal data have been or may have been compromised.

- ☐ Low level of impact
- ☐ Medium level of impact
- ☒ High level of impact
- ☐ Don't know

Q14.
Based on your chosen data incident, please indicate the overall *actual, likely or could have* level of distress (for example, anxiety) that the individuals have or may have suffered as a consequence of the data incident:

- ☐ Low level of distress
- ☐ Medium level of distress
- ☐ High level of distress
- ☐ Don't know

Figure Z- 4 Pre-Dashboard: Scenario description Q12

Qualtrics | Questionnaire | Pre and Post

cityunilondon.eu.qualtrics.com/jfe/form/SV_eEvsq7XX9dXqZvL

ata Chain cPanel Login data research2017 stuff incident ethics crypto privacy Basic Project

CITY
UNIVERSITY OF LONDON
EST 1894

User evaluation of a prototype dashboard for privacy harm assessment during initial personal data incident response - to notify or not?

Q15.
Were the individuals whose personal data have been or may be compromised, initially notified of the data incident?
If yes, please select 'Next' to continue.

☒ If no, please comment:
No - concern over potential impact regarding prosecution

Back Next

Figure Z- 5 Pre-Dashboard: Breach notification Q15

Qualtrics | Questionnaire | Pre and Post

cityunilondon.eu.qualtrics.com/jfe/form/SV_eEvsq7XX9dXqZvL

Data Chain cPanel Login data research2017 stuff incident ethics crypto privacy Basic Project

CITY
UNIVERSITY OF LONDON
EST 1894

User evaluation of a prototype dashboard for privacy harm assessment during initial personal data incident response - to notify or not?

Q18. If the ICO was initially notified, how soon was the ICO notified?

☒ As soon as possible, without undue delay (no thorough investigation) of being aware of the incident.

☐ Within 72 hours (no thorough investigation) of being aware of the incident.

☐ After more thorough investigation, and within 72 hours of being aware of the incident.

☐ After more thorough investigation, and outside 72 hours of being aware of the incident.

☐ Other. Please comment:

Back Next

Figure Z- 6 Pre-dashboard: Breach Notification Q18

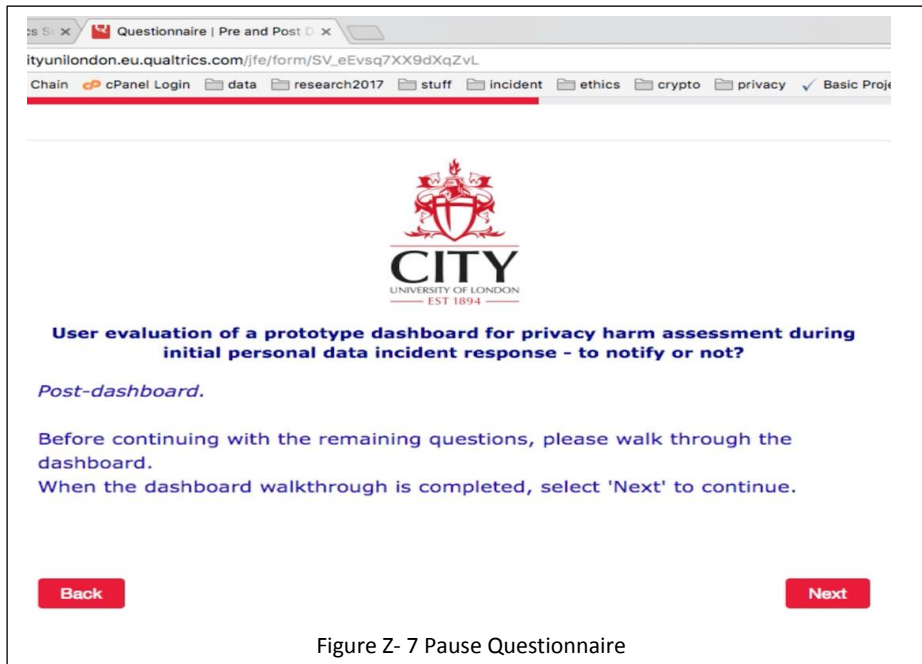


Figure Z- 7 Pause Questionnaire

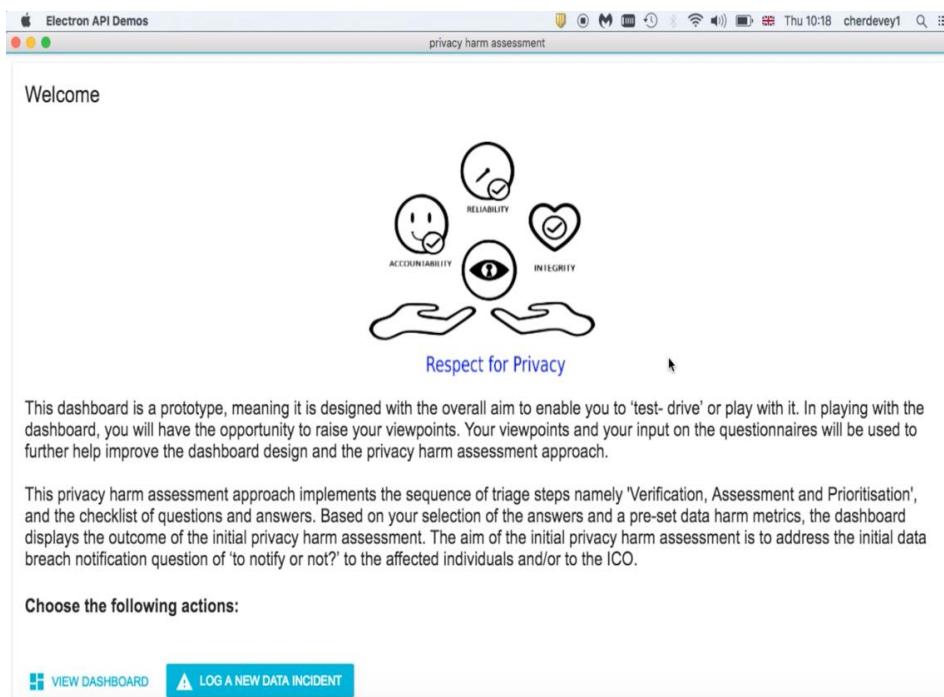


Figure Z- 8 Dashboard: Welcome Screen

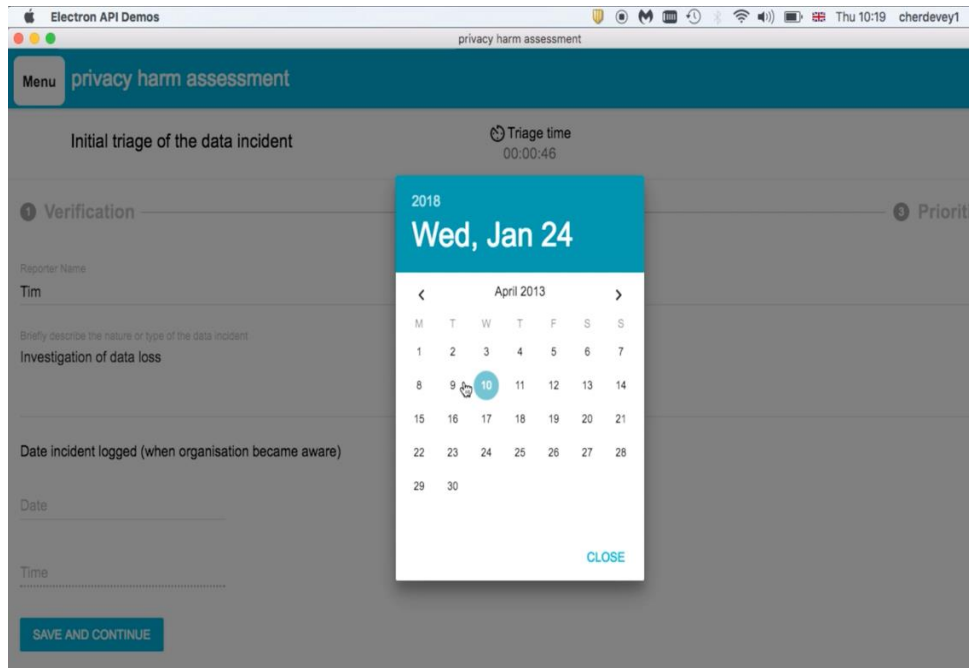


Figure Z- 9 Dashboard: Select date incident logged

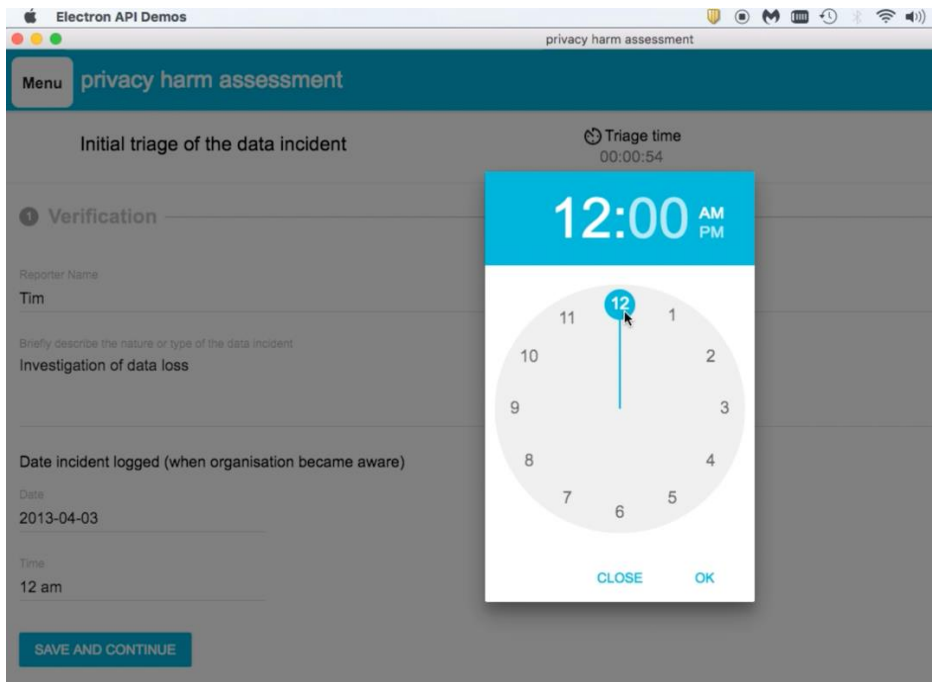


Figure Z- 10 Dashboard: Select time incident logged

privacy harm assessment

start gathering information and determining what the following initial questions:

✓ Are any individuals affected?

✓ Where are the individuals based?

3 Who are the individuals?

☐ Employees

☒ Customer/Client

☐ Patient

☐ Child

☐ Criminal

☐ Subscriber/Member

☐ Student/Researcher

☐ Donor

☐ Don't Know

SAVE AND CONTINUE

4 What types of personal data have been compromised?

Figure Z- 11 Dashboard: Verification Checklists Individuals

4 What types of personal data have been compromised?

☐ Genetic

☐ Health

☐ Biometric

☐ Sex life or sexual orientation

☐ Political views

☒ Racial or ethnic origin

☒ Religious or philosophical beliefs

☐ Trade union membership

☒ Economic/Financial

☒ Name

☒ Identification number

☐ Online identifier

☒ Location Data

☐ Picture/Image/Video

☐ Social (Not metadata)

☐ Cultural

Figure Z- 12 Dashboard: Verification Checklists Data

Initial triage of the data incident
Triage time
00:05:31
Notification due reached on
6 April 2013 10:00 AM

1 Verification
2 Assessment
3 Prioritisation

Assessment of compromised data

These are the categories you have identified:

1 Economic/Financial - 2 Identification number - 3 Name - 4 Location Data - 5 Racial or ethnic origin - 6 Religious or philosophical

We are going to ask a few questions about each category to determine the likely impact of data harm to affected individuals

With **Economic/Financial** data in mind answer the following questions:

1 Volume of data? 2 Data in digital form? 3 ???

Indicate the initial approximate number of records that have been compromised:

HIGH LOW DONT KNOW

Low means less than or equal to 100

Figure Z- 13 Dashboard: assessment data volume

Initial triage of the data incident
Triage time
00:05:51
Notification due reached on
6 April 2013 10:00 AM

1 Verification
2 Assessment
3 Prioritisation

Assessment of compromised data

These are the categories you have identified:

1 Economic/Financial - 2 Identification number - 3 Name - 4 Location Data - 5 Racial or ethnic origin - 6 Religious or philosophical

We are going to ask a few questions about each category to determine the likely impact of data harm to affected individuals

With **Economic/Financial** data in mind answer the following questions:

1 Volume of data? 2 Data in digital form? 3 ???

Was the compromised data in digital form or digital media?

YES NO DONT KNOW

Figure Z- 14 Dashboard: assessment data form

privacy harm assessment

Initial triage of the data incident

Triage completed in 00:06:47

Notification due reached on 6 April 2013 10:00 AM

Verification Assessment **Prioritisation**

Status: Active
Date incident logged: 3 April 2013 10:00 AM

First, do no harm : To notify or not?

Individual	Impact	Notify individual	Notify ICO
Customer/Client	Low	Yes why?	Yes why?

Do please notify the individuals as a matter of good business practice. Minimising distress to the affected individuals must be your first priority

Likely level of data impact

Type of data	Impact
Economic/Financial (non-digital)	High
Identification number (non-digital)	Medium
Name (non-digital)	Medium

Figure Z- 15 Dashboard: Prioritisation screen

privacy harm assessment

Initial triage of the data incident

Triage completed in 00:06:47

Notification due reached on 6 April 2013 10:00 AM

Verification Assessment **Prioritisation**

Status: Active
Date incident logged: 3 April 2013 10:00 AM

First, do no harm : To notify or not?

Individual	Impact	Notify individual	Notify ICO
Customer/Client	Low	Yes why?	Yes why?

Do please notify the individuals as a matter of good business practice. Minimising distress to the affected individuals must be your first priority

Likely level of data impact

Type of data	Impact
Economic/Financial (non-digital)	High
Identification number (non-digital)	Medium
Name (non-digital)	Medium

Under Art. 34 GDPR Communication of a personal data breach to the data subject - 'likely to result in a high risk to the rights and freedoms of natural persons (i.e. affected individuals)' - to notify the individuals without undue delay.

Likely data impact is High for following data types:
Economic/Financial: High
Racial or ethnic origin: High
Religious or philosophical beliefs: High

[CLOSE](#)

Figure Z- 16 Dashboard: Why notify the individuals?

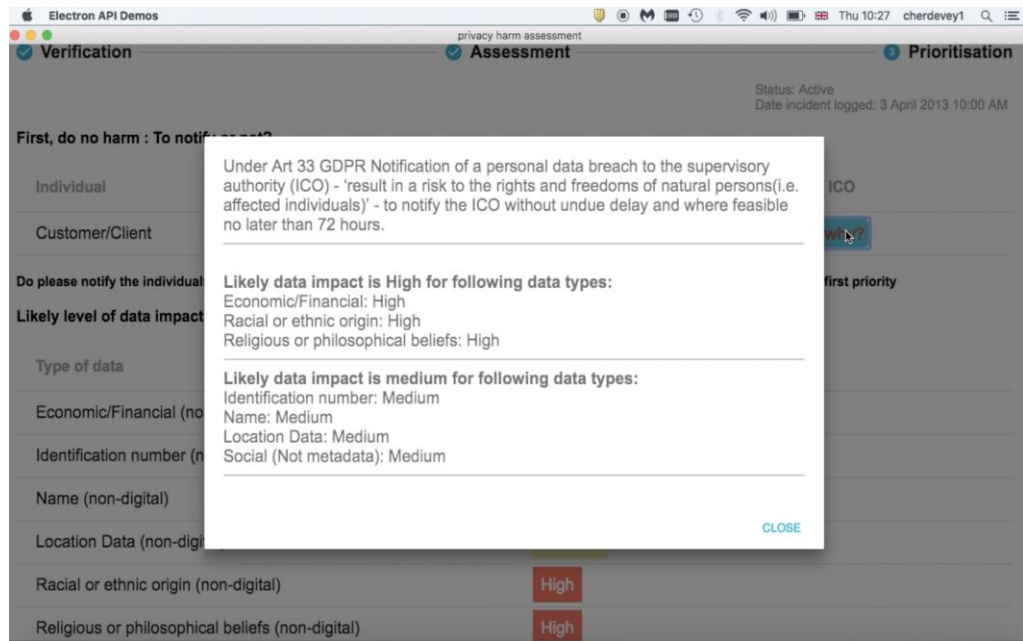


Figure Z- 17 Dashboard: Why notify the ICO?

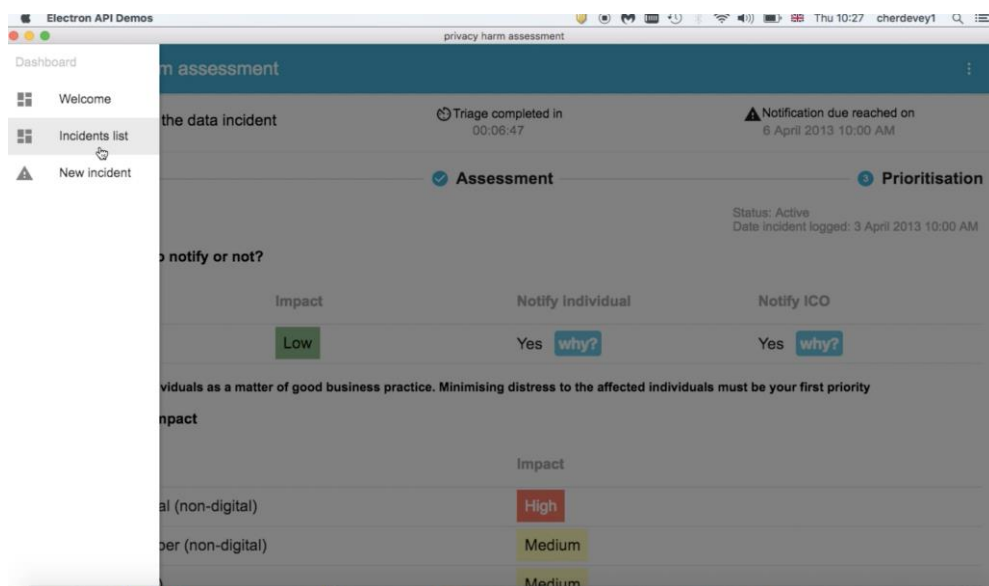
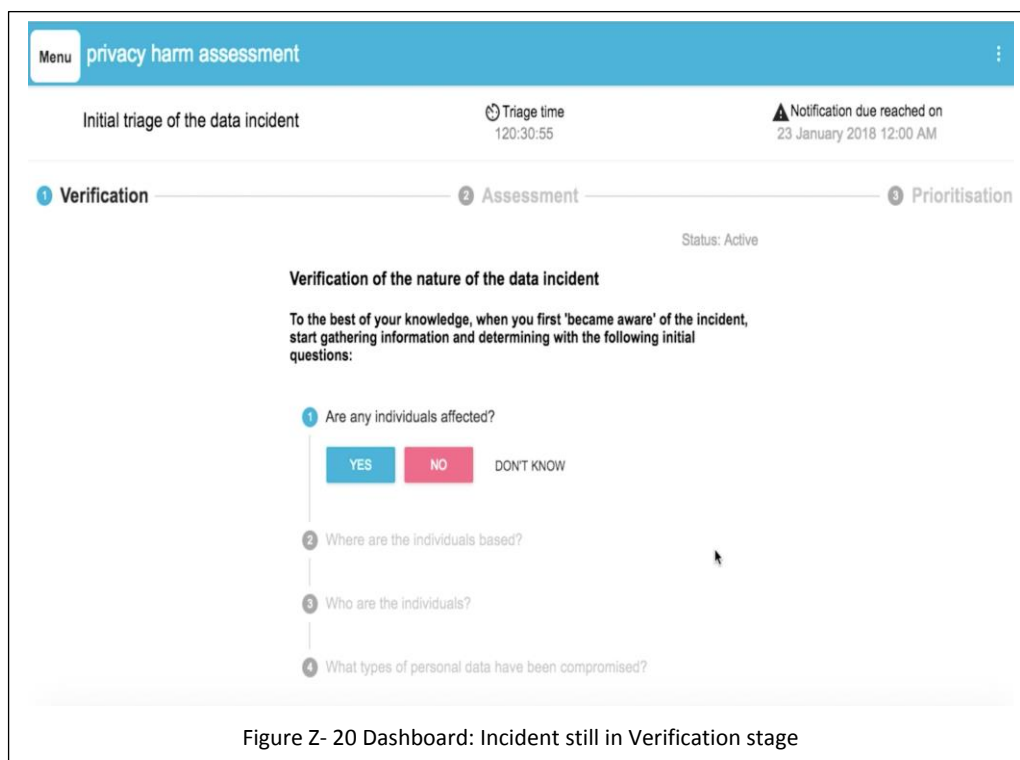
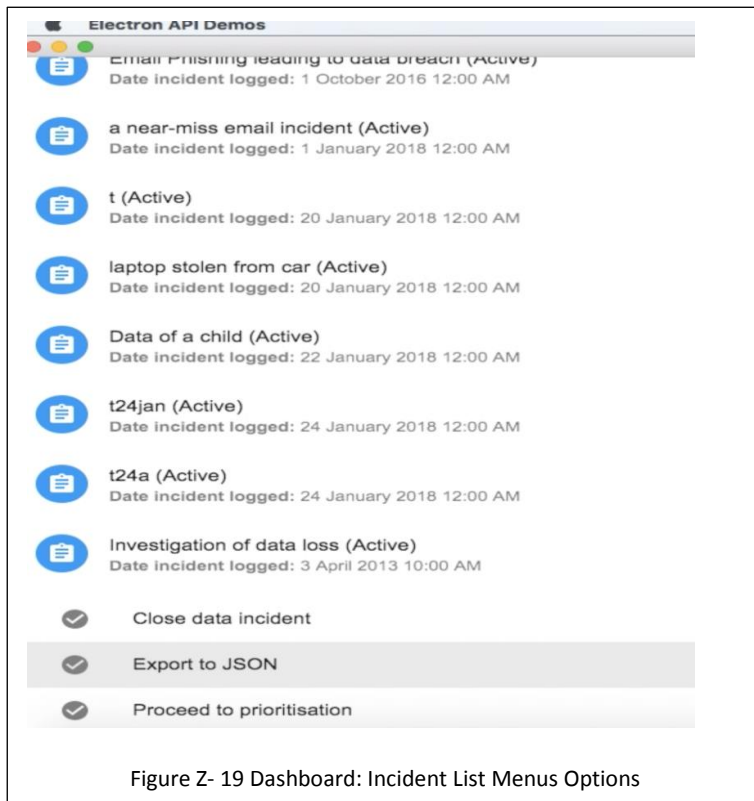


Figure Z- 18 Dashboard: Menu



User evaluation of a prototype dashboard for privacy harm assessment during initial personal data incident response - to notify or not?

Q19.

The verification, assessment and prioritisation steps are sufficient for conducting initial data incident response activities.

- ☐ Strongly agree
- ☒ Somewhat agree
- ☐ Neither agree nor disagree
- ☐ Somewhat disagree
- ☐ Strongly disagree

Figure Z- 21 Post-Dashboard: Triage sequence of steps Q1

Q22. The questions and answers in the dashboard are simple to follow.

- ☒ Strongly agree
- ☐ Somewhat agree
- ☐ Neither agree nor disagree
- ☐ Somewhat disagree
- ☐ Strongly disagree

Q23. The questions and answers in the dashboard are useful for quick checking of the necessary breach information.

- ☒ Strongly agree
- ☐ Somewhat agree
- ☐ Neither agree nor disagree
- ☐ Somewhat disagree
- ☐ Strongly disagree

Figure Z- 22 Post-Dashboard: Checklists Q22-Q23

Q27. The dashboard allows breach notification actions to be prioritised in a short timeframe.

- ☒ Strongly agree
☐ Somewhat agree
☐ Neither agree nor disagree
☐ Somewhat disagree
☐ Strongly disagree

Q28. The dashboard provides notification alerts which are useful for the prioritisation of breach notification.

- ☐ Strongly agree
☐ Somewhat agree
☐ Neither agree nor disagree
☐ Somewhat disagree
☐ Strongly disagree

Figure Z- 23 Post-Dashboard: Notification & Alerts Q27-Q28

Q30. What impact would the dashboard have on your initial data incident response?

	Extremely effective	Very effective	Moderately effective	Slightly effective	Not effective at all
Gathering of information	☐	☒	☐	☐	☐
Internal communication during the response	☐	☒	☐	☐	☐
Recording the incident response actions	☒	☐	☐	☐	☐

Q31. What improvements would you make to the dashboard?

Figure Z- 24 Post-Dashboard: Impact & Improvements Q30-Q31

Appendix AA: UES Group2: a User Walkthrough screenshots

Group2 User (I14)

The screenshot shows a web interface for a 'privacy harm assessment'. At the top, there's a blue header with a 'Menu' button and the title 'privacy harm assessment'. Below the header, there's a status bar with 'Initial triage of the data incident', 'Triage time 00:01:56', and 'Notification due in 70:48:12'. The main content area has a progress bar with three steps: '1 Verification', '2 Assessment', and '3 Prioritisation'. The 'Verification' step is active, showing a section titled 'Verification of the nature of the data incident'. Below this, there's a text prompt: 'To the best of your knowledge, when you first 'became aware' of the incident, start gathering information and determining with the following initial questions:'. A vertical list of questions follows: 1. 'Are any individuals affected?' with buttons for 'YES', 'NO', and 'DON'T KNOW'. 2. 'Where are the individuals based?'. 3. 'Who are the individuals?'. 4. 'What is your confidence level that these individuals may suffer emotional distress?'. 5. 'What types of personal data have been compromised?'. A 'Incident created successfully' message is visible in the bottom right corner.

Menu privacy harm assessment You can stop and continue (via Menu)

Initial triage of the data incident Triage time 00:01:56 Notification due in 70:48:12

1 Verification 2 Assessment 3 Prioritisation

Verification of the nature of the data incident

To the best of your knowledge, when you first 'became aware' of the incident, start gathering information and determining with the following initial questions:

1 Are any individuals affected?

YES NO DON'T KNOW

2 Where are the individuals based?

3 Who are the individuals?

4 What is your confidence level that these individuals may suffer emotional distress?

5 What types of personal data have been compromised?

Incident created successfully

Figure AA- 1 DashboardV2: Help Text

This screenshot shows the same 'Verification' step as Figure AA-1, but with more progress. The first three questions are now marked with blue checkmarks, indicating they have been answered. The fourth question, 'What is your confidence level that these individuals may suffer emotional distress?', is the current focus. It has three buttons: 'HIGH', 'MEDIUM', and 'LOW'. A tooltip is visible over the 'MEDIUM' button, displaying the text 'Less than 60%, greater than or equal to 30%'. The fifth question, 'What types of personal data have been compromised?', is partially visible at the bottom. The status bar at the top shows 'Triage time 00:03:45' and 'Notification due in 70:46:23'.

Initial triage of the data incident Triage time 00:03:45 Notification due in 70:46:23

1 Verification 2 Assessment 3

Verification of the nature of the data incident

To the best of your knowledge, when you first 'became aware' of the incident, start gathering information and determining with the following initial questions:

✓ Are any individuals affected?

✓ Where are the individuals based?

✓ Who are the individuals?

4 What is your confidence level that these individuals may suffer emotional distress?

HIGH MEDIUM LOW

Less than 60%, greater than or equal to 30%

5 What types of personal data have been compromised?

6 What is your confidence level that these personal data have been compromised?

Figure AA- 2 DashboardV2: Verification-Confidence Level-distress

Initial triage of the data incident
Triage time
00:06:47
Notification due in
70:43:21

1 Verification
2 Assessment
3 Prioritization

Verification of the nature of the data incident

To the best of your knowledge, when you first 'became aware' of the incident, start gathering information and determining with the following initial questions:

- Are any individuals affected?
- Where are the individuals based?
- Who are the individuals?
- What is your confidence level that these individuals may suffer emotional distress?
- What types of personal data have been compromised?
- What is your confidence level that these personal data have been compromised?

HIGH
MEDIUM
LOW

Figure AA- 3 DashboardV2: Verification-Confidence Level-data

Menu
privacy harm assessment

Initial triage of the data incident
Triage time
00:08:11
Notification due in
70:41:57

1 Verification
2 Assessment
3 Prioritization

Assessment of compromised data

These are the categories you have identified:

Name
Location Data
Economic/Financial
Racial or ethnic origin

We are going to ask a few questions about each category to determine the likely impact of data harm to affected individuals

What is your confidence level for the compromised volume of data?

HIGH
MEDIUM
LOW

Figure AA- 4 DashboardV2: Assessment-Confidence Level-volume

Initial triage of the data incident
Triage time
00:08:53
Notification due in
70:41:57

1 Verification
2 Assessment
3 Prioritization

Assessment of compromised data

These are the categories you have identified:

Name
Location Data
Economic/Financial
Racial or ethnic origin

We are going to ask a few questions about each category to determine the likely impact of data harm to affected individuals

What is your confidence level for the security protection and safety measures?

HIGH
MEDIUM
LOW

Greater than or equal 60%

Figure AA- 5 DashboardV2: Assessment-Confidence Level-security

Do please notify the individuals as a matter of good business practice. Minimising distress to the affected individuals must be your first priority

Likely level of data impact

Type of data	Impact
Name (digital)	Medium
Location Data (digital)	Medium
Economic/Financial (digital)	High
Racial or ethnic origin (digital)	High



Figure AA- 6 DashboardV2: Prioritisation-Confidence Level-display

Racial or ethnic origin (digital)

High



Be mindful with personal data

Figure AA- 7 DashboardV2: Prioritisation-Confidence Level-display2

Appendix AB: UES Users: MSD Dashboard screenshots

A Group1 User JSON file imported into MSD

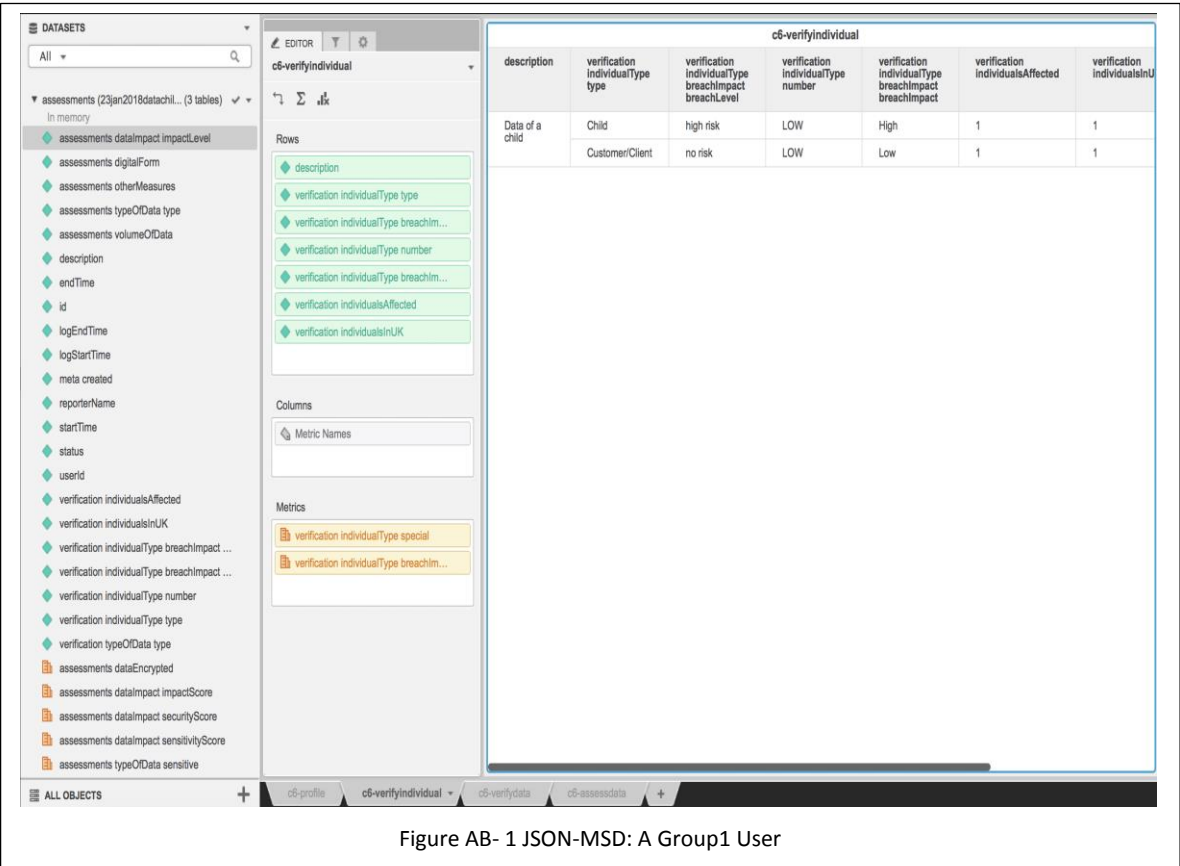


Figure AB- 1 JSON-MSD: A Group1 User

A Group2 User JSON file imported into MSD

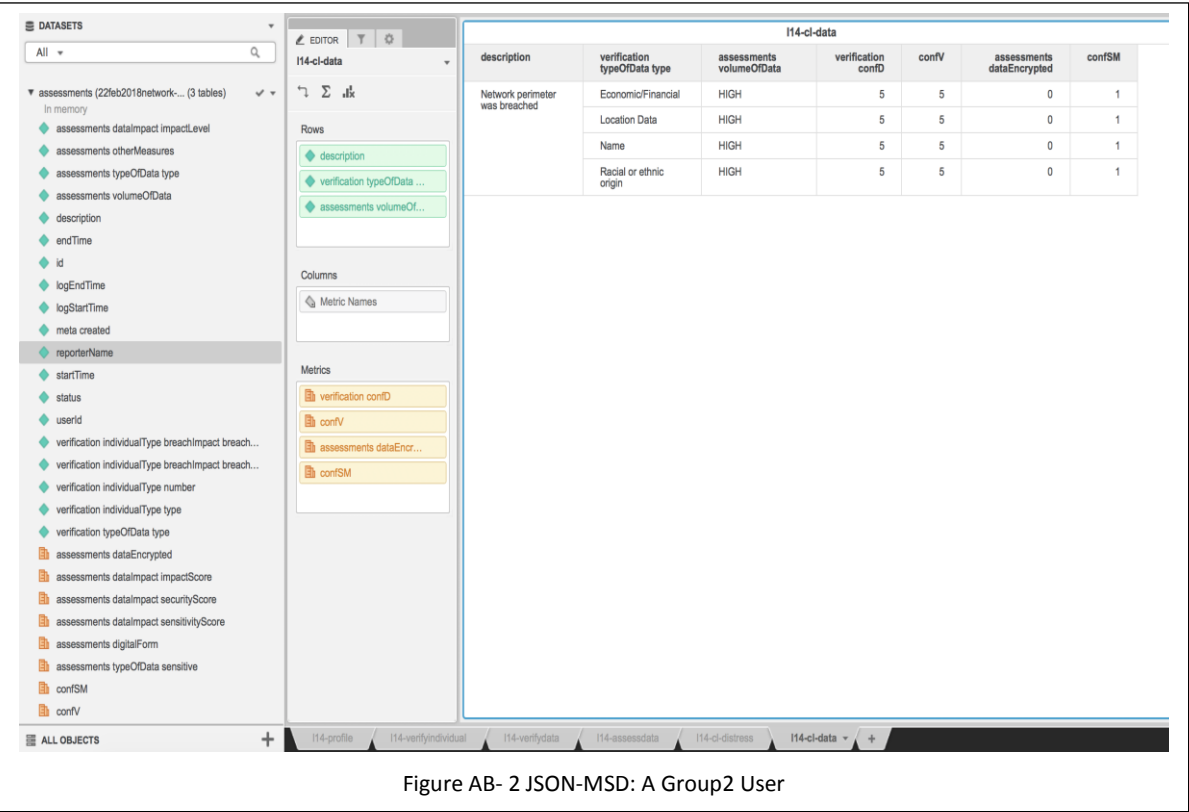


Figure AB- 2 JSON-MSD: A Group2 User

Appendix AC: UES Groups: MSD Dashboard screenshots

Integrated Group1 Dashboard: A chart showing impact levels on individuals & notifications



Integrated Group2 Dashboard: A chart showing the data impact levels.



Appendix AD: UES Groups: Qualtrics reports transformation

A snapshot of the Qualtrics tsv exported file (many fields)

Start Date	End Date	Response Type	IP Address	Progress	Duration (in seconds)	Finished	Recorded Date	Response ID	Distribution Channel	ID
{"Importid": "start Date", "timeZone": "Europe/London"}	{"Importid": "end Date", "timeZone": "Europe/London"}	{"Importid": "status"}	{"Importid": "ip Address"}	{"Importid": "progress"}	{"Importid": "duration"}	{"Importid": "finished"}	{"Importid": "recordedDate", "timeZone": "Europe/London"}	{"Importid": "recordid"}	{"Importid": "distributionChannel"}	{"Importid": "id"}
10/01/2018 14:52	10/01/2018 16:33	Imported	198.8.160.36	100	6057	TRUE	09/02/2018 11:41	R_8bQpHm	anonymous	f1
10/01/2018 21:09	11/01/2018 11:58	Imported	138.40.67.206	100	53295	TRUE	09/02/2018 11:41	R_6MaEzTd	anonymous	e2
14/01/2018 10:22	14/01/2018 10:59	Imported	31.153.74.205	100	2240	TRUE	09/02/2018 11:41	R_bPO0NjH	anonymous	b3
15/01/2018 09:50	18/01/2018 16:19	Imported	89.197.120.10	100	282544	TRUE	09/02/2018 11:41	R_9ZeSrYm	anonymous	o4
18/01/2018 18:00	18/01/2018 18:43	Imported	91.216.55.150	100	2579	TRUE	09/02/2018 11:41	R_CgPVH	anonymous	h5
23/01/2018 11:09	23/01/2018 12:14	Imported	94.14.224.224	100	0	TRUE	09/02/2018 11:41	R_OUtUchHr		c6
25/01/2018 09:45	25/01/2018 10:49	Imported	138.40.67.162	100	3840	TRUE	09/02/2018 11:41	R_OuluniJK	anonymous	g7
01/02/2018 12:38	01/02/2018 14:41	Imported	138.40.67.190	100	7388	TRUE	09/02/2018 11:41	R_eVA4sdt	anonymous	f8

Figure AD- 1 UES Qualtrics Export

A snapshot of the Qualtrics (cleaned-up) Excel file: Group1

StartDate	What is your role or title?	How long have you been in this role or title?	What are the responsibilities of your role or title?	conducted PIA?	conducted PHA during DBI response?	data incident scenario	nature or type of chosen data incident:	the overall level of distress	The sequence of vap steps is appropriate during initial DBI	The Q&A in the dashboard are simple to follow.	In closing this study, what else would you like to add?	0
10/01/2018 14:52	Underwriting Manager, Vice President, Strategic	8 years	Responsible for a portfolio of insurance business.	No.	Other	experience	A phishing attempt led to the breach by an HR	Medium level of distress	Somewhat agree	Strongly agree		f1
10/01/2018 21:09	Information Compliance Officer	2 years 7 months	I am responsible for providing advice to C on its obligations.	Yes.	Yes.	experience	Data was stored in an not secured mem. The	High level of distress	Somewhat agree	Strongly agree	None	e2
14/01/2018 10:22	CEO	30 years	Running & governance of my	Yes.	Yes.	hypothetical	Unauthorised access	High level of distress	Somewhat agree	Somewhat agree	It would be nice to be able	b3
15/01/2018 09:50	Chief Executive Officer	8 Years	Responsible for oversight of the Institute executive team	No.	No.	experience	Data loss due to email phishing activity	Low level of distress	Strongly agree	Strongly agree	No thank you.	o4
18/01/2018 18:00	Information governance	5.5 years	All aspects of Information governance inc. Incident	Yes.	Yes.	experience	An email is sent to an external reliable source	Medium level of distress	Somewhat agree	Neither agree nor disagree	Correlation with Privacy Harm Risk Matrix	h5
23/01/2018 11:09	K - chief data protection officer, finance based	K - 3 months, prior to this, in finance	DPO/PPM	Yes.	Other	experience	Data about a child	High level of distress	Strongly agree	Strongly agree	None	c6
25/01/2018 09:45	Compliance and Information Governance	18 years in local government, 20	Previously I have been nominated data protection	Yes.	Other	experience	Loss of fraud investigation files from	High level of distress	Strongly agree	Strongly agree	Assumption this form would be hosted? Or	g7
01/02/2018 12:38	Title MD. Role is advising firms from the children to	overall, 15 years.	Explaining what good assessment is and how it is	No.	No.	experience	My personal data was taken from a tablet	High level of distress	Somewhat agree	Strongly agree	This has great potential. Firms should want and	f8

Figure AD- 2 UES Qualtrics Group1 Report

A snapshot of the Qualtrics (cleaned-up) Excel file: Group2

StartDate	What is your role or title?	How long have you been in this role or title?	What are the responsibilities of your role or title?	conducted PIA?	conducted PHA during DBI	data incident scenario	nature or type of chosen data incident:	the overall level of distress	0
07/02/2018 17:28	Managing Director	6 years	I run and deliver consultancy on the commercial side of	Yes.	No.	experience	A person employed by a health	High level of distress	h9
12/02/2018 12:05	Head of Infosec	5 years STC company 20 years experience	Oversee ISMS. Manage Cyber	No.	Yes.	experience	Set of correspondence has been	Low level of distress	c10
12/02/2018 18:34	Director	5 yrs + 10 yrs banking + 3 yrs with a BIG consultancy firm	Managing Director	Other	No.	response planning	Walkthrough the TalkTalk data incident.	Medium level of distress	b11
13/02/2018 17:54	Backend Java Software Engineer	2 years	Developing microservices which monitor most of the	Yes.	No.	response planning	In this scenario a web application service is responsible for handling the	Medium level of distress	b12
15/02/2018 13:14	Information Management Consultant	30 years	Ensuring data protection compliance, adequate	Yes.	Yes.	experience	Student accessing health records which are restricted.	Low level of distress	b13
22/02/2018 17:02	Principal Consultant	15+ years	Provide business intelligence,	No.	Yes.	experience	Network perimeter was breached that	High level of distress	t14
06/03/2018 14:06	Independent Consultant	8 years and 38 years in IT	Providing consultancy advice in IT related matters.	No.	No.	hypothetical	my bank has been hacked	High level of distress	b15
10/03/2018 10:44	Deputy General Manager	6 years	I manage a team of 50 Catering staff members. My	No.	No.	hypothetical	Hypothetically, personnel data has been stolen from a locked HR cabinet.	High level of distress	b16
12/03/2018 13:24	GDPR Project Manager	9 months this role. 30 years overall.	Responsible for all delivery	Yes.	Yes.	hypothetical	USB stick left on a train by a member of	Medium level of distress	f17

Figure AD- 3 UES Qualtrics Group2 Report

Appendix AE: UES Groups: Questionnaire-MSD

Questionnaire Excel in MSD - Questions organised by topics/themes

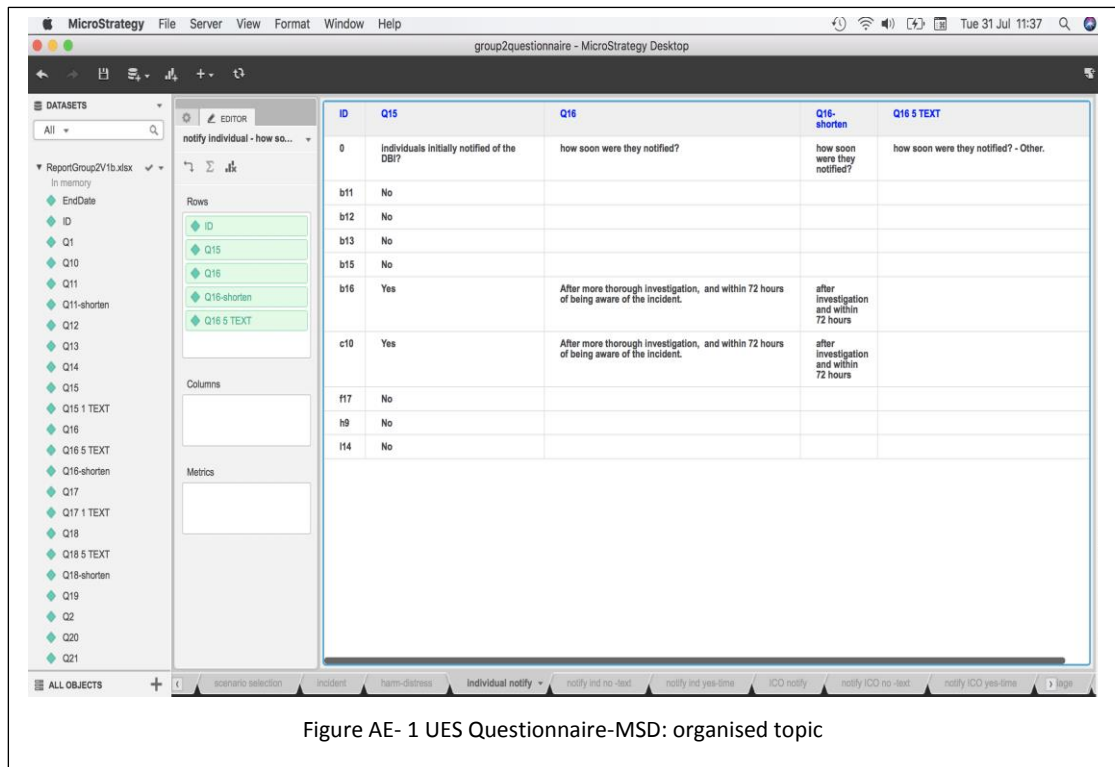


Figure AE- 1 UES Questionnaire-MSD: organised topic

Group1 Questionnaire: Checklist results

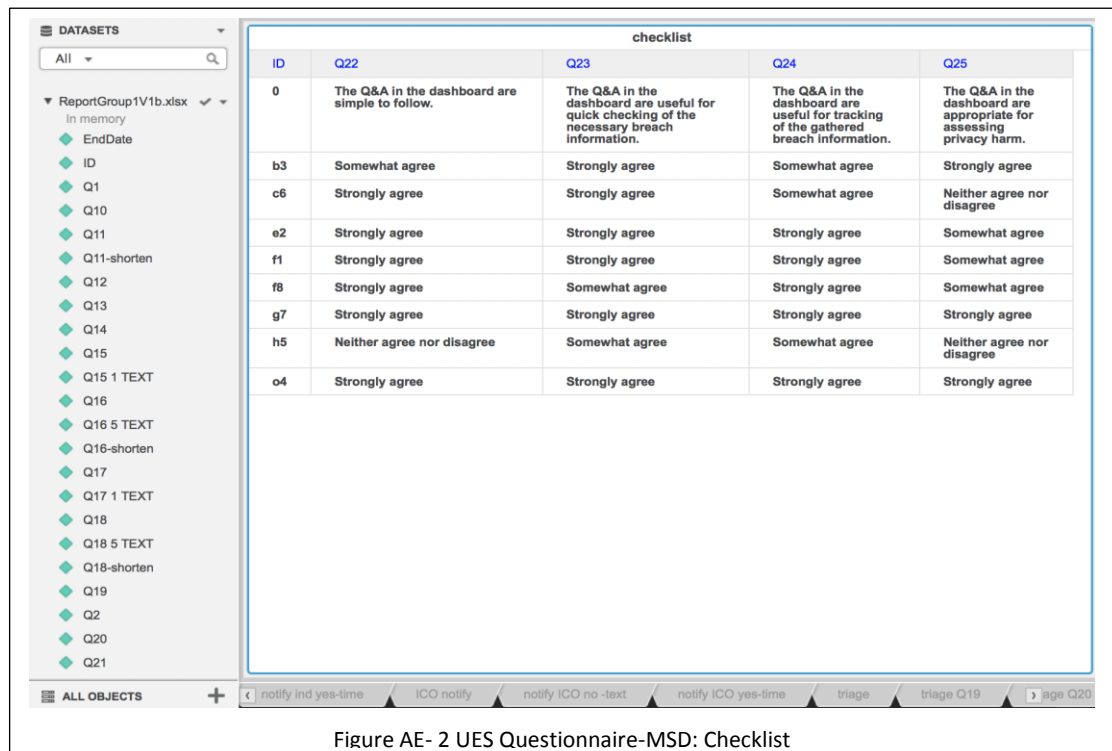


Figure AE- 2 UES Questionnaire-MSD: Checklist

Group2 Questionnaire: Other remarks (Q31-Q32)

DATASETS		Open question & closing remarks		
All		ID	Q31	Q32
▼ ReportGroup2V1b.xlsx		0	What improvements would you make to the dashboard?	In closing this study, what else would you like to add?
In memory		b11	Integration with other data inventory or asset management or CMDB.	Easy to use during a crisis.
◆ EndDate		b12	The dashboard is user friendly, easy to use and very clear The menu options are simple and not confusing It is great to have the incident alert which would be triggered after 72 hours	Incidents Response is very important and logging incidents are not just beneficial for legal purposes but also for resolving the incidents The dashboard is a very good centralized auditing system which can be used to log incidents and share knowledge of the incidents with the team and external stakeholders.
◆ ID		b13	Allow summary of reported incidents and alerts assigned to management showing high risks. Use numbers and appropriate colors to show relative levels of risk.	Run a pilot with the enhanced features. Look at W29 articles for further enhancement.
◆ Q1		b15	It is very pertinent to the solutions of a very important problem.	The quicker it can be transferred to organisations for their use the better.
◆ Q10		b16	No improvements - very clear and quick Would like a printout of the summary screen	It is a very quick and easy to navigate system. My hypothetical scenario took only 5 minutes and 30 seconds to complete during first use therefore it is a quick dashboard - ideal for use by those with a hectic work schedule but need to find out answers within the time restraints. Upon reflection, it is possible to have both digital and non-digital formats of the same data therefore the question in the dashboard asking if there is non-digital data, this neglects the fact that there is both digital and non-digital. It would be helpful if there was some help text to direct users that a separate incident needs to be logged to cover both digital and non-digital in the prototype. Post prototype for a real system, maybe additions need to be made to include both for efficiency purposes.
◆ Q11		c10	Expand the information gathering activities. Build intelligence into the dashboard - decision algorithm a platform for further development - aiding or supporting analysis and decision-making additionally more reporting capabilities for different categories e.g. technical team information	A good foundation for sound analysis of incident and the impact of incidents; further development of the tool could provide a very useful management decision-making and the technical aspects of incident response.
◆ Q11-shorten		f17	Internal comms: dashboard / questions talk about the data subject and the ICO - to support internal comms, need to also identify other interested stakeholders e.g. current client has an "Incident Response Team" and an "IT Security Group" that would also need to be notified immediately. Gathering of info: may be other forms of protection that could influence impact e.g. end-point encryption, file passwording or high-level questions such as "Is data aggregated?" Notification: Assumes 72 hour response? If acting as a processor, may need to respond more quickly to the controller so that they can meet their own deadline - so maybe need to be able to influence countdown. Overall: good, simple format - useful to support internal comms and audit evidence.	For dashboarding at high level, fine as is.. Maybe for future and to be able to make more relevant to different organisations, maybe some parameter-driven elements
◆ Q12		h9	As a deployed tool, it might be useful to have internal notifications sent automatically	I think this tool has huge potential to support organisations with a simple structured assessment in an area where there is little knowledge or understanding
◆ Q13		i14	Initial thoughts are that the dashboard is intuitive and provide the requisite checkpoints for recording all the relevant information to undertake an investigation. The questions prompt as well as direct the would be responder to think carefully and precisely about the answers to provide, as these drive the manner in which the output directs the responder to respond to the incident. Suggestions: 1) Alert notification could be more impactful i.e. appear in red or in bold, or provide the possibility of sending a text alert or email notification.	As this is work in progress/a prototype, continuous improvement based on the answers from participants is key to the continuous modelling of the dashboard.
◆ Q14				
◆ Q15				
◆ Q15 1 TEXT				
◆ Q16				
◆ Q16 5 TEXT				
◆ Q16-shorten				
◆ Q17				
◆ Q17 1 TEXT				
◆ Q18				
◆ Q18 5 TEXT				
◆ Q18-shorten				
◆ Q19				
◆ Q2				
◆ Q20				
◆ Q21				
◆ Q22				
◆ Q23				
◆ Q24				
◆ Q25				
◆ Q26				
ALL OBJECTS				
		notify ind yes-time	ICO notify	notify ICO no -text
		notify ICO yes-time	triage	checklist
		dashboard	Q28	Q29
				impact res

Figure AE- 3 UES Questionnaire-MSD: Other remarks (Q31-Q32)

Figure AE- 3 UES Questionnaire-MSD: Other remarks (Q31-Q32)

Appendix AF: UES NVivo Samples

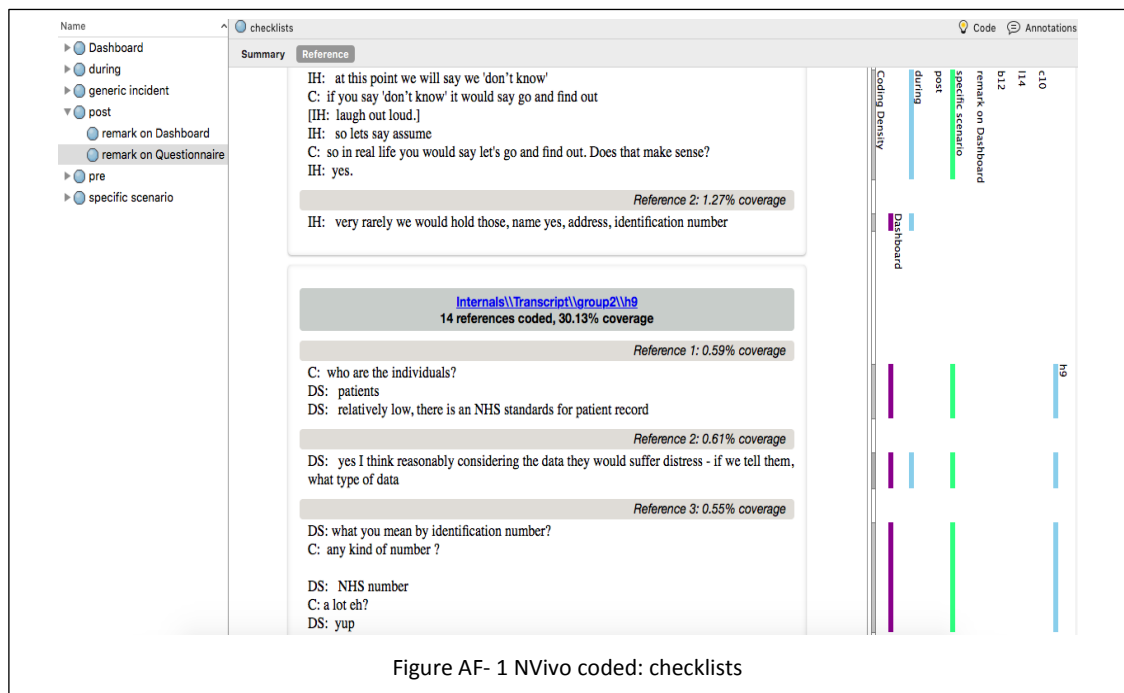


Figure AF- 1 NVivo coded: checklists

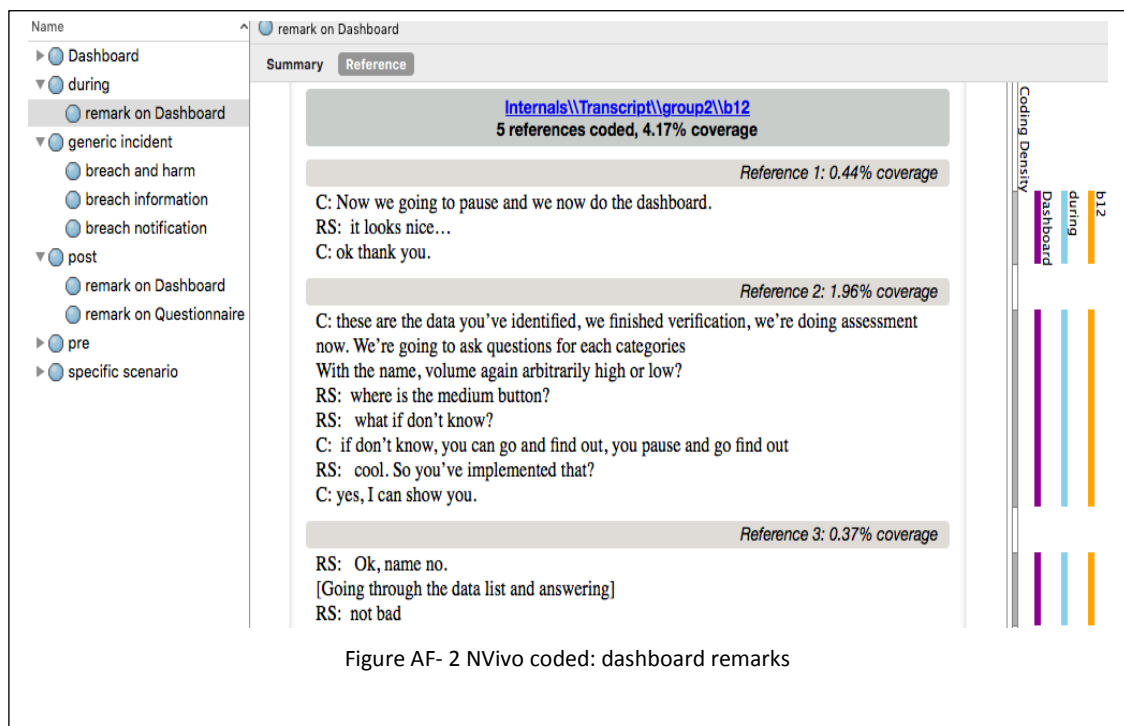


Figure AF- 2 NVivo coded: dashboard remarks

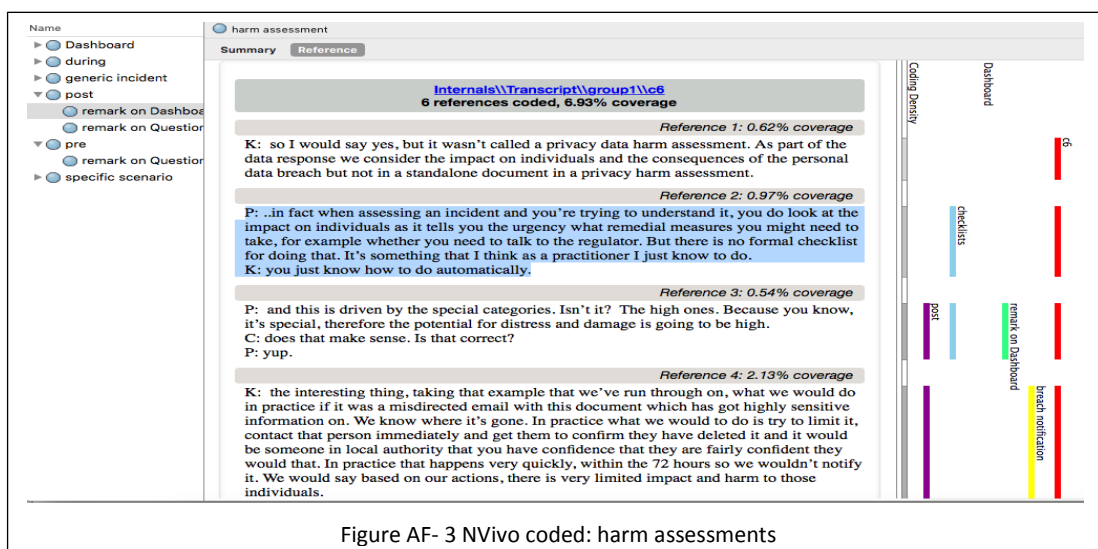


Figure AF- 3 NVivo coded: harm assessments

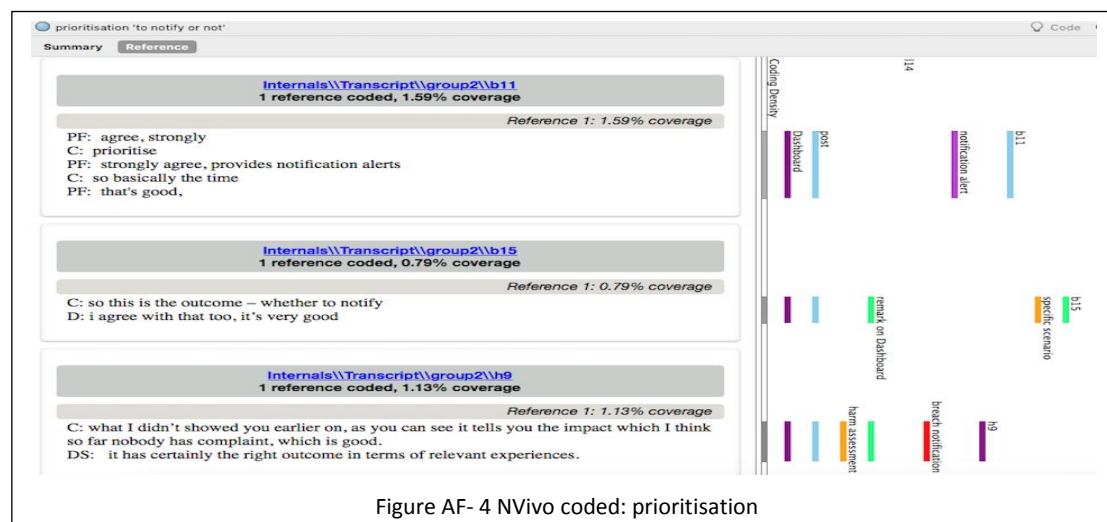


Figure AF- 4 NVivo coded: prioritisation

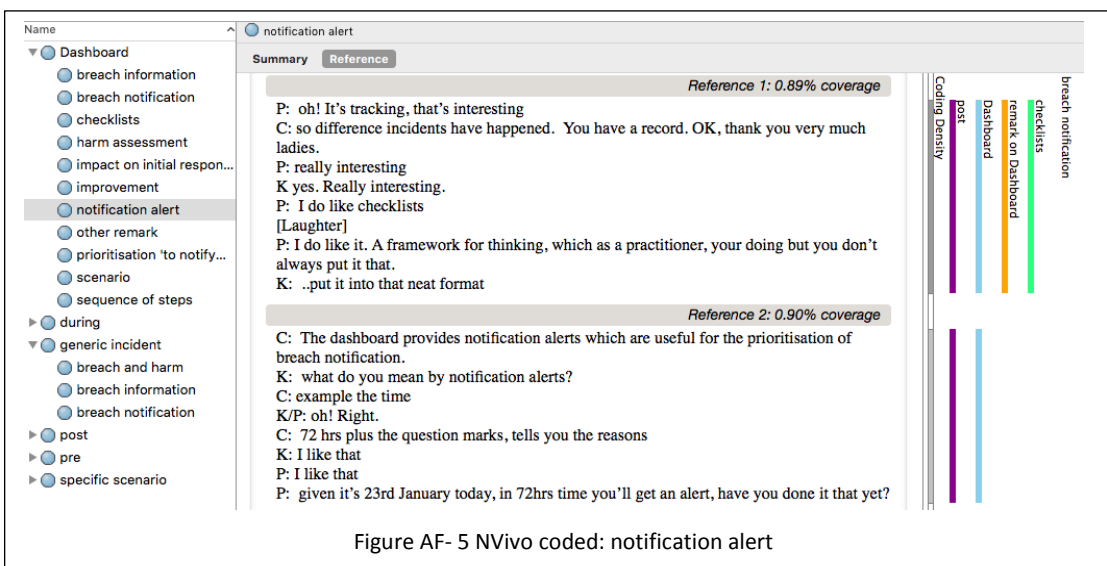


Figure AF- 5 NVivo coded: notification alert

Appendix AG: Specific incidents descriptions

ID	Incident type (Q11)	Specific incident (Q12)
e2	real	Data was stored in an old disused room. The data contained sensitive personal data of participants of a previous study, it contained approximately 450 sensitive personal data. upon identification, I noticed it was a breach of the 7th DPA and took steps to moved it to a secure storage and conducted a review and made recommendation to report to ICO.
h5	real	An email is sent to an external reliable source without encryption. Firstly it was intended to send anonymous information but the sender has not realised that it involves some hidden data in pivot table.
b3	hypothetical	Unauthorised access to and theft of a client's personal data
c6	real	Data about a child (social work information, highly sensitive) shared with an unrelated agency - sent to wrong place, by email.
g7	real	Loss of fraud investigation files from public house. Material had been taken out of the office without permission, though officer intending to clear backlog - therefore well-meaning. Files in a unlocked bag left unattended. Suspicion that assailants were after laptop but only files were in the bag. Likely conclusion that bag was disposed of, however no confirmation to that effect. Files were of individuals being investigated for benefit fraud, therefore sensitive personal data, and concern over prosecution action that might have followed. 17 paper files lost.
o4	real	Data loss due to email phishing activity
f8	real	My personal data was taken from a stolen, 3rd party, laptop.
f1	real	A phishing attempt led to the breach by an HR department of c.25,000 employee social security numbers in the US (W2 breach).

Figure AG- 1 Group1 specific incidents description

ID	Incident type (Q11)	Specific incident (Q12)
b13	real	Student accessing health records which are restricted.
c10	real	Set of correspondence has been printed. But due to a format change that was not tested adequately. Information was printed out of sequence, thus data pertaining to other individuals was printed on the back of the valid letter and sent out. Thus breaching confidentiality.
h9	real	A person employed by a health provider took paper-based records home at the end of their working day, in breach of policy. Their house was burgled and the records were taken. The police caught the burglar but failed to recover the records. The records contained safeguarding information about children.
b11	response planning	Walkthrough the TalkTalk data incident.
b16	hypothetical	Hypothetically, personnel data has been stolen from a locked HR cabinet in my office
f17	hypothetical	USB stick left on a train by a member of one of the insurance admin teams
l14	real	Network perimeter was breached that led to exposure of personal data in a number of relational databases that hold client and limited employee data.
b12	response planning	In this scenario a web application service is responsible for handling the login of user's to a site. After succesful login, the service is expected to redirect the user to the companies home page or a page on the site. This is controlled using a query param on the page. The security vulnerability was that the web application did not verify the redirect site. This could be intercepted by an attacker and could be changed to an attackers site. The attacker could potentially collect usernames and passwords.
b15	hypothetical	my bank has been hacked

Figure AG- 2 Group2 specific incidents description

Appendix AH: Data scenarios: data and impact

data	description	ID		
Cultural(digital)	Data of a child	c6		Medium
Cultural(non-digital)	paper records left in a room	e2		Medium
Economic/Financial(digital)	Data of a child	c6		High
	Personal data from a stolen laptop	f8		High
	Phishing	f1		High
	Unauthorised access to and stealing of personal client data	b3		High
Economic/Financial(non-digital)	Investigation of data loss	g7		High
Health(digital)	Data of a child	c6		High
Health(non-digital)	paper records left in a room	e2		High
Identification number(digital)	a near-miss email incident	h5		Medium
	Email Phishing leading to data breach	o4		Medium
	Personal data from a stolen laptop	f8		Medium
	Unauthorised access to and stealing of personal client data	b3		Medium
Identification number(non-digital)	Investigation of data loss	g7		Medium
	paper records left in a room	e2		Medium
Location Data(digital)	Data of a child	c6		Medium
	Email Phishing leading to data breach	o4		Medium
	Personal data from a stolen laptop	f8		Medium
	Phishing	f1		Medium
	Unauthorised access to and stealing of personal client data	b3		Medium
Location Data(non-digital)	Investigation of data loss	g7		Medium
Name(digital)	a near-miss email incident	h5		Medium
	Data of a child	c6		Medium
	Email Phishing leading to data breach	o4		Medium
	Personal data from a stolen laptop	f8		Medium
	Phishing	f1		Medium
	Unauthorised access to and stealing of personal client data	b3		Medium
Name(non-digital)	Investigation of data loss	g7		Medium
	paper records left in a room	e2		Medium
Online identifier(digital)	Unauthorised access to and stealing of personal client data	b3		Medium
Racial or ethnic origin(digital)	Data of a child	c6		High
Racial or ethnic origin(non-digital)	Investigation of data loss	g7		High
	paper records left in a room	e2		High
Religious or philosophical beliefs(digital)	Data of a child	c6		High
Religious or philosophical beliefs(non-digital)	Investigation of data loss	g7		High
Sex life or sexual orientation(digital)	Data of a child	c6		High
Sex life or sexual orientation(non-digital)	paper records left in a room	e2		High
Social (Not metadata)(digital)	Data of a child	c6		Medium
Social (Not metadata)(non-digital)	Investigation of data loss	g7		Medium
	paper records left in a room	e2		Medium

Figure AH- 1 Group1 data types and impact levels

data	description	ID	Impact
Cultural(non-digital)	Paper record stolen	h9	Low
Economic/Financial(digital)	bank account at risk	b15	High
	Error in coding and lack of verification checking (printing)	c10	High
	Network perimeter was breached	i14	High
	Stolen data	b16	High
	TalkTalk data incident	b11	High
Health(digital)	Student access restricted health records	b13	High
Health(non-digital)	Paper record stolen	h9	High
	Stolen data	b16	High
Identification number(digital)	USB stick lost on train	f17	Medium
	web service redirect vulnerability	b12	Low
Identification number(non-digital)	Paper record stolen	h9	Low
	Stolen data	b16	Low
Location Data(digital)	bank account at risk	b15	Medium
	Error in coding and lack of verification checking (printing)	c10	Medium
	Network perimeter was breached	i14	Medium
	TalkTalk data incident	b11	Medium
	USB stick lost on train	f17	Medium
Location Data(non-digital)	Paper record stolen	h9	Low
	Stolen data	b16	Low
Name(digital)	bank account at risk	b15	Medium
	Error in coding and lack of verification checking (printing)	c10	Medium
	Network perimeter was breached	i14	Medium
	Stolen data	b16	Medium
	TalkTalk data incident	b11	Medium
	USB stick lost on train	f17	Medium
	web service redirect vulnerability	b12	Medium
Name(non-digital)	Paper record stolen	h9	Low
Online identifier(digital)	bank account at risk	b15	Medium
	TalkTalk data incident	b11	Medium
Picture/Image/Video(non-digital)	Stolen data	b16	Low
Racial or ethnic origin(digital)	Network perimeter was breached	i14	High
Racial or ethnic origin(non-digital)	Paper record stolen	h9	High
	Stolen data	b16	High
Religious or philosophical beliefs(non-digital)	Paper record stolen	h9	High
	Stolen data	b16	High
Sex life or sexual orientation(non-digital)	Paper record stolen	h9	High
Trade union membership(non-digital)	Stolen data	b16	High

Figure AH- 2 Group2 data types and impact levels

Individual	notify individual	notify ICO	ID	
Child	Yes	Yes	c6	High
Customer/Client	Yes	Yes	b3	Medium
			c6	Low
			e2	Medium
			f8	Low
			g7	Low
Employees	Yes	Yes	f1	Medium
Patient	Yes	Yes	h5	High
Student/Researcher	No	Yes	o4	Medium
Subscriber/Member	No	Yes	o4	Medium

Figure AH- 3 Group1 individual types and impact levels

Individual	notify individual	notify ICO	ID	
Child	Yes	Yes	h9	High
Customer/Client	No	Yes	b12	Low
			f17	Medium
			b11	Medium
	Yes	Yes	b15	Medium
			l14	Medium
			c10	Medium
Employees	Yes	Yes	b15	Medium
			b16	Low
			l14	Medium
Patient	Yes	Yes	b13	High
			h9	High

Figure AH- 4 Group2 individual types and impact levels