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

List of Diagrams in Appendices

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 Commissoner'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, *artefact* was used throughout this research except in direct quotes where *artifact* 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	*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* (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 25th 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 25th 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 *The incident management lifecycle process*, 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	*Key word in context*: 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 *tables* (i.e. sheets) are presented as *images.* Editing large *tables* in MS Office (Mac version) *text* 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 *first aware.* 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 *the likely consequences of the data breach* 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 *scripts* sounds more in tune with the nature of the usage of a playbook. Playbook also denotes *action*, unlike a framework. A *frame for workin*g rather than a *script for action*.
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 *privacy harm* and *harm* are used synonymously. The terms *consequence* or *damage* instead *of harm* are also used. For example, the GDPR uses *damage* instead of *harm.*
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 *italics*	Questions, original texts and quotations are in *italics*. 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. 1st use of a shortening label. Also, data captured in the prototype dashboard is shown in *italic* **and bold** 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 practitioners[1] 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 presented at the BCS Office in London. Most recently in 2018, this researcher publicised[2] her research

[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

[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].

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 2012[3], 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 researchers[4]. 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 *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.

---

[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].

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.

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,

[5] The authors cited Solove (2006).

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) *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?*		
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 **2nd 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*: to notify or not affected individuals and/or the ICO?*	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 jurisdictions[6].

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).

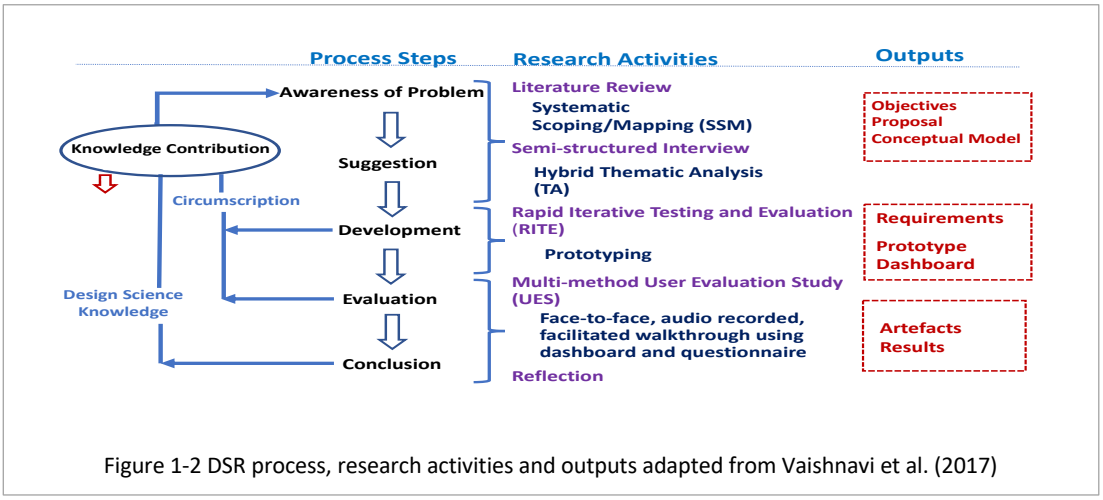

Figure 1-2 DSR process, research activities and outputs adapted from Vaishnavi et al. (2017)

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.

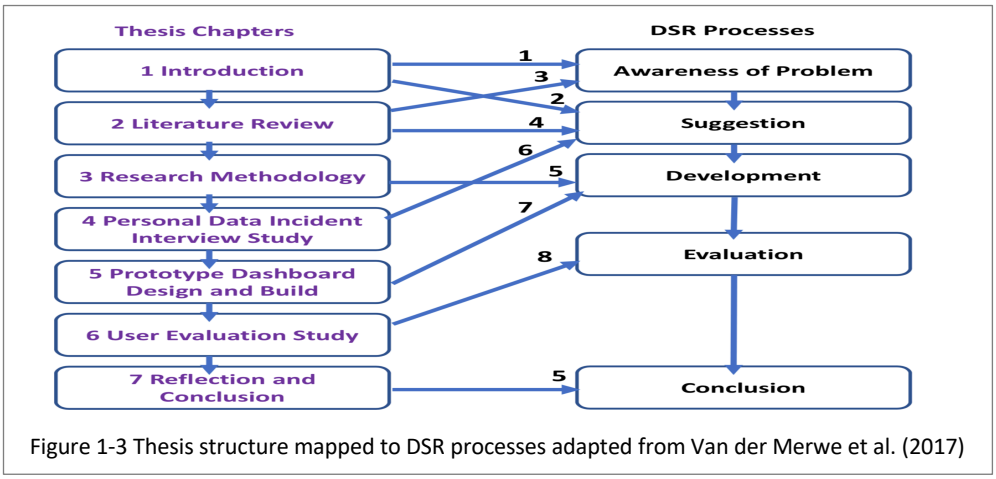

Figure 1-3 Thesis structure mapped to DSR processes adapted from Van der Merwe et al. (2017)

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.