"When Data Breaches Happen, Where Does the Buck Stop? . . . and where should it stop?"

Partha Das Chowdhury
University of Bristol
Bristol, United Kingdom
partha.daschowdhury@bristol.ac.uk

Karen Renaud
University of Strathclyde
Glasgow, Scotland, UK
karen.renaud@strath.ac.uk

Awais Rashid
University of Bristol
Bristol, United Kingdom
awais.rashid@bristol.ac.uk

Abstract

A digital-first society requires its citizens to carry out essential activities online e.g., applying for a passport, managing pension funds or scheduling medical appointments. Sensitive and personal information is requested and provided in the hope that the confidentiality, integrity and availability thereof will be preserved. In reality, data breaches occur with distressing regularity. When this occurs, 'second' victims are created: the customers whose data has been leaked. In many cases, service providers demonstrate very little care or concern for these victims, responsibilizing instead of supporting them. We surveyed 175 respondents, including second victims, non-victims and managers. It becomes clear that a 'feudal security' paradigm informs organisations' responses to data breaches. Indeed, the buck seems to stop with second victims, instead of with the breached service provider. We propose an 'Ethical Responsibilization' paradigm which would see second victims treated more equitably and fairly.

ACM Reference Format:
Partha Das Chowdhury, Karen Renaud, and Awais Rashid. 2024. "When Data Breaches Happen, Where Does the Buck Stop? . . . and where should it stop?". In *New Security Paradigms Workshop (NSPW '24), September 16–19, 2024, Bedford, PA, USA.* ACM, New York, NY, USA, 20 pages. https://doi.org/10.1145/3703465.3703474

1 Introduction

Data breaches proliferate[1]. A study involving organisations across 65 countries reported that only 14% did not suffer a data breach in a three year period ending in 2022 [77]. In the two-year period (2018-2019) there were 10,000 major data breaches with an estimated breach of up to 22 billion records [67]. An ENISA report revealed that 97 zettabytes of data were produced and consumed in 2022. A year-on-year growth predicts 181 zettabytes of lost data by 2025. This includes tweets, emails, messages, and google searches [39]. This data belongs to customers, who depend on service providers to prevent unauthorised exposure and consequent malicious use of their personal data [99]. However, the security vs. usability trade-off [4] and the increasing use of AI tools by hackers [83] can make it challenging for service providers to prevent data breaches.

Leaked data cannot be *unleaked* [28]. The aftermaths of breach events can constitute a conundrum for *second victims* (whose data was leaked during the organisation's breach event). Corporate entities often put these victims in an untenable position by leaving them to navigate obstacles and cope with consequent harms [59]. We refer to those whose data is held by organisations as 'customers', to customers whose data has been breached as 'victims' (with 'non-victims' not having suffered a data breach), and those who are left with the responsibility to manage the aftermath as 'second victims'. In using the term 'victim', we follow the code of practice in various jurisdictions: "a victim is defined as a person who has suffered physical or emotional harm, property damage, or economic loss as a result of a crime"[2].

A data breach by an act of omission or commission can cause physical, emotional harm and can lead to economic loss and/or property damage. We refer to individuals who suffered data breaches as *'victims'* or *'second victims'* interchangeably.

Motivating Example: Consider the UK's Universities Superannuation Scheme (USS) [37], whose customers' *title, initial(s), name; date of birth; national insurance number; USS member number* was leaked, essentially very sensitive data. USS had contracted Capita to store their customers' data (without informing customers). When Capita had a breach, USS informed their customers that Capita had leaked their personal details. Instead of getting support from USS, individual victims had to personally implement countermeasures: e.g., creating Experian accounts and monitoring their accounts for suspicious activity, all without guidance on what they should do if something happens. There was no attempt by USS to take responsibility (noting that it was Capita's issue). Responsibility was pushed onto second victims. No responsibility was taken by Capita either, except that they committed to monitor the dark web.

This left second victims to manage a risk they did not cause and the consequences of which they might be ill-equipped to manage. They were expected to absorb any losses that occurred as a consequence of the breach. In essence, second victims were *responsibilized*, a popular cybersecurity regime: people are given advice and then left to manage by themselves, despite often needing more support [82].

If 21^{st} century citizens had a choice, they could simply not provide their information but, in reality, they have no choice in our digital-first society. When organisations fail in their curatorship responsibilities and data breaches occur, the second victims face potential harm through no fault of their own. Research specific to

[1] The European Council defines data breaches as: "*A data breach occurs when the data for which your company/ organisation is responsible suffers a security incident resulting in a breach of confidentiality, availability or integrity*" [40]

[2] https://www.justice.gc.ca/eng/cj-jp/victims-victimes/rights-droits/who-qui.html

This work is licensed under a Creative Commons Attribution International 4.0 License.

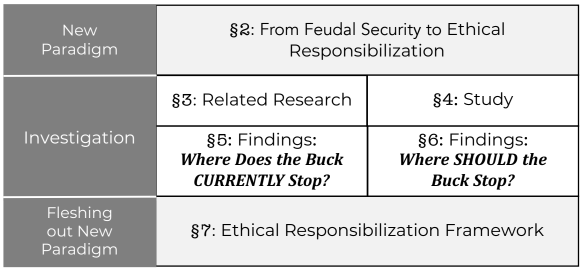
NSPW '24, September 16–19, 2024, Bedford, PA, USA
© 2024 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-1128-2/24/09
https://doi.org/10.1145/3703465.3703474

data breaches primarily cover aspects of breach management [55] and measures to regain trust [52]. Legal scholarship has identified the limitations of extant legal frameworks to counter mass harvesting of data [30, 91]. However, examining data breach management from the victim's perspective is an understudied area.

We surveyed 175 respondents, including 131 declared 'second victims' of data breaches. We found that second victims of data breaches were generally left to recover without much assistance i.e., the buck stopped with them. We conclude that the *status quo* in responding to victims is akin to **feudal security**, a term coined by Bruce Schneier [86].

> "*Today's internet feudalism, however, is* ad hoc *and one-sided. We give companies our data and trust them with our security, but we receive very few assurances of protection in return, and those companies have very few restrictions on what they can do. This needs to change......it's time we step in our role as governments (both national and international) to create the regulatory environments that protect us vassals (and the lords as well). Otherwise, we really are just serfs.*" [86].

As such, there is a gap in exploring socio-technical insights and evolving a comprehensive *responsibilization* paradigm to counter extant *feudalism* in the space of data breaches. Here, we propose an alternative paradigm: ***Ethical Responsibilization***, to be situated at the policy layer. We use the term *ethical* to be cognizant of shared understanding of expected behavior which are not always codified in law. The paradigm evolves from the responses of our study and synergizes with the alternate formulation of justice articulated in Amartya Sen's Idea of Justice [87]. We detail the three core ingredients of this new paradigm as: *1) obligations of effective power, (2) capability and (3) comprehensive outcome.* These ingredients point to the pertinent ground realities that can continually inform regulatory frameworks. They are not necessarily mutually exclusive and, indeed, influence each other. The structure of the paper is shown in Figure 1.



New Paradigm	§2: From Feudal Security to Ethical Responsibilization	
Investigation	§3: Related Research	§4: Study
	§5: Findings: ***Where Does the Buck CURRENTLY Stop?***	§6: Findings: ***Where SHOULD the Buck Stop?***
Fleshing out New Paradigm	§7: Ethical Responsibilization Framework	

Figure 1: Paper Structure (with Section Numbers)

2 From Feudal Security to Ethical Responsibilization

An *Ethical Responsibilization* paradigm draws upon the alternate formulations of justice articulated by Sen [87]. We briefly summarise the prevailing and alternate paradigms of jurisprudence to ground our new paradigm proposal.

The prevailing model of jurisprudence in the West goes back to Hobbes [98] and is known as the contractarian model after Rousseau's social contract [29]. The contractarian model aims to build perfect institutions to govern society and mandates citizens to follow specific rules laid down by the institutions. The contractarian model discounts how societies evolve and incentives these rules place on people to abide by them.

Feudal security is akin to the contractarian model of justice; we define security policies, identify perfect institutions and protocols that would implement those policies. In the process, there is an expectation that all entities governed by the said institutions and will abide by the said policies and protocols. Security is as much technical as it is about perverse incentives, moral hazards, and liability dumping [3]. Like the contractarian model, *feudal security* does not take into account actual societies, their diverse dispositions and situations. Consequently, systems are not only hard to use, they fail to meet the legitimate needs of their users.

The alternative to the contractarian model is the *realisation* based paradigm found in the works of notable philosophers including Adam Smith [58], Jeremy Bentham [15] and and Amartya Sen [87]. The *realisation* based paradigm lays explicit emphasis on how societies evolve, consequences, agencies involved and processes used. This means departing from a presumption of ideal behaviour and taking into account how societies evolve and using that to redress manifest injustices. Prior security research has built upon the *realisation* paradigm to include social realities in secure systems engineering [33]. We depart from the contractarian model and propose to adopt a *realisation* based approach to jurisprudence to design a *ethical responsibilization* framework.

Why Ethical?

Sen, while articulating on human rights, establishes the importance of significant human rights which are yet to be or could not be coded into a coercive legal rule [87]. Yet, their moral imperative is widely recognized[3]. In our usage of the term *'ethical'* we ground the moral and participatory emphasis of the proposed paradigm. This means that due recognition to conventions that are yet to have a legal force or difficult to accommodate in the legislative route.

For example, many participants in our study emphasize the importance of empathy and comprehension of the human consequence (like shame) of breaches. The participatory element will foreground contextual realities in identifying who could have prevented a breach but failed to do so. This is a departure from the existing paradigm where powerful entities often wriggle out through gaps in the legislation. For example, a participatory deliberation to assign responsibility will ask *is GDPR enough to address misuse of data at a aggregate scale like the Cambridge Analytica scandal?.* In effect, the participatory element will identify the *winners and losers* of existing legal frameworks [92]. A related example is where Facebook's legal threat against NYU's ad observatory was argued to be *ethically wrong* [30]. The moral, as well hard legal *realisations*, can feed back into a *responsibilization* paradigm as practices or coded laws.

Operationalizing the Paradigm

The ingredients of our *ethical responsibilization* paradigm focus

[3] Recognizing the rights of women in family matters in sexist societies (pp 365) [87]

on identifying effective power (responsible entity), capabilities of each stakeholder and human consequences of data breaches. Such information can significantly help in post breach investigations and inform regulatory content and regime. Regulatory mandates have positively contributed to industry wide safety mechanisms [5] and equitable provisioning of public goods in general [38]. Moore, Clayton and Anderson highlight cyber security, too, is a *classic collective action problem* [65]. This means a coordination between private entities, law enforcement, regulators, and relevant stakeholders to combat Internet crimes. Our proposed paradigm can complement existing efforts by Cybersecurity & Infrastructure Security Agency (CISA) to evolve directives through a reasoned understanding of power asymmetry, capability, followed by an evaluation of their effectiveness. Research enterprises can engage with our paradigm to explore human centered realistic & effective breach management protocols.

3 Related Research

Cybersecurity measures taken by organisations are essentially risk management efforts. Approaches include [17]:

(1) **Accepting:** deciding that the risk is acceptable and that no measures need to be taken to reduce it. Acceptance would likely lead to massive fines (at least in the UK) if/when the organisation experiences a breach event.
(2) **Avoiding:** eliminating the source of risk or avoiding activities that involve risk. The risk of a data breach cannot be avoided by organisations in the 21st century, when businesses often have no choice but to go online, so this is not an option.
(3) **Mitigating:** allocating resources to mitigate the risk. This includes putting measures in place to reduce data breaches [54].
(4) **Transferring:** shifting the risk to another party, such as an insurance company that offers cyber insurance.

Mitigating and transferring are the only two viable options for modern-day organisations.

We commenced with a scoping review with the aim of understanding the state of play with respect to responses and responsibilization in data breach aftermaths.

Step 1 – Search
We searched Scopus, Google Scholar, IEEE Explorer, Consensus and ACM DL for all the papers with the keywords: Mitigating Risk:*responsibility and 'data breach'* and Transferring Risk: *'cyber insurance'* and *'data breach'*

Step 2 – Selection
We used the following inclusion and exclusion criteria to determine whether a paper was included or not.
Inclusion : Peer reviewed; discusses data breaches, responses, responsibility or has responsibilization as a topic.
Exclusion: Published before 2014; No access (not in the public domain).

Step 3 – Charting
To trace and understand the responses and responsibilization, we will review and record the following data items concerning each paper:

(1) Publication details (authors, year, title of the study, journal/venue name, DOI, and number of citations)
(2) The reported breach, causes and blast radius.
(a) Advocated responses to address data breaches, including how to assist those whose data was lost (staff/ customers/ clients).
(b) Plans to re-establish trust in staff/customers/clients.

Table 1: Specific Breach Examples (AWS=Amazon Web Services; ICO=Information Commissioner;FBI=Federal Bureau of Investigation)

	Equifax (2017)	**Capital One (2019)** [41]	**UBER (2016)**
Notification	Delayed [81]	Delayed [68]	Delayed [81]
3rd party used	No	AWS	AWS
Who blamed	Employees not patching [49]	Insecurities in the AWS metadata service	Third party UWS
Responsibilities pushed onto customers	Sign up for free credit monitoring [97]	Monitor own credit record; request a free copy of credit report annually[4] [21]	Free credit monitoring and identity theft protection [93]
Apology	CEO Richard Smith [18]	Bank's chief executive [41]	UBER boss [90]
Fine	Fined by ICO in UK [51]	USA banking regulator [103]	Fined by ICO in UK [13]
Customer Response	Raged online [69]	Class action suit [70]	Outrage [102]
Notable	Tried to remove consumers' ability to sue them as they registered for credit monitoring service [97]	Had another breach in 2023 [25]	Hacker paid against FBI advice [74]

Take Away Literature has documented the acts of omission or commission by entities involved in major breaches. Some organisations negatively exploited their positional advantage and their customers were not appropriately treated. Prior work also brings to the fore complex supply chains and abrupt re-engineering of internal business processes by organisations.

3.1 Mitigating Risk

3.1.1 *Power Asymmetry.*

Our scoping review highlighted the power and information asymmetry between service providers and their staff/customers. In many cases, the asymmetry influenced organisations' responses to data breach incidents. Kim *et al.* [55] analysed responses in data breach aftermaths and categorised them as (examples added by us):

(1) **Attacking the accuser** e.g., threatening to sue anyone who claims that a breach occurred[5];
(2) **Denial** e.g. Target[6];
(3) **Scapegoating** blaming employees instead of considering technical issues [47];
(4) **Excuse** i.e. minimising responsibility by claiming it was merely part of the operation of a typical organisation;
(5) **Justification** i.e. falsely claiming that damage was minor e.g., LastPass[7];
(6) **Ingratiation** [26] i.e. reminding second victims of past performance;
(7) **Compensation** i.e. Arnold Clark offered free identify protection and credit monitoring services to second victims[8]. The UK's National Health Service has paid compensation to second victims [1];
(8) **Regret** i.e. expressing remorse, e.g., Neiman Marcus: "*We deeply regret the data breach*"[9];
(9) **Apology** [16] e.g., Telstra[10].

Whatever actions the breached organisation takes, being willing to acknowledge customers' concerns, and being honest, is crucial [23]. Mohammed [64] enumerates four areas of recovery: (1) customer recovery, (2) employee recovery, (3) process recovery and (4) regulatory recovery, which suggests that the list given above needs to be extended.

Victim Self Blaming
Prior research investigating individual responses to data breaches highlights a culture of self blame by second victims [57]. They tend to blame themselves for not exercising caution during their online interactions.

Internal Governance
An investigation into 271 data breaches between 2004-2012 highlights the role of improved internal governance to prevent data breaches. This study finds that companies with better governance and social responsibility are less likely to suffer data breaches. Companies who improve on these counts after suffering a breach do better at mitigating future breaches. Better governance means a small board, less independent directors, realistic compensations with right spending. Social responsibility means care for environment and other causes [56]. The role of social responsibility and better governance in limiting the consequences of data breaches has been discussed by [10].

Prior work makes a strong case for improved data governance and a transparent regime for breach notifications. Dane [32] argues that even if companies allow third-party firms to store their customer data, they themselves are still liable if the data is breached. This could be termed as *outsourcing the work while 'in-sourcing' the liability.* While third party firms are responsible for notifying the companies they serve of a data breach, the data owner is liable for dealing with their customers. Frei [42] points out that online businesses bear full responsibility for the consequences of data breaches. For example, Masuch *et al.* [61] says that, in addition to providing information about the incident, information to customers should include recovery actions designed to reassure. Moreover, offering compensation can positively impact customer attitudes.

> **Take Away** A power asymmetry exists between organisations and customers, which contributes to self blame. Prior studies have shown the positive contribution of improved internal governance to prevent future data breaches.

3.1.2 *Regaining Trust.*

Companies that suffer data breaches invariably suffer financial losses in terms of pay out to victims or fines or legal fees or significant erosion in share prices [71]. A school in the USA paid damages and legal costs after sensitive information pertaining to a student was leaked [12]. Karyda [52] confirmed that breach notifications negatively impacted customer loyalty by reducing trust. Chen and Jai [23] interviewed loyalty program customers and found that their trust in organisation reduced after a data breach crisis.

Prior work identifies the importance of a cogent response strategy in containing the blast radius and costs post a data breach. The key ingredients of a response include identification of a incident management team, financial forecasting based on nature of the attack, communications, investigation of the technical nature of the attack [20]. A willingness to offer apologies is a potent tool to regain trust. A study with a hotel loyalty customers shows that the response strategies reflect hotels' willingness to acknowledge stakeholders' concerns. Apologies to customers and appropriate communications were considered effective response strategies [23]. Carre *et al.* [22] highlights that an apology is the best way to rebuild trust after a breach. In the context of healthcare, a study found that a combination of apology and compensation contributes positively towards addressing customer concerns [61].

A study explores the role of corporate social responsibility on rebuilding trust post a breach. They find that the initial level of trust in a website is not positively correlated to their endorsement of social causes. Consequently, websites endorsing social causes suffer equally in terms of loss of trust after a breach. However, the level of repaired trust subsequent to a breach and apology is higher for sites that endorse social causes [11]. Increasing awareness of data breaches among customers and employees can become an effective corporate social responsibility activity [96].

> **Take Away** Prior research suggests that breaches harm organisations. However, studies highlight the positive role of empathy and transparency in breach responses and extant social responsibility in re-establishing trust.

[5] https://www.washingtonpost.com/news/worldviews/wp/2018/01/08/an-indian-journalist-exposed-a-huge-breach-in-a-government-database-now-shes-facing-a-police-complaint/
[6] https://www.dailymail.co.uk/news/article-2529035/Target-warns-customers-aware-phishing-scams-hackers-steal-details-45-million-credit-cards.html
[7] https://www.cybersecuritydive.com/news/lastpass-cyberattack-timeline/643958/
[8] https://www.arnoldclark.com/newsroom/3718-arnold-clark-and-tracker-offers-customers-added-protection-against-keyless-car-theft
[9] https://www.washingtonpost.com/business/technology/neiman-marcus-we-deeply-regret-data-breach/2014/01/16/7bd54b30-7ee8-11e3-93c1-0e888170b723_story.html
[10] https://www.abc.net.au/news/2022-12-11/telstra-apologises-for-online-data-leak/101759006

3.1.3 *Service Providers' Duty of Care.*

While asymmetry is inescapable, prior deliberations have focused on the obligations of service providers in alleviating manifest insecurities. There are arguments for a regime where individuals can hold organisations accountable for breaches [12]. The term *fiduciary responsibility* has been discussed in the context for protecting pensions data and financial information in the USA and Australia, respectively. *Principles of responsible investments* convened by the United Nations Secretary general, describes *fiduciary responsibility* as:

> "*Fiduciary duty exists to ensure that those who manage other people's money act in the interests of beneficiaries, rather than serving their own interests*" [76].

The notion of *prudence* is consciousness of the processes and practices employed by organisations and not merely the outcome. While *prudence* might not always lead to the best outcome, it can provide a documentary evidence that processes were indeed followed. The introduction of a *reasonable* or *prudent* person helps to make an objective assessment of the actions of individuals and organisations. We argue that the demonstration of *prudence* might not be straightforward unless there is an accepted standard of *prudence.* The broad domain of jurisprudence has explored the role of *reasonable persons*; the normative and deontological elements of reasonable behaviour are diverse [87]. The question to ask is whether such diversities would be the case for security mechanisms where two *prudent* individuals might have diverse views of what are appropriate and commensurate security measures.

Prior research has also conceptually explored mechanisms to attribute actions to individuals through access control mechanisms. A responsibility model has been proposed by Kayes *et al.* [53] which codifies *who is responsible for what data, and for how long*. The context information is used to design an access control model to assign responsibilities in the event of a breach.

Take Away A regime of fiduciary responsibility has found acceptance but needs further unravelling of its elements such as clear steps satisfying duty of care. There are suggestions of a *detached reasonable person* to establish the notion of prudent behavior which is independent of the outcome.

Table 2: Aspects Covered by Cyber Insurance Basic Policy for Incident Response (Info from their own Websites). Numbers refer to insurance offerings in Table 5.

	1	2	3	4	5	6	7	8	9	10
Immediate Recovery from Data Breach										
Investigating the cybercrime	•		•	•	•					•
Recovering data lost in a security breach	•	•	•	•					•	•
Helping to restore computer systems	•	•					•	•		
Legal experts to advise on GDPR, data breaches and next steps		•			•		•			•
Funding to cover business interruption and recovery costs	•		•	•		•	•	•		•
Complying with regulatory proceedings, fines, and penalties						•				•
Fallout										
Extortion payments demanded by hackers	•		•			•			•	•
Third-party claims for financial loss			•	•		•	•			
Public Relations										
Reputation management	•	•	•	•	•		•	•	•	•
For benefit of third party whose data was breached										
Notification costs, in the case you are required to notify third parties affected	•		•		•	•			•	•
Funding of Identity Theft and/or Credit Monitoring Services			•	•	•			•		•

3.2 Transferring Risk

Here, we consider businesses adding cyber insurance to their other insurance provisions. It is instructive to consider what they consider the organisation's responsibility to be in the aftermath of a data breach. We referred to the websites of prominent cyber insurance providers as indicated in Table 5 in the Appendix to provide a snapshot of coverage by cyber insurance companies in Table 2.

The relationship between insured and insurers assumes that of a binding relationship. Insurance companies share appropriate expertise to implement processes, absorb many risks and actively participate in post-breach legal and other recovery processes [95]. Prior research investigated the risk-assessment processes of insurance companies through in-depth analysis of their policies, declared inclusions and exclusions. They highlight the role of various data points, such as organisational governance, technical measures employed by organisations, hiring policies and compliance mechanisms in assessing risk [84].

Some risks have led to hardening of the insurance industry. Mott *et al.* [66] interviewed 96 professionals spanning cyber insurance, cyber security, ransomware negotiations, law enforcement and report that ransomware incidents led to a hardening at all levels of the cyber insurance market. This hardening of the insurance industry raises the acceptable standards of cyber security for firms to be able to purchase cyber insurance but, at the same time, prevents many from availing cyber insurance [66]. Consequently, poorer firms are left without the access to expertise that they probably need [95]. This exclusion raises an important debate as to the effectiveness of insurance companies being *de-facto* arbitrators of security practices. Martinez *et al.* [60] highlighted barriers faced by firms wanting insurance and found that they include a lack of a common language across the industry and appropriate policy coverage for specific companies. The lack of standardization was also highlighted as a key challenge by [8, 73].

Insurance companies face an asymmetry of information which negatively affects actuarial services. A notable systematization effort reconstructed 10 well-known data breaches and showed that information pertaining to many breaches was incomplete [85]. A related systematization effort highlighted key research challenges surrounding risk measurement, automated data collection and catastrophe modelling [31]. Avanzi *et al.* [7] investigated the USA state attorneys general's publications of data breaches show a persistent delay in reporting data breaches and inconsistent reporting. Lack of data negatively affects risk assessment efforts, cyber insurance pricing, underwriting and actuarial services. The difficulty to reconstruct attacks and breaches was also reported in [72, 73]. The diversity of cyber attacks makes it difficult to calculate financial impact. Poyraz *et al.* [75] propose a distinction between personally-identifiable information and non personally-identifiable information to enable more informed estimation of financial impact. Wheatley *et al.* [101] proposed considering data breaches within the *catastrophe framework* for improved insights for cyber insurance and overall risk assessment. Related work also argued for a bureau for cyber statistics and for governments to underwrite cyber risks [45].

Take Away A general hardening of the industry coupled with information asymmetry further exacerbates the gap between companies with access to insurance and expertise and those without. We further explore the uptake of cyber insurance and consider the potential impact on data breaches in our study.

3.3 Research Questions

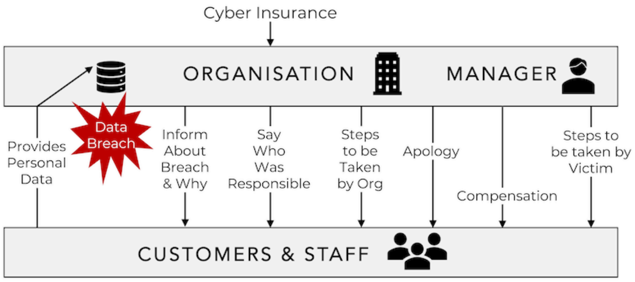


Figure 2: Aspects of Data Breach to be Studied

The key considerations that came out of the scoping survey are depicted in Figure 2. Based on this analysis of the current state of responsibilization practices in the industry, we suggest the following research questions:

RQ1: What is the extant state of organisational data breach responses (see Figure 2)? In particular:

(a) what realities are experienced by actual *victims* of data breaches?
(b) what are the expectations of *non-victims* should they become a second victim?
(c) what are the perceptions of *managers*: (1) with respect to organisations that experienced data breaches, what they did, and (2) for all managers, what they think *should* happen if a breach occurs.

RQ2: What does an ideal responsibilization regime look like?

(i) Who should be responsible?
(ii) How should stakeholders respond?
(iii) Who is liable to take actionable steps and what are the steps?

4 Study

4.1 Methodology

Design:
To explore the situation, we decided to survey citizens of the USA and the UK. An alternative would be to conduct interviews but given the sensitivity of the topic (personal data being leaked), it seemed wiser to elicit responses using a mechanism that guaranteed anonymity. The questions are a combination of those that can be quantitatively analysed and open text responses that can be qualitatively analysed. Examples of the former are: "*Have you fallen victim to a data breach due to some organisation suffering a breach where your personal information was leaked?*". Examples of the latter are: "*How did you learn of the breach?*". Finally, we posed some questions using a Likert Scale. For example, to non-victims, asking for agreement: "*I would want them to tell me who they think was responsible for the breach.*".

Table 3 maps the two research questions to the survey questions provided in the Appendix.

Table 3: Survey Questions mapped to Research Questions

RQ	Survey Questions
RQ1(a)	V1, V2, V3
RQ1(b)	NV1, NV2, NV3
RQ1(c)	M1, M2, M3, M4, M5
RQ2	NV1-3, V(n), M4(j,k) and M5(a-m)

Survey Design:
To explore the research questions, we posed survey questions to explore: (1) Did they fall victim to a breach of their personal data held by another entity? (1a) If so, ask questions about what happened in the aftermath. (1b) If not, what would they expect to happen if their data were breached? For those respondents who were managers (self reported via question D3), we explored their experiences when they had to deal with a data breach in their organisation or, if they hadn't experienced a breach, we asked about what they thought should be done if their organisation experienced a data breach.

Survey Piloting:
We asked two individuals to pilot the survey and then checked Qualtrics for the amount of time it took. We asked them to give us feedback about the clarity of the questions; one provided

suggestions for improvement.

Analysis:
We used a collaborative platform Miro [63] to support analysis of the data. We used Braun and Clarke's [19] staged thematic analysis: (1) data familiarisation; (2) initial code development; (3) thematic search; (4) review; and (5) defining and naming themes. Longer sentences such as: *They should, most of all, apologize for what happened and, depending on the type of breach, offer compensation or something* were coded into first order themes as *empathy and compensation* and aggregate dimensions as *comprehensive outcome* and *obligations of effective power* respectively.

Codes were discussed and agreed upon in an iterative process between the authors. Following reading and re-reading, we grouped first-order codes into first order themes [19], which were again grouped into aggregate dimensions to support answering of the research questions. The final codes are available via this link[11].

We also carried out a descriptive analysis of responses where Yes/No responses were selected. The results can be seen in Figures 4, 5, 6 and 7. Figure 8 depicts the contrast between expectation and reality (from second victims).

Ethics:
We applied for and gained institutional and research center ethics approval. We did not ask for, or record, any information that is sensitive or could identify the participants. Survey responses are stored on our institution's secure data servers.

4.2 Recruiting

We first sent out invites through the national slack channel of the research center, social media accounts and personal connections. We then used the Prolific platform to gain more respondents from the USA and the UK. Prolific workers were paid £12 per hour for a 10 minute survey, which exceeds the UK's living wage. Demographics are shown in Table 4. We indicate the age and gender to convey the diversity of our participants. These were not used to support analyse in this study.

Table 4: Participant Demographics

Gender			Age Range (1 Withheld)				
Male	Female	Withheld/ Other	18-29	30-39	40-49	50-59	≥60
88	79	6	33	57	37	27	18

4.3 Threats to Validity

Internal: Participants were recruited from the Prolific platform. This means, on the one hand, that they are accustomed to working with technology, and probably better informed than others. Moreover, they, too, could become second victims.

The survey study included questions that allowed individuals to respond in free text. This was to encourage them to provide comprehensive responses. Face-to-face conversations would undeniably elicit more in-depth information and allow the posing of follow-up questions.

External: We had 175 participants in total. However, we did not force responses: some questions were specific to victims, some to non-victims and some to managers. In some cases, participants responded *'as mentioned earlier'*, instead of repeating prior comments. From now on, we explicitly mention relevant questions and explain how many responses were received in support of a particular theme.

Please see Appendix A for adherence to SIGSOFT guidelines.

5 Findings: RQ1 - Where Does the Buck Stop?

Of the 175 participants, 131 had fallen victim to a data breach where their information had been held by a third party. The first order and aggregate themes are shown in Figure 3. We discuss the themes below. The questions we refer to can all be found in the Appendix. We discuss responses in the light of *communication, organisation behaviour* and *actions taken by victims*, which were the aggregate dimensions that emerged m the data.

5.1 Communication

[Questions V1, V2, V3(a), V4(a-c), V3(b).]

Figure 4 shows how organisations communicated with participants, and how they first came to hear about breach. We asked participants if they were informed by their service provider, and, if so, whether this occurred immediately or after a delay. Figure 4a shows that 50 participants said there was a delay and 45 were promptly informed. Thirty two participants were not informed by the service provider and none did not want to be informed.

While these choice based answers in Figure 4a captured whether they received intimation from the breached organisation, we qualitatively analysed their textual responses against questions V1 and V3(b) to find out how they initially found out about the breach. The results are captured in Figure 4b.

67/131 respondents found out independently whereas 59/131 were informed by the service provider with 21 of them experiencing a delay. The delay stretched even for months before the organisation informed victims in some cases —

> *I found out through online news before the company told us. For months before it came out via the news I would enquire, I was only ever told from many higher up staff that 'an attempt was made but nothing was taken'* (P2).

We gleaned the methods and sources that informed participants of the breaches.

Ten participants reported pro-actively using services such as https://haveibeenpwned.com — "*The breach was only made known to me because I have subscribed to 'haveibeenpwned.com' and it was months after the breach had occured!*" (P145). Clearly, this participant was not informed by the service provider he/she trusted with their data. Two participants said that they would have preferred to find out sooner than they did.

Participants mentioned the role of platforms in making them aware of data breaches. 10 participants learnt of the breaches from Google password manager, or through Apple notifications.

[11] https://osf.io/kbwj2/?view_only=8713f8eb86514f\1d9e6fba9fe78756a6

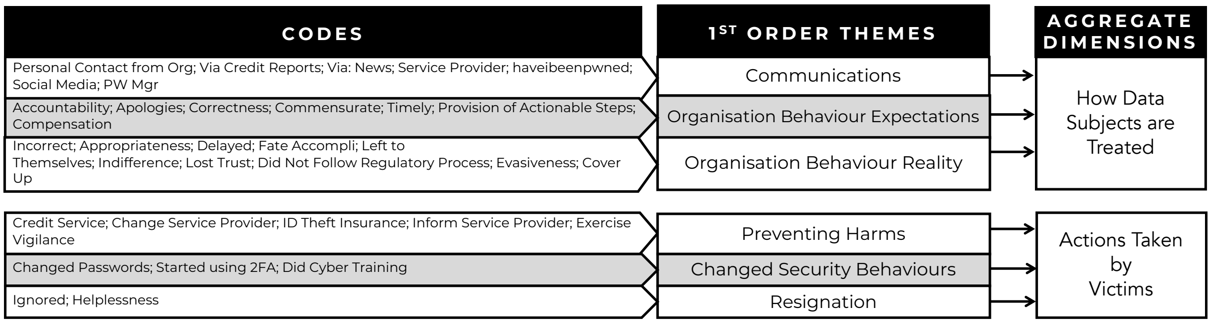
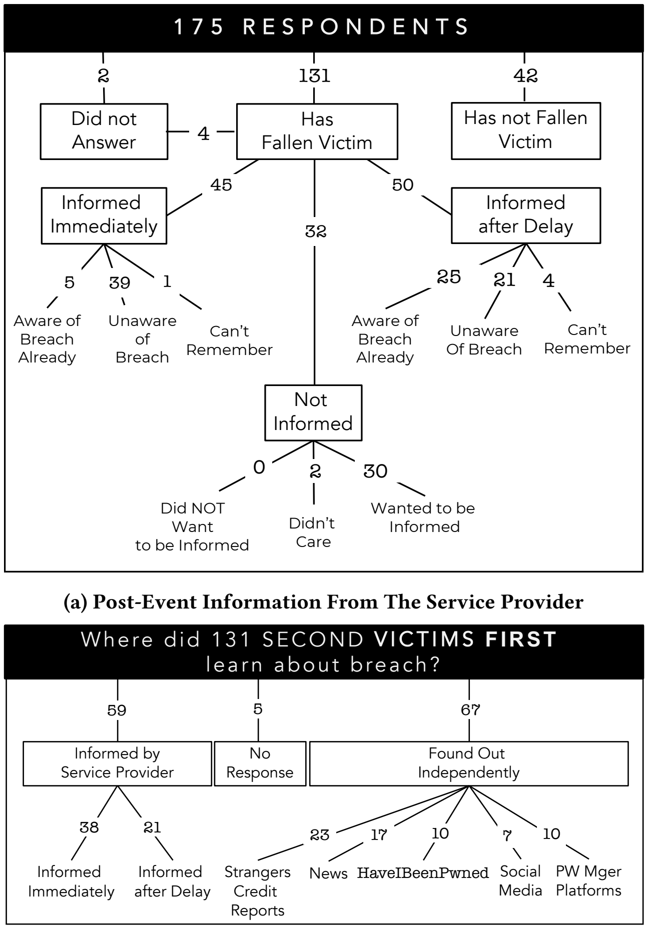

CODES
1ST ORDER THEMES
AGGREGATE DIMENSIONS
Personal Contact from Org; Via Credit Reports; Via: News; Service Provider; haveibeenpwned; Social Media; PW Mgr
Communications
Accountability; Apologies; Correctness; Commensurate; Timely; Provision of Actionable Steps; Compensation
Organisation Behaviour Expectations
Incorrect; Appropriateness; Delayed; Fate Accompli; Left to Themselves; Indifference; Lost Trust; Did Not Follow Regulatory Process; Evasiveness; Cover Up
Organisation Behaviour Reality
How Data Subjects are Treated
Credit Service; Change Service Provider; ID Theft Insurance; Inform Service Provider; Exercise Vigilance
Preventing Harms
Changed Passwords; Started using 2FA; Did Cyber Training
Changed Security Behaviours
Ignored; Helplessness
Resignation
Actions Taken by Victims

Figure 3: Codes, Themes and Aggregate Dimensions



(a) Post-Event Information From The Service Provider

(b) First Becoming Aware of the Breach

Figure 4: Breach Communication

Social media was also mentioned by 7 participants — "*On facebook when the person the information was leaked to went public due to non appropriate responses from the GP surgery*" (P32). Four participants in this group said that they read about it after a delay.

Seventeen participants mentioned that they first found out through news reports and 7 felt that was quite late. "*It was found through general news articles on the BBC*" (P110).

Twenty three participants found about the breaches through means other than those mentioned above. For example, strangers informed victims without any communication from the responsible entity — "*A letter with my personal information and details had been sent to the wrong address instead of mine, and the recipient found me on social media to contact me to say that they had received it*" (P37). In this category participants reported getting suspicious due to unusual text messages, fraudulent activity on their online shopping accounts and only then finding about the breach. Participants also reported proactively monitoring their credit reports.

Take Away Many participants found out about breaches to their personal data by themselves. Participants reported significant delays or even absence of any communication from service providers who had experienced the data breach.

5.2 Organisational Behaviours

[Questions V3(c) - V3(k)]
We asked participants if they were contacted by the organisations that collected and stored their data. If so, did the communication include:

- intimation of any third party involvement.
- compensation being offered.
- an apology being extended.
- reasons for the breach being explained.
- information on steps being taken by the organisation to resolve the damage and prevent future occurrences.
- steps victims themselves should take.

The choice-based responses are captured in Figure 5. The key takeaways are that apologies and compensation were rarely offered, and reasons behind the breach were seldom communicated. So far as third party involvement, the majority of organisations did not mention any third party involvement. (They might not use a third party service to store their customer/staff data as USS did). The majority did outline the steps they were taking and expected their customers to take.

We further sought textual responses on their expectations from these organisations with respect to the breaches they experienced

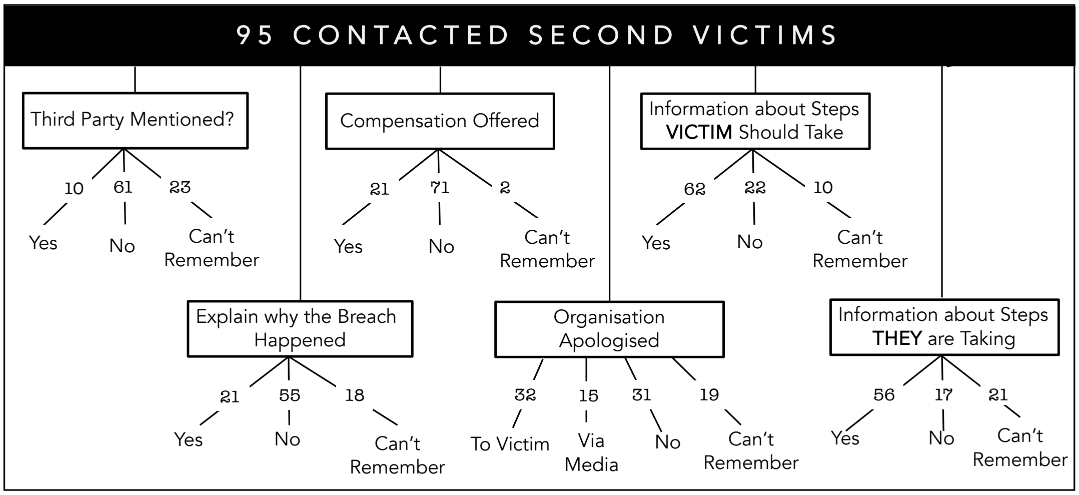


Figure 5: Post-Event Information and Interactions

and their experience of organisational behaviour. The responses were qualitatively analyzed.

Twenty nine participants were happy with the responses from their service providers. "*These things happen and they did their best to contain any issues arising*" (P87). Four said that they were happy with the overall response from their service provider but flagged delay and communications as being below their expectations. "*It was adequate although communications could have been better*" (P85).

Thirteen participants thought that organisations should be *accountable* and extend an *apology* in every instance of a breach. "*It just felt like 'brushing it under the rug', I wanted more accountability or explanation.*" (P53) "*been more genuine in apology*" (102).

Fifteen participants said that the organisations were *indifferent* to the human consequences of data breaches. "*I felt it was careless and they lacked concern. Nothing about it was prompt or transparent so I felt uncared for*" (P133).

Twenty one participants expected correct and adequate information from the service providers they had shared their data with. "*There was almost no communication whatsoever. I would have liked to have been supplied with information about the breach and been kept updated as time went on*" (P45).

Sixteen participants thought the their service providers were *evasive*: there were attempts to cover up the breach.

> *I thought it made them look more guilty because of how cagy and secretive they were with information. My trust was not restored since I had no information about what, if anything, they were doing about the breach and future cybersecurity* (P82).

Sixty two participants mentioned that they expected to hear about *commensurate steps* that are being taken by organisations. Responses also included steps that can be taken by individuals to protect themselves from future breaches. "*To prevent it? Or after the breach? I don't remember. They confidently implied that they had everything under control*" (P119).

While *delay* was an overwhelming experience in the context of communication after the breach, 34 participants mentioned it in the context of their expectations from organisations they share their data with. "*They could have contacted me sooner. They said it was as soon as they had found out, but it later transpired that this was actually over a week after knowing about the breach*" (P152).

Compensation against loss of data was raised by 35 participants in response to a choice-based question (V3e). Thirteen participants mentioned compensation in their textual responses:

> *Pay for a year's worth of identity protection, or something along those lines as other organisations have done in past data breaches, particularly since in this particular case, I did not have access or any real control over the data retained by the organisation* (P46).

Nine participants expressed a sense of *resignation* as insecurities are inevitable on the Internet. Eight participants said the service providers had left them to navigate out of the crises by themselves. "*I felt like they didn't care because they didn't inform me of it, I had to find out another way by trying to sign up to another website*" (P34).

Twenty one participants said they *lost trust* on the organisations they trusted with their data due to their subsequent responses. "*I lost trust in them and couldn't expect them to treat my personal information with the correct level of care*" (P98).

Take Away Participants stated their expectations of accountability, apology and actionable steps for assurance. Majority of the participants we studied were given incorrect information, not adequately supported or compensated and found the responses to be indifferent to the human cost of the breach.

5.3 What Actions Victims Took

[Questions V3(l-m)]
In response to the choice based question *Did you yourself take any steps once you learnt about the breach?*, 96 said they did, 24 did not, and 5 couldn't remember. This was further backed with textual responses on the steps victims took post-breach incidents. We qualitatively analyzed the responses and they show a range of shared

understanding among users with respect to managing their security. The categories of security tasks below are not mutually exclusive with some participants mentioning multiple security tasks.

Sixty nine participants stated they *changed their passwords* and this has been the overwhelming step taken. "*I changed my passwords on important sites, I changed all passwords where I used the same one that had been leaked*" (P36). Two mentioned using password manager, one for checking breaches and another for changing their passwords. "*Changed all my passwords to unique ones using a password manager*" (P146). Two participants reported that they tried to secure their passwords and yet they fear they will not prevent future breaches. "*I tried to change my passwords of my bank accounts and social media accounts. nothing else could be done about this I think*" (P76).

Eleven participants enrolled for *credit monitoring services* and one froze their credit report [P99]. P2 enrolled for Experian credit checker and transferred their salary account to another branch. "*Experian credit checker. Created another bank account to move my salary pay into that account so my jeopardised bank account can only have so much money stolen*" (P2). One participant indicated that the service was paid by their employer. Multiple participants subscribed to credit monitoring services.

Fourteen participants changed their service provider or unsubscribed from the services where the data breach happened.

> *First thing first, I changed my password for the account and deleted all my linked card details. I also cancelled the cards which were linked to my bank to avoid any bank account scams. I deleted all the addresses linked and never used that account to be on the safe side* (P121).

Identity theft insurance was used by 3 participants; One participant mentioned that their organisation provided the service along with *cybersecurity training* while 2 said they themselves had paid for the service. "*I updated my passwords, registered for the identity theft insurance provided by my organisation, completed the newest cybersecurity training offered by my organisation*" (P15).

Five participants said that they opted for *multifactor authentication/biometrics.* "*The bank had to issue a new credit card and the old one was cancelled. Also password reset. I also started adding two step verification to anything I could*" (P91).

Four participants resorted to *formal complaints* and sought explanations, with one threatening to follow up with the information commissioner's office (ICO). "*I put in a complaint with the organisation, stating that I would take it to the ICO if I didn't receive a satisfactory explanation of exactly what happened and how they will prevent this happening again*" (P152).

One participant put in a GDPR request with the business to delete all the data it held on him. "*I also made a GDPR request with the business to delete all data it holds on me*" (P162).

One participant reported *a sense of resignation* arising from an unresponsive service provider — "*I contacted them directly. Which was almost wasted effort. I even got into contact with other people about it who did take it seriously to begin with, but again, nothing happened in the end*" (P54).

Our qualitative analysis of the responses showed a *change in security behaviour* from 22 participants. The participants expressed exercised vigilance to online communications and a generally heightened level of alertness. "*Kept a closer eye on banking transactions also for unusual activity, including putting additional notifications in place to get real time activity reports*" (P31). A significant finding from our study is that end users are not passive and that they are indeed stepping up to protect themselves where possible.

Take Away Changed password are the most likely response by second victims. It is interesting to note the self-blame here. The breach did not occur because of the customer's behaviour but they automatically blamed their own passwords. Very few respondents mentioned using credit reference agencies and cyber security training was mentioned by only one participant.

5.4 Manager Perceptions and Practices

[Questions M1, M2, M3, M4(a-i), M5(a-m)]
Seventy five participants were in a managerial role in their respective organisations. The responses from managers are captured in Figure 6 as:

(1) fourteen organisations suffered a breach, with their responses shown in the lefthand box.
(2) the responses on *ideal* breach management are shown in Figure 6 in the righthand box.

We discuss the responses from managers in a breach situation while in their respective organisations. Responses regarding ideal breach management are discussed while outlining the new paradigm in Section 7.

In choice-based questions, we asked mangers if they or third parties offered compensation for the breaches. Nine participants said their organisations did not offer any compensation, while 2 did.

Nine of fourteen managers said that their organisations apologized to the second victims, while 2 participants were unaware and 3 said their organisations did not apologise. One manager said they received effective support from the insurance company when they had a breach. 10 did not share the results of investigations with their customers while 3 did. 1 did not answer this question.

11 managers said that their organisations outlined the steps they were taking while 2 did not. Six participants said that their organisations laid out the steps their customers should take to protect themselves from data breaches. Four managers expected their customers to follow at least some of these steps.

We further qualitatively analysed their textual answers to questions M4(c,d and j) and the responses are as below.

Response. Ten of the 14 managers were unaware of how their organisations interacted with the victims. Two participants highlighted instances where they were asked to downplay the incident or provide a 'vague' response to victims. "*There was a very vague email written in the form of an apology, month after the breach happened*" (P45). "*I was made to down play the extent of the breach by my superiors while little was done by way or preventing the issue in future besides the ingenuity i used to deescalate the threat*" (P60).

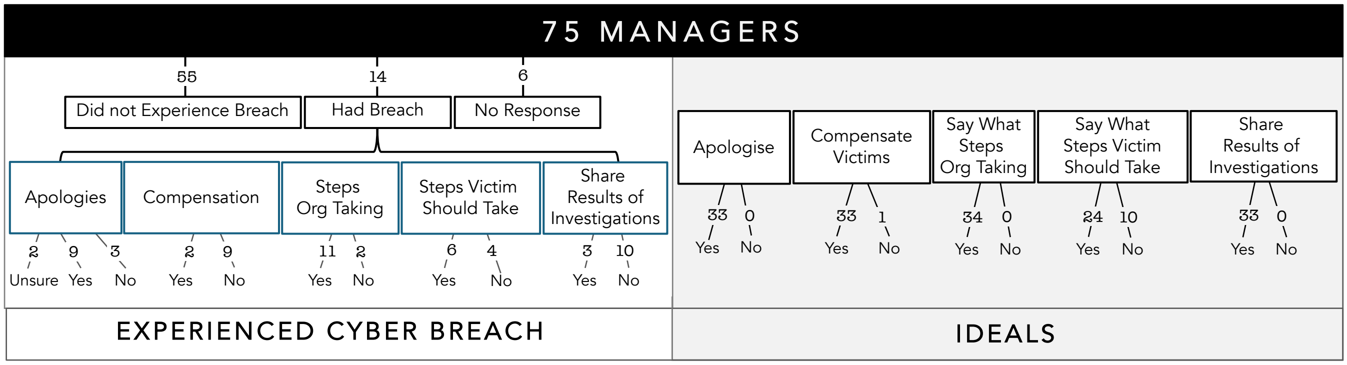


Figure 6: Manager Experiences and Expectations

Two participants said they either referred to their IT manager or they have a organisational process.

Transparency. We asked participants if their organisations explicitly declare the use of third parties to their customers. Seven participants answered this question and the responses show a mix of transparency and opacity. Four participants said their organisations informed their customers — "*Yes, we would reveal this to all customers and staff after the breach*" (P55). Two participants in this group said that they referred their customers to third parties post-breach incident. Three participants did not inform of the involvement of third parties — "*No, we try to avoid that even though we expected staff/customers to have read policy statements which in reality we knew that they didn't*" (P60). One in this latter group said for a particular breach it was not revealed but he was not aware of the general policy in his organisation.

Responsibility. Twelve participants clearly stated that organisations (including first party and third parties) should be liable for data breaches and one participant thought that data owners should be responsible. Six of the 12 participants who thought organisations were liable, however, considers that customers also had a role in preventing data breaches. These participants further detailed the steps they thought customers should take. The steps ranged from *secure devices, general alertness to availing credit reference agencies.* A pair of representative quotes from the group that said organisations should shoulder responsibilities, but also thought customers have a role to play, is — "*The executive board members of the organisation*" (P85). With respect to end users' responsibilities, the same participant said: "*To be vigilant and aware of phishing emails and suspicious links, to regularly change their passwords and be aware of keeping data secure*" (P85). In the textual responses, 2 participants saw the role of everyone in managing data breaches.

Take Away Managers reveal that compensation is not the norm, while apology was more prevalent. Organisations were not transparent about the use of third parties and cover ups were revealed. The majority of the participants said organisations did not share the outcomes of investigations. Many thought organisations should be responsible but that customers, too, should share responsibility.

5.5 Cyber Insurance

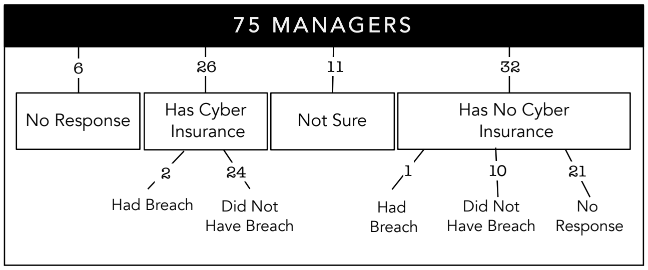


Figure 7: Cyber Insurance Uptake

[Questions M1 and M4(b)]
Figure 7 captures the responses of managers related to their organisations' cyber insurance. 26 organisations were insured against adverse cyber events. Only 2 of the 24 insured suffered breaches. One participant commented on the helpfulness of cyber insurance in managing the aftermath of a breach. "*They were quite helpful, they were available when we needed them and offered support for the future*" (P53).

32 managers said that their organisations did not have insurance against adverse cyber events. Only one of these admitted to their organisation having been breached. We did not receive responses from the other 21 participants in this group.

Take Away Cyber insurance uptake is not yet universally obtained, which is strange given the prevalence of data breaches. There is not much difference in breaches between the insured and the uninsured. However, this is not a large sample so it is hard to draw definitive conclusions.

5.6 In Summary

We can now return to RQ1:

RQ1a: Breach communication was generally unsatisfactory and deficient. Almost as many participants found about breaches through their own efforts as directly from the breached organisations. A significant number of participants experienced delays in

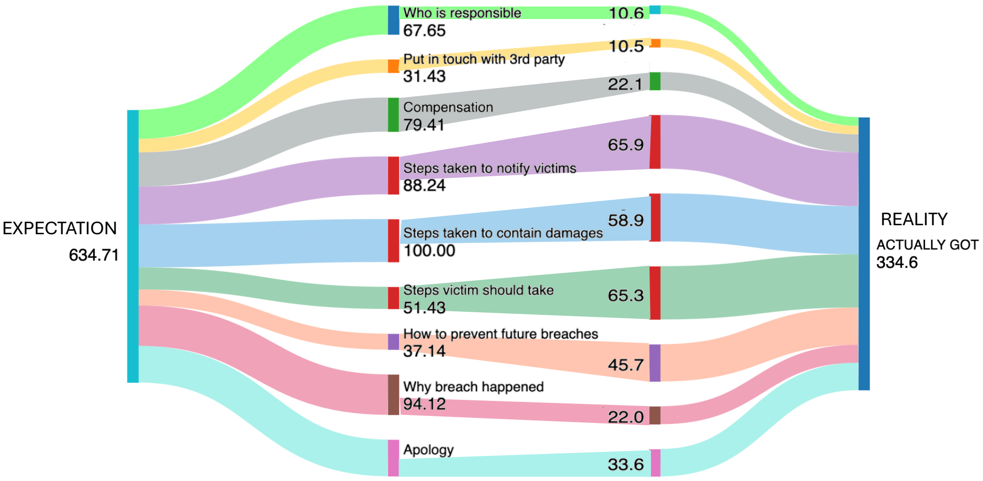


Figure 8: What Non-Victims Want vs. What Actual Victims Received (Numbers in the middle are Percentages)

receiving breach communications. Compensation and apologies were seldom proffered.

RQ1b: Respondents highlighted their need for empathy, transparency and truth in organisational communications to victims. There was overwhelming consensus on the fact that the responsibility should lie with the service provider rather than with customer/staff member 'second s'.

RQ1c: Managers' responses confirm that compensation is not the norm, nor are apologies, although more apologies were offered than was compensation. Moreover, some organisations were not transparent with respect to using third parties for data storage. Cyber Insurance uptake is not widespread. Managers largely agreed that responsibility lie with the organisations but users too should participate to control data breaches.

6 Findings: RQ2 - Where Should the Buck Stop?

While some data breaches leak both customer and staff data, we will refer to all as 'customers' in this section. We draw on responses to questions NV1-3 and V1-3 in Appendix B to construct Figure 8. It depicts the stark disconnect between what second victims expect and what organisations actually deliver when it comes to managing the aftermath of a data breach. This confirms the responsibilization of these customers members by organisations, where it's deployment is usually a governmental strategy. Moreover, its use in the data breach context is a clear dereliction of duty and a renunciation of organisational responsibility for something that becomes their legal remit once they receive the person's data. This situation cannot be sustained or excused with the increase in data breaches creating vast numbers of second victims across the globe.

To answer RQ2, we elicited responses from participants about their idea of an ideal responsibilization regime. This includes responses to NV1-3, V(n), M4(j,k) and M5(a-m) in Appendix B to draw out the themes in this section and Section 7. The key propositions that emerged are:

- **Responsibility.** Service providers are in a better position to address data breaches as compared to end users and the responsibility lies with them. Even if there are third party contractual arrangements with service providers, yet the responsibility lies with the first party service provider facing the end user. It is pertinent to mention that insurance and other contractual arrangements to manage risks and aftermaths are examples of transferring responsibility by organisations. We discuss the cyber insurance state of play in Section 3.2 & responses from managers in Section 5.5.
- **User participation.** There was a tie in the responses specific to the questions on whether users should take steps to protect themselves from breaches; while an overwhelming majority said that organisations should ask users to take security steps to protect themselves. We know from the responses of second victims the steps they took.
- **Communication and Assurance.** Participants said that data breaches have human consequences and post breach responses should demonstrate empathy. Furthermore, participants underscored the importance of a transparent process whereby they are assured by the effectiveness of technical measures to protect their data.

In answer to **RQ2**, we conclude that second victims want organisations to accept responsibility if they caused data breaches and cease responsibilizing victims. They are clear about the responses they want to see organisations engaging in (Figure 8 and don't want all the onus to be on them to mitigate the consequences of organisational data breaches.

The next section lays out our proposal for an **Ethical Responsibilization Paradigm** which will change the current state of play for the better.

7 Ethical Responsibilization

[Questions V3(n), V4, NV(1,2, and 3), M4(j,k) and M5(a-m)]
The insights from this study advocate evolving a *responsibilization*

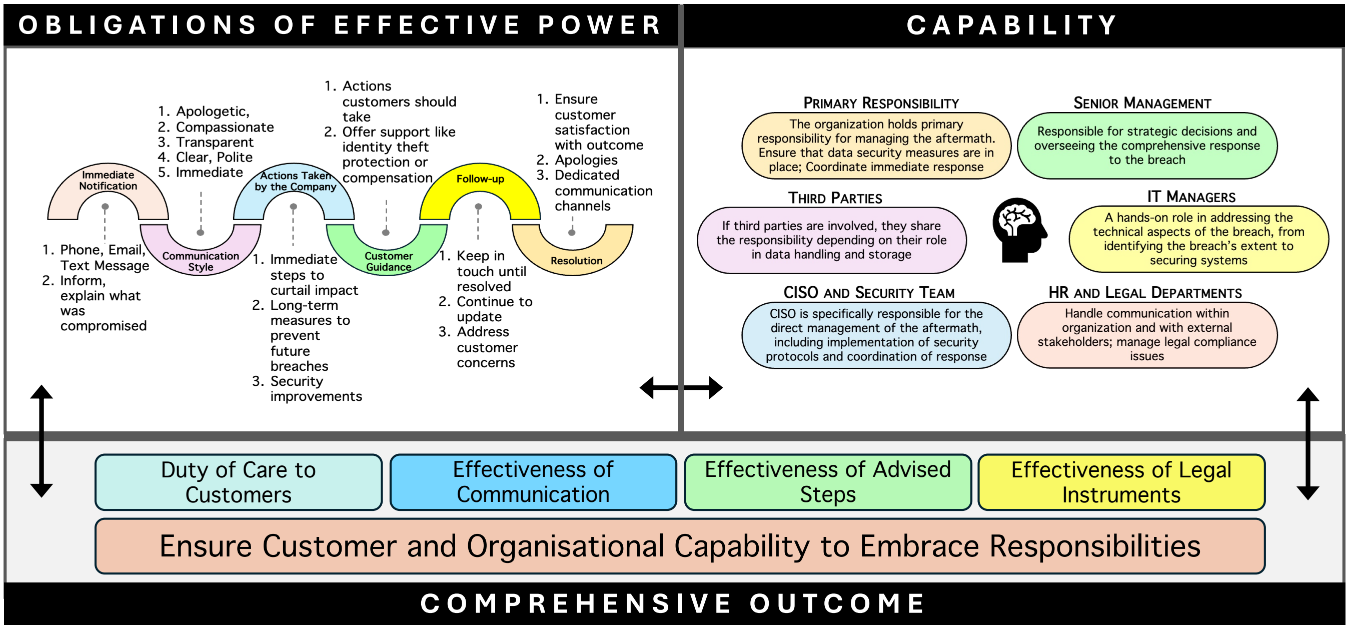

OBLIGATIONS OF EFFECTIVE POWER
CAPABILITY
Immediate Notification
1. Phone, Email, Text Message
2. Inform, explain what was compromised
Communication Style
1. Apologetic,
2. Compassionate
3. Transparent
4. Clear, Polite
5. Immediate
Actions Taken by the Company
1. Immediate steps to curtail impact
2. Long-term measures to prevent future breaches
3. Security improvements
Customer Guidance
1. Actions customers should take
2. Offer support like identity theft protection or compensation
Follow-up
1. Keep in touch until resolved
2. Continue to update
3. Address customer concerns
Resolution
1. Ensure customer satisfaction with outcome
2. Apologies
3. Dedicated communication channels
PRIMARY RESPONSIBILITY
The organization holds primary responsibility for managing the aftermath. Ensure that data security measures are in place; Coordinate immediate response
SENIOR MANAGEMENT
Responsible for strategic decisions and overseeing the comprehensive response to the breach
THIRD PARTIES
If third parties are involved, they share the responsibility depending on their role in data handling and storage
IT MANAGERS
A hands-on role in addressing the technical aspects of the breach, from identifying the breach’s extent to securing systems
CISO AND SECURITY TEAM
CISO is specifically responsible for the direct management of the aftermath, including implementation of security protocols and coordination of response
HR AND LEGAL DEPARTMENTS
Handle communication within organization and with external stakeholders; manage legal compliance issues
Duty of Care to Customers
Effectiveness of Communication
Effectiveness of Advised Steps
Effectiveness of Legal Instruments
Ensure Customer and Organisational Capability to Embrace Responsibilities
COMPREHENSIVE OUTCOME

Figure 9: Ethical Responsibilization Framework

paradigm that focuses on ground realities such as power asymmetry, market realities, human consequences and ability of users to participate to control data breaches. Social and political arrangements that build upon realities on the ground have their roots in the *realisation* based paradigm of jurisprudence. Motivated by this resonance we coded participant responses into top level themes as *obligations of effective power, capability and comprehensive outcome* by drawing upon Amartya Sen’s *Idea of Justice* [87]. The overarching themes and their containing sub themes are shown in Figure 9. We ground the overarching themes drawing upon their description in [87], pertinent study responses and specify how they can contribute to existing regulatory frameworks.

7.1 Obligations of Effective Power

Sen discusses the *obligations of effective power* to remedy instances of manifest injustices. Effective power essentially means the entity which is more powerful in particular situations is responsible to address instances of manifest injustices. However, identification of *effective power* in a *realisation* based paradigm of jurisprudence should be contextual and continuous.

We asked participants to elicit their understanding of the entity responsible for data breaches. Majority of our participants highlighted gaps in the current *responsibilization* regime; there exists a power/informational asymmetry between end users and service providers and the latter has a positional advantage to address breaches in a complete way. Figure 9 show that terms like *honesty, transparency, apology, timeliness, compensation* found more mentions along with others.

We received 56 responses from 75 managers. The bottom half of the diagram in Figure 6 reveals choice-based answers. We qualitatively analysed the textual responses. 54 participants answered that organisations should be responsible for managing the aftermath of breaches. Participants think that organisations are in a better position to manage their supply chains and risks arising of a complex supply chain. “*Behind closed doors, the third party, but to the customer, it has to be the organisation they entered into the relationship with, not their third parties. It’s not on the customer to understand a companies supply chain*” (P3).

56 managers responded ‘yes’ when asked if organisations should explicitly inform customers if their data was breached by a third party. The reasons varied as *transparency, consent and to enable customers to take remedial actions.* “*100% yes....we should be made aware and a concurrence sought*” (P12). However, 35 of 56 respondents said ‘no’ when asked if customers should be referred to third parties in the event of a breach.

76 victims were not managers and and we received 71 responses from them with respect to their expectations and reality having suffered a breach. This group highlighted accountability as “It just felt like ’brushing it under the rug’, I wanted more accountability or explanation” (P53).

The responses from 37/43 non-victims to choice-based questions (Appendix B) is plotted in Figure 8. There is emphasis on *compensation, transparency* and identification of *effective power.* The distance between expectation and reality have been discussed in the literature and also figured in the responses of our study. The elements of perverse incentives, profit maximisation and opacity figured both in the literature and in the responses from our participants.

The pertinent question here is whether or not existing regulatory frameworks engage with continuous evaluation of realities as they evolve. A *realisation*-based paradigm means continuous and careful understanding of markets, complex supply chain and using that to identify effective powers and lay down their obligations. The UK competition markets authority (CMA) effectively classified Google and Apple as duopolies with a *vice like grip* on the market. The role of Google has been discussed in the context of anti-trust laws [50], influencing copyright laws [46] and recently trials have commenced in U.S. courts for abusing its dominance over digital advertising [44].

Identification of effective responsible power (in the event of breaches) will require in-depth if not complete understanding of the data collection practices of organisations. For example, recent research identified myriads of non rivalrous data collection points through various essential software development services provided by platforms [79] spawning the ability for comprehensive datafication [78]. These happen unbeknownst to users [94] and even developers [36]. Facebook data harvesting by Cambridge Analytica is an example of the opacity behind which firms operate making it difficult to apportion liability.

There are many examples in security where *realisations* through expert investigations have contributed to the identification of the responsible *effective power*. During the early 90s, banks in England deflected liability onto customers, arguing that their systems used strong cryptography and hardware security modules and thus could not be breached, with banks wrongly blaming innocent individuals for lost funds. However, investigations revealed the perfidy of such blanket assertions. Banks refused to provide evidence of their so-called ironclad security to independent experts [6]. Consequently, many victims who were wrongly accused of fraud eventually got justice. The UK's Post Office scandal, too, demonstrates that widespread public action can lead to appropriate apportioning of liability on the software provider instead of the 'buck' being passed to its users [62]. The CISA directive that organisations take responsibility of their customer data, captures *obligations of effective power* [24].

Implication. An *ethical responsibilization* based identification of *effective power* means understanding markets, incentives, systems engineering and the effectiveness of regulations. An advantage of continued engagement with the realities as they evolve is the ability to incrementally strengthen the regulatory environment rather than trying to get it right at its inception.

7.2 Capability

Sen formulated *capability approach* as a framework of thought to assess the opportunities individuals have to live a life they can and they value [88]. For example, one cannot provision cycle as transport to someone with impairment in their legs.

The *capability* theme emerged from responses pertaining to the steps that were taken by breach victims and what participants thought as to the steps that can be taken by end users in an 'ideal' responsibility regime.

We asked participants if organisations should explicitly ask their customers to take specific steps to contain the fallout from the breach and to mitigate consequences. We received 51 responses from 56 managers. 47 respondents said they would expect end users to carry out *all or some* of the advised steps. In responding to the question on whether participants themselves should take steps, 28 said 'yes' and 28 said 'no'.

The 28 participants arguing for victims to shoulder some responsibility mentioned specific steps. 2 participants mentioned using *multiple identities* for distinct services, 18 participants suggested adoption of *improved security hygiene* like *multi factor authentication, strong password*, 6 participants suggested *GDPR awareness and improved data sharing practices*, 1 participant suggested *changing service providers* and 2 participants suggested *periodic credit checks*. "*I feel customers need to take some action in order to protect their own interests, such as properly securing their accounts, keeping an eye on their credit report and keeping an eye on their accounts for any unusual activity*" (P151). We find an overwhelming presence of *passwords* in Figure 9.

Twenty eight manager participants said they did not expect customers to take any steps to protect themselves.

> *Customers no, staff yes.... The IT dept and security team are responsible for implementing the necessary controls, staying ahead of the threat landscape and educating colleagues on modern security best practice. Staff need to understand cyber hygiene in the organisation, and work as secure and resilient colleagues in that business* (P3).

There is clearly a delineation of the entity that is technically ideally placed to implement the protection mechanisms.

Ninety Five of the victims took steps to protect themselves. The steps ranged from *changing their passwords, subscribing to alerts and credit reference agencies*. Most of the victims opted for changing their passwords with a sense of *resignation* among some of them. Multi factor authentication was adopted by few of the victims and the other actions taken by participants fall in the non technical domain like subscribing to fraud alerts and credit reference agencies. An assessment of capability can build upon this activity oriented nature of end-users to design prevention or post breach management mechanisms. However, such mechanisms should be in compatible with their agency and dignity.

Consider that, of 36 non-victims, 22 believed customers should shoulder responsibilities while 14 did not believe that they had a role.

Many participants both end users and managers expect customers to take steps up-to varying degrees to protect their data. How far is this expectation in sync with reality for both organisations as well as individuals? Are they based on an understanding of organisational or individual opportunities?

A notable study with 239 employees of small and medium enterprises (SMEs) in Europe reveal organisational challenges in implementing data protections. The respondents flag lack of usable resources like Privacy Enhancing Technologies (PETs) catalogue, access to skills or ability to identify data based on their sensitivity contribute among others [9]. SMEs find it difficult to comprehend applicable provisions of [43] and then implement them [89]. Some SMEs find PETs too expensive [48] and/or difficult to use [27].

With respect to end-users, individuals differ in their education, ability, age, and personal circumstances and these diversities influence their ability to engage with digital systems [35]. To that end, Das Chowdhury *et al.* [34] proposed the adoption of *capability approach* as a methodological foundation for adequate assessment of individual dispositions. Subsequently, a study was carried to evaluate the barriers individuals over 65 years face in carrying out 5 widely recommended cyber security tasks. These cyber security tasks are as setting up *strong passwords, back ups, secure WiFi*, using *multi factor authentication* and applying *software upgrade*. The study reported a range of accessibility barriers such as *vision, dexterity*, skills, emotional issues [35]. A *realisation* based *responsibilization* paradigm means adequate evaluation of organisational and individual needs while incorporating expectations about steps they can tale to prevent data breaches. Revisiting the example of CISA directive, their opportunities to meet their obligations need assessment through the lens of *capability*.

Implication. *Ethical responsibilization* would depart from designing mechanisms *that others cannot reasonably reject* to mechanisms *that others can reasonably accept*. This has implications in conceiving *fiduciary responsibilities* in data protection. Capability assessments should also be carried out while pushing credit monitoring and other remedial measures that, in essence, require considerable victim participation to control the risks or consequences of a data breach.

7.3 Comprehensive Outcome

Sen uses *comprehensive outcome* to suggests an expansion of the informational basis for a jurisprudence framework to take into account realisations on the ground. This means understanding how legal provisions affect human lives and using that feedback to advance the cause of justice.

We propose to evolve a *responsibilization* paradigm through a *realisation* based understanding; this means taking into account the *consequences* (of data breach), agencies involved and processes used. Figure 9 shows the emphasis on empathy, human-mediated responses and assurances on the organisational responses.

The responses from our participants mention the importance of an understanding (from service providers) of human consequences and provisioning human support (rather than impersonal communication methods). With respect to processes used, we find that our participants underlined the need for *being with the victim till effective remedy*.

We asked our participants about the manner of appropriate response from service providers to victims of data breach. Twenty two participants mentioned the importance of *empathy* and response through a *human*. "*They should be humble and understand that this will cause a lot of anxiety to people as they could lose their homes or more because of that*" (P141). "*Phone call with trained customer service staff who are knowledgeable about the breach and can put customers minds at ease*" (P3).

Responses from many victims of data breaches can be represented by the quote "*absolute disregard to personal data protection*" (P26). 30 victims of data breaches in our study explicitly referred to the organisational response as: *indifferent*, victims being *left to themselves* and victims accepting breaches as *fate accompli*.

With respect to the process of assisting victims, we cite the responses of a victim — "*I think the all hands meeting was great, but we have received no further detail now that we are 9 months on as to what stage things are at now with security. An update would be very helpful*" (P73).

A non-victim responded about expected behaviour as "*Apologetically, ensure it wont happen again and how to prevent it on both sides*" (P150). These responses highlight the need for an evaluation of the processes to prevent data breaches. Processes often lack information on how they fail in practice [2]. A feedback on technical mechanisms can help prepare commensurate technical response. These technical mechanisms can be internal to organisations, their supply chain as well as the security tasks they expect their customers to adopt. The latter is tied to the evaluation of individual opportunities using *capability approach*.

A *realisation*-based evolution of *responsibilization* will also examine the actual effectiveness of existing legal paradigm to appropriately align responsibilities. Legal research suggests that GDPR as it stands could not have prevented mass harvesting by Cambridge Analytica [100]. Legal scholarship also argues that the privacy paradigm is not enough to contain or prevent mass harvesting of data. Data breaches or mass harvesting of data result in aggregate harm while the privacy paradigm largely captures individual harm and thus inadequate [14]. Consent is an important ingredient of the privacy paradigm; recent legal scholarship suggests that it is used as a veil for unwarranted legitimacy to data collection [91]. A *realisation* based paradigm will scrutinise if existing legal instruments can potentially throttle public interest; for example, Facebook's legal challenge against NYU's Ad Observatory taking recourse to The Computer Fraud and Abuse Act [30]. Continuous evaluation of the effectiveness of existing regulatory framework will feedback to plug manifest gaps or design effective regulations.

Data breaches have human consequences. For example, the 2022 hack on International Red Cross data, exposed 515,000 individuals in disadvantaged positions due to conflict, migration and disaster, to immediate and potential long term harm. Consideration of consequences brings in the necessary feedback of human cost into any *responsibilization* framework. We add here that we do not advocate a consequentialist view completely ruling out the moral needs of a effective *responsibilization* framework. *Comprehensive outcome* specifies continual assessment of the effectiveness of initiatives such as CISA directives on the ground to feed back into their obligations and augment their capabilities where needed.

Implication. Taking into consideration human consequences can help evolve a *ethical responsibilization* framework which is not indifferent to individual lives and liberty. An assessment of the effectiveness of process can inform how they fail in practice. This eventually can feedback into designing improved processes.

8 Conclusion

We sought to investigate the aftermaths of data breaches where the data organisations hold of customers/staff is leaked. We wanted to know how organisations act in these cases, and how those who fell victim felt about how the breach aftermath was managed. We also surveyed those who hadn't fallen victim would want the aftermath to be managed.

We found that data breach victims experienced a sense of *abandonment* and sought accountability, empathy and reassurance from the breached organisation. The existing regulatory paradigm clearly has exploitable gaps using which allows responsible entities to delay informing victims, unfairly responsibilize them, not compensate them and wiggle out of the situation leaving second victims high and dry. We argue that the shortcomings in the extant regulatory frameworks stem from discounting social, economic and environmental realities as they evolve. Ignoring the socio-economic realities can create a false sense of security and accountability. Continuous engagement with evolving realities can help identify redressable manifest exploitable gaps.

We have proposed an alternative called *ethical responsibilization* framework. The intent was to ground the moral obligations of a *responsibilization* regime through continuous engagement with socio-economic realities as they evolve. These *obligations of effective power* will help the regulatory process to navigate opaque supply chains, delineate *obligations* and hold the responsible parties accountable for lapses. The new paradigm will appropriately *responsibilize* customer and staff 'second victims' through a *capability*-based evaluation of their opportunities.

Comprehensive outcome aims to incrementally expand the reach of *ethical responsibilization* through a continuous assessment of *obligations* and *expectations of customer participation* delineated through the paradigm. This assessment takes into account consequences and involved agencies. Thus, feedback is inherent in the paradigm.

The element of feedback makes the three ingredients as related rather than distinct components. On the other hand, from a policy perspective, feedback, in turn, would help deliver the development of policies and practices that are aligned to the reality of the situation rather than an ideal of how it ought to be.

The Ethical Responsibilization Framework we present does not aim to achieve a epistemological status of perfect *ethical responsibilization* for data breaches. Rather, we highlight the issues under each of the dimensions of the paradigm. These can only be enriched and refined through continuous feedback. This, we believe, presents an opportunity for future policy research to build upon. Undoubtedly, something has to change, and this paradigm provides a reasoned way forward.

Acknowledgments

This work is supported by REPHRAIN: National Research centre on Privacy, Harm Reduction and Adversarial Influence online (EPSRC Grant: EP/V011189/1).

References

[1] Joseph Anderson. 2024. Exclusive:Revealed: The scale of pay-outs to victims for NHS Scotland data breaches. https://www.scotsman.com/health/revealed-the-scale-of-pay-outs-to-victims-for-nhs-scotland-data-breaches-4684335.

[2] Ross Anderson. 1993. Why cryptosystems fail. In *Proceedings of the 1st ACM Conference on Computer and Communications Security*. ACM, Fairfax, Virginia, USA, November 3-5, 215–227. https://doi.org/10.1145/168588.168615.

[3] Ross Anderson. 2001. Why information security is hard-an economic perspective. In *Seventeenth Annual Computer Security Applications Conference*. IEEE, New Orleans, USA, 358–365. https://doi.org/10.1109/ACSAC.2001.991552.

[4] Ross Anderson. 2020. *Security engineering: a guide to building dependable distributed systems.* John Wiley & Sons, Indianapolis, USA.

[5] R.J. Anderson, Eireann Leverett, and Richard Clayton. 2018. Standardisation and Certification of the Internet of Things. https://www.repository.cam.ac.uk/handle/1810/287966 10.17863/CAM.35286.

[6] Ross J Anderson. 1994. Liability and computer security: Nine principles. In *Computer Security—ESORICS 94: Third European Symposium on Research in Computer Security November 7–9, 1994 Proceedings 3*. Springer, Brighton, United Kingdom, 231–245. https://doi.org/10.1007/3-540-58618-0_67.

[7] Benjamin Avanzi, Xingyun Tan, Greg Taylor, and Bernard Wong. 2023. Cyber Insurance Risk: Reporting Delays, Third-Party Cyber Events, and Changes in Reporting Propensity–An Analysis Using Data Breaches Published by US State Attorneys General. arXiv preprint arXiv:2310.04786.

[8] Baharuddin Aziz, Suhardi, and Kurnia. 2020. A systematic literature review of cyber insurance challenges. In *2020 International Conference on Information Technology Systems and Innovation (ICITSI)*. IEEE, Bandung, Indonesia, 357–363. https://doi.org/10.1109/ICITSI50517.2020.9264966.

[9] Maria Bada, Steven Furnell, Jason RC Nurse, and Jason Dymydiuk. 2023. Supporting Small and Medium-Sized Enterprises in Using Privacy Enhancing Technologies. In *International Conference on Human-Computer Interaction*. Springer, 274–289. https://doi.org/10.1007/978-3-031-35822-7_19.

[10] Vassiliki Bamiatzi, Michael Dowling, Fabian Gogolin, Fearghal Kearney, and Samuel Vigne. 2023. Are the good spared? Corporate social responsibility as insurance against cyber security incidents. *Risk Analysis* 43, 12 (2023), 2503–2518. https://doi.org/10.1111/risa.14122.

[11] Gaurav Bansal. 2018. Data Breaches and Trust Rebuilding: Moderating Impact of Signaling of Corporate Social Responsibility. In *HCI in Business, Government, and Organizations: 5th International Conference, HCIBGO 2018, Held as Part of HCI International*. Springer, Las Vegas, NV, USA, July 15-20, 253–261.

[12] Justin Bathon. 2013. How little data breaches cause big problems for schools. *The Journal* 40, 10 (2013), 26–29.

[13] BBC. 2018. Uber fined £385,000 for losing UK customer data. https://www.bbc.com/news/technology-46357001.

[14] Omri Ben-Shahar. 2019. Data pollution. *Journal of Legal Analysis* 11 (2019), 104–159. https://doi.org/10.1093/jla/laz005.

[15] Jeremy Bentham. 1970. An Introduction to the Principles of Morals and Legislation (1789). In *The collected works of Jeremy Bentham*, J. H. Burns and H. L. A. Hart (Eds.). Clarendon Press, New York.

[16] Joshua M Bentley, Kimberly R Oostman, and Sayyed Fawad Ali Shah. 2018. We're sorry but it's not our fault: Organizational apologies in ambiguous crisis situations. *Journal of Contingencies and Crisis Management* 26, 1 (2018), 138–149. https://doi.org/10.1111/1468-5973.12169.

[17] Heinz-Peter Berg. 2010. Risk management: procedures, methods and experiences. *Reliability: Theory & Applications* 5, 2 (17) (2010), 79–95.

[18] Donna Borak. 2017. Former Equifax CEO Richard Smith: 'I am deeply sorry'. https://money.cnn.com/2017/10/02/news/companies/equifax-smith-cyber-breach-apology/index.html.

[19] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101. https://doi.org/10.1191/1478088706qp063oa.

[20] Hart S Brown. 2016. After the data breach: Managing the crisis and mitigating the impact. *Journal of Business Continuity & Emergency Planning* 9, 4 (2016), 317–328.

[21] Capital One. 2019. Information on the Capital One cyber incident. https://www.capitalone.com/digital/facts2019/.

[22] Jessica Rose Carre, Shelby R Curtis, and Daniel Nelson Jones. 2018. Ascribing responsibility for online security and data breaches. *Managerial Auditing Journal* 33, 4 (2018), 436–446. https://doi.org/10.1108/MAJ-11-2017-1693.

[23] Hsiangting Shatina Chen and Tun-Min Jai. 2021. Trust fall: data breach perceptions from loyalty and non-loyalty customers. *The Service industries journal* 41, 13-14 (2021), 947–963. https://doi.org/10.1080/02642069.2019.1603296.

[24] CISA. 2012. Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches. https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Protecting_Sensitive_and_Personal_Information_from_Ransomware-Caused_Data_Breaches-508C.pdf.

[25] Richard Console. 2018. Capital One Confirms Sensitive Customer Info Leaked Following NCB Management Services, Inc. Data Breach. https://www.jdsupra.com/legalnews/capital-one-confirms-sensitive-customer-4713230/.

[26] W Timothy Coombs. 2007. Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review* 10 (2007), 163–176. https://doi.org/10.1057/palgrave.crr.1550049.

[27] Kovila PL Coopamootoo. 2020. Usage patterns of privacy-enhancing technologies. In *Proceedings of the SIGSAC Conference on Computer and Communications Security*. ACM, Virtual Event, 1371–1390. https://doi.org/10.1145/3372297.342334.

[28] Cory Doctorow. 2024. Health data – it isn't just Palantir or bust. https://goodlawproject.org/cory-doctorow-health-data-it-isnt-just-palantir-or-bust/.

[29] Maurice Cranston. 1989. Jean-Jacques Rousseau and the fusion of democratic sovereignty with aristocratic government. *History of European Ideas* 11, 1-6 (1989), 417–425. https://doi.org/10.1016/0191-6599(89)90229-5.

[30] Andres Crocker, Cory Doctorow, and Naomi Gilens. 2020. Facebook’s Election-Week War on Accountability is Wrong, Wrong, Wrong. https://www.eff.org/deeplinks/2020/10/facebooks-election-week-war-accountability-wrong-wrong-wrong.

[31] Savino Dambra, Leyla Bilge, and Davide Balzarotti. 2020. SoK: Cyber insurance–technical challenges and a system security roadmap. In *IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, USA, 1367–1383. https://doi.org/10.1109/SP40000.2020.00019.

[32] Kristopher Dane. 2012. *Considering Data Breaches: Public Information, Corporate Responsibility, and Market Valuations.* Master’s thesis. Interdisciplinary Arts and Sciences, University of Washington.

[33] Partha Das Chowdhury and Bruce Christianson. 2010. More Security or Less Insecurity. In *The 18th International Security Protocols Workshop (Lecture Notes in Computer Science, Vol. 7061)*, B. Christianson and J. A. Malcolm (Eds.). Springer Verlag, Cambridge, UK, 115–119. https://doi.org/10.1007/978-3-662-45921-8_19.

[34] Partha Das Chowdhury, Andrés Domínguez Hernández, Marvin Ramokapane, and Awais Rashid. 2022. From Utility to Capability: A New Paradigm to Conceptualize and Develop Inclusive PETs. In *New Security Paradigms Workshop*. ACM, New Hampshire, USA, 60–74. https://doi.org/10.1145/3584318.3584323.

[35] Partha Das Chowdhury and Karen Renaud. 2023. ‘Ought’ should not assume ‘Can’. Basic Capabilities in Cybersecurity to Ground Sen’s Capability Approach. In *Proceedings of the 2023 New Security Paradigms Workshop*. ACM, Spain, 76–91. https://doi.org/10.1145/3633500.3633506.

[36] Michalis Diamantaris, Elias P Papadopoulos, Evangelos P Markatos, Sotiris Ioannidis, and Jason Polakis. 2019. Reaper: real-time app analysis for augmenting the Android permission system. In *Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy*. ACM, Texas, USA, 37–48. https://doi.org/10.1145/3292006.3300027.

[37] Dooley Harte. 2023. Update on USS Capita Data Breach. https://www.ucu.org.uk/article/13020/Update-on-USS-Capita-data-breach.

[38] Jean Drèze and Amartya Sen. 2012. Putting growth in its place. *Yojana* 56 (2012), 36–40.

[39] ENISA. 2023. ENISA THREAT LANDSCAPE 2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

[40] European Commission. undated. What is a data breach and what do we have to do in case of a data breach? https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_en.

[41] Emily Flitter and Karen Weise. 2019. Capital One Data Breach Compromises Data of Over 100 Million. https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html.

[42] Stefan Frei. 2014. *Why your data breach is my problem.* Technical Report. NSS Labs. https://www.researchgate.net/publication/268800330.

[43] M da C Freitas and Miguel Mira da Silva. 2018. GDPR Compliance in SMEs: There is much to be done. *Journal of Information Systems Engineering & Management* 3, 4 (2018), 30. https://doi.org/10.20897/jisem/3941.

[44] Brian Fung. 2024. DOJ antitrust case targeting Google’s ad-tech business will go to trial in September, federal judge rules. https://edition.cnn.com/2024/02/05/tech/doj-antitrust-case-google-ad-trial-september/index.html.

[45] B Ganapathi Subramaniam, T Chithralekha, and B Amudhambigai. 2023. What Ails Cyber Insurance? An Analysis of Barriers and Drivers Using Fuzzy TOPSIS Method. *SN Computer Science* 5, 1 (2023), 20. https://doi.org/10.1007/s42979-023-02266-2.

[46] Joanne Elizabeth Gray. 2020. *Google rules: The history and future of copyright under the influence of Google.* Oxford University Press, New York, USA.

[47] Craig Hale. 2023. Employees are nearly always to blame for data breaches. https://www.techradar.com/pro/employees-are-nearly-always-to-blame-for-data-breaches.

[48] Tahereh Hasani, Davar Rezania, Nadège Levallet, Norman O’Reilly, and Mohammad Mohammadi. 2023. Privacy enhancing technology adoption and its impact on SMEs’ performance. *International Journal of Engineering Business Management* 15 (2023), 18479790231172874. https://doi.org/10.1177/18479790231172874.

[49] Zahra Hassanzadeh, Sky Marsen, and Robert Biddle. 2020. We’re Here to Help: Company Image Repair and User Perception of Data Breaches. In *Graphics Interface, 28-29 May*. ACM, Ontario, Canada.

[50] Benjamin Clay Hughes. 2020. Time for Change: How Google’s Anticompetitive Conduct Reveals the Deficiencies of Modern Antitrust Regulation. *Cardozo Int’l & Comp. L. Rev.* 4 (2020), 399.

[51] Connor Jones. 2023. Equifax scores £11.1M slap on wrist over 2017 mega breach. https://www.theregister.com/2023/10/13/equifax_fca_fine/?ref=upstract.com.

[52] Maria Karyda and Lilian Mitrou. 2016. Data breach notification: issues and challenges for security management. In *Tenth Mediterranean Conference on Information Systems (MCIS)*. AIS, Paphos, Cyprus.

[53] A.S.M. Kayes, Mohammad Hammoudeh, Shahriar Badsha, Paul A Watters, Alex Ng, Fatma Mohammed, and Mofakharul Islam. 2020. Responsibility Attribution Against Data Breaches. In *IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*. IEEE, Doha, Qatar, 498–503.

[54] Hiroaki Kikuchi, Michihiro Yamada, Kazuki Ikegami, and Koji Inui. 2021. Best Security Measures to Reduce Cyber-Incident and Data Breach Risks. In *International Workshop on Data Privacy Management*. Springer, Darmstadt, Germany, 3–19. https://doi.org/10.1007/978-3-030-93944-1_1.

[55] Bokyung Kim, Kristine Johnson, and Sun-Young Park. 2017. Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity. *Cogent Business & Management* 4, 1 (2017), 1354525. https://doi.org/10.1080/23311975.2017.1354525.

[56] Claire Lending, Kristina Minnick, and Patrick J Schorno. 2018. Corporate governance, social responsibility, and data breaches. *Financial Review* 53, 2 (2018), 413–455. https://doi.org/10.1111/fire.12160.

[57] Tony Liao and Haley Fite. 2021. ‘It’s My Fault For Posting In The First Place’: How Individual Responsibility And Self-blame Are Sustained And Internalized. In *The 22nd Annual Conference of the Association of Internet Researchers*. AoIR, Online. https://doi.org/10.5210/spir.v2021i0.12200, 13-16 Oct.

[58] David Lieberman. 1999. Adam Smith on justice, rights, and law. http://dx.doi.org/10.2139/ssrn.215213.

[59] Marissa MacWhirter. 2023. Glasgow Arnold Clark customers at risk after major cyber attack. https://www.glasgowtimes.co.uk/news/scottish-news/23321904.glasgow-arnold-clark-customers-risk-major-cyber-attack/.

[60] Leo P Martinez. 2020. Cyber Risks: Three Basic Structural Issues to Resolve. In *InsurTech: A Legal and Regulatory View*, Pierpaolo Marano and Kyriaki Noussia (Eds.). Springer, 211–230. https://doi.org/10.1007/978-3-030-27386-6_10.

[61] Kristin Masuch, Maike Greve, and Simon Trang. 2021. What to do after a data breach? Examining apology and compensation as response strategies for health service providers. *Electronic Markets* 31, 4 (2021), 829–848. https://doi.org/10.1007/s12525-021-00490-3.

[62] M.R. McGuire and Karen Renaud. 2023. Harm, injustice & technology: Reflections on the UK’s subpostmasters’ case. *The Howard Journal of Crime and Justice* 62, 4 (2023), 441–461. https://doi.org/10.1111/hojo.12533.

[63] Miro. 2022. Miro | Online Whiteboard for Visual Collaboration. https://miro.com/.

[64] Zareef Mohammed. 2022. Data breach recovery areas: an exploration of organization’s recovery strategies for surviving data breaches. *Organizational Cybersecurity Journal: Practice, Process and People* 2, 1 (2022), 41–59. https://doi.org/10.1108/OCJ-05-2021-0014.

[65] Tyler Moore, Richard Clayton, and Ross Anderson. 2009. The Economics of Online Crime. *The Journal of Economic Perspectives* 23, 3 (2009), 3–20.

[66] Gareth Mott, Sarah Turner, Jason RC Nurse, Jamie MacColl, James Sullivan, Anna Cartwright, and Edward Cartwright. 2023. Between a rock and a hard (ening) place: Cyber insurance in the ransomware era. *Computers & Security* 128 (2023), 103162. https://doi.org/10.1016/j.cose.2023.103162.

[67] Nelson Novaes Neto, Stuart Madnick, Anchises Moraes G De Paula, and Natasha Malara Borges. 2021. Developing a global data breach database and the challenges encountered. *Journal of Data and Information Quality (JDIQ)* 13, 1 (2021), 1–33. https://doi.org/10.1145/3439873.

[68] Lily Hay Newman. 2019. Everything We Know About the Capital One Hacking Case So Far. https://www.wired.com/story/capital-one-paige-thompson-case-hacking-spree/.

[69] Alfred Ng. 2023. How the Equifax hack happened, and what still needs to be done. https://www.cnet.com/news/privacy/equifaxs-hack-one-year-later-a-look-back-at-how-it-happened-and-whats-changed/.

[70] Lananh Nguyen. 2021. Capital One settles a class-action lawsuit for $190 million in a 2019 hacking. https://www.nytimes.com/2021/12/23/business/capital-one-hacking-settlement.html.

[71] Charlie Osborne. 2019. This is the impact of a data breach on enterprise share prices. https://www.zdnet.com/article/this-is-how-a-data-breach-at-your-company-can-hit-share-prices/.

[72] Kjartan Palsson, Steinn Gudmundsson, and Sachin Shetty. 2020. Analysis of the impact of cyber events for cyber insurance. *The Geneva Papers on Risk and Insurance-Issues and Practice* 45 (2020), 564–579. https://doi.org/10.1057/s41288-020-00171-w.

[73] Sakshyam Panda, Aristeidis Farao, Emmanouil Panaousis, and Christos Xenakis. 2021. Cyber-insurance: Past, present and future. In *Encyclopedia of Cryptography, Security and Privacy*. Springer, 1–4. https://doi.org/10.1007/978-3-642-27739-9_1624-1.

[74] Nicole Perlroth and Mike Isaac. 2018. Inside Uber’s $100,000 Payment to a Hacker, and the Fallout. https://www.nytimes.com/2018/01/12/technology/uber-hacker-payment-100000.html.

[75] Omer Ilker Poyraz, Sarah Bouazzaoui, Omer Keskin, Michael McShane, and C Ariel Pinto. 2020. Cyber-assets at risk (CAR): The cost of personally identifiable information data breaches. In *ICCWS 2020 15th International Conference on Cyber Warfare and Security*, Vol. 402. Academic Conferences and publishing limited, Norfolk, USA, 402–410.

[76] Principles of Responsible Investment. no date. Fiduciary Duty in the 21^{st} Century: A Final Report. https://www.unpri.org/download?ac=11972.

[77] PwC. 2022. Global Digital Trust Insights Survey. https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights-2022.html.

[78] Jennifer Pybus and Mark Coté. 2022. Did you give permission? Datafication in the mobile ecosystem. *Information, Communication & Society* 25, 11 (2022), 1650–1668. https://doi.org/10.1080/1369118X.2021.1877771.

[79] Jennifer Pybus and Mark Cote. 2024. Super SDKs: Tracking Personal Data and Platform Monopolies in the Mobile. *Big Data & Society* 11, 1 (2024). https://doi.org/10.1177/20539517241231270.

[80] Paul Ralph. 2021. ACM SIGSOFT empirical standards released. *ACM SIGSOFT Software Engineering Notes* 46, 1 (2021), 19–19. https://doi.org/10.1145/3437479.3437483.

[81] James Rasalam and Raymond J Elson. 2019. Cybersecurity And Management's Ethical Responsibilities: The Case Of Equifax And Uber. *Global Journal of Business Pedagogy* 3, 2 (2019), 8–15.

[82] Karen Renaud, Stephen Flowerday, Merrill Warkentin, Paul Cockshott, and Craig Orgeron. 2018. Is the responsibilization of the cyber security risk reasonable and judicious? *Computers & Security* 78 (2018), 198–211. https://doi.org/10.1016/j.cose.2018.06.006.

[83] Karen Renaud, Merrill Warkentin, and George Westerman. 2023. *From ChatGPT to HackGPT: Meeting the cybersecurity threat of generative AI.* MIT Sloan Management Review. 64428 pages.

[84] Sasha Romanosky, Lillian Ablon, Andreas Kuehn, and Therese Jones. 2019. Content analysis of cyber insurance policies: how do carriers price cyber risk? *Journal of Cybersecurity* 5, 1 (2019), tyz002. https://doi.org/10.1093/cybsec/tyz002.

[85] Hamza Saleem and Muhammad Naveed. 2020. Sok: Anatomy of data breaches. In *Proceedings on Privacy Enhancing Technologies*. sciendo, 153–174. https://doi.org/10.2478/popets-2020-0067.

[86] Bruce Schneier. 2012. Feudal Security. https://www.schneier.com/blog/archives/2012/12/feudal_sec.html.

[87] Amartya Sen. 2009. *The Idea Of Justice.* Penguin.

[88] Amartya K. Sen. 1979. Equality of What? In *McMurrin S Tanner Lectures on Human Values.* Vol. 1. Cambridge: Cambridge University Press, 1987, Cambridge, UK. Reprinted in John Rawls and Charles Fried and Amartya Sen and Thomas C Schelling. Sterling M. McMurrin (Ed), Liberty, Equality and Law.

[89] Sean Sirur, Jason RC Nurse, and Helena Webb. 2018. Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). In *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security.* ACM, Toronto Canada, 88–95. https://doi.org/10.1145/3267357.3267368.

[90] Sky News. 2017. Uber boss Dara Khosrowshahi apologises to London for 'mistakes we've made'. https://news.sky.com/story/uber-boss-dara-khosrowshahi-apologises-and-asks-customers-to-work-with-us-11052842.

[91] Daniel J Solove. 2023. *Murky consent: an approach to the fictions of consent in privacy law.* Technical Report Paper No. 2023-23. GWU Legal Studies Research Paper No. 2023-23.

[92] Lior Jacob Strahilevitz. 2013. *Toward a Positive Theory of Privacy Law.* Technical Report. COASE-SANDOR Institute for Law and Economics Working Paper No. 637 Public Law and Legal Theory Working Paper NO. 421, University of Chicago.

[93] Steve Symanovich. 2021. Uber Data Breach Affects 57 Million Rider and Driver Accounts. https://lifelock.norton.com/learn/data-breaches/uber-data-breach-affects-57-million-rider-and-driver-accounts.

[94] Mohammad Tahaei, Julia Bernd, and Awais Rashid. 2022. Privacy, permissions, and the health app ecosystem: A stack overflow exploration. In *Proceedings of the European Symposium on Usable Security.* ACM, Karlsruhe, Germany, 117–130. https://doi.org/10.1145/3549015.3555669.

[95] Shauhin A Talesh. 2018. Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers" for businesses. *Law & Social Inquiry* 43, 2 (2018), 417–440.

[96] Anna Tarabasz. 2019. Corporate social responsibility in times of Internet (in) security. In *Responsible Organizations in the Global Context: Current Challenges and Forward-Thinking Perspectives*, Annie Bartoli, Jose-Luis Guerrero, and Philippe Hermel (Eds.). Springer, 237–250.

[97] Jason E. Thomas. 2019. A Case Study Analysis of the Equifax Data Breach 1 A Case Study Analysis of the Equifax Data Breach. https://doi.org/10.13140/RG.2.2.16468.76161.

[98] Richard Tuck (Ed.). 1991. *Hobbes: Leviathan.* Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511808166.

[99] European Union. 2018. General Data Protection Regulations. https://gdpr-info.eu

[100] Alexis Ward. 2022. The oldest trick in the Facebook: Would the general data protection regulation have stopped the Cambridge analytica scandal? *Trinity CL Rev.* 25 (2022), 221.

[101] Spencer Wheatley, Annette Hofmann, and Didier Sornette. 2021. Addressing insurance of data breach cyber risks in the catastrophe framework. *The Geneva Papers on Risk and Insurance-Issues and Practice* 46 (2021), 53–78.

[102] Julia Carrie Wong. 2017. Uber concealed massive hack that exposed data of 57m users and drivers. https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack.

[103] Zacks Equity Research. 2020. Capital One to Pay $80M Penalty Over Data Breach Incident. https://www.nasdaq.com/articles/capital-one-to-pay-%2480m-penalty-over-data-breach-incident-2020-08-07.

A Adherence to SIGSOFT guidelines

The adherence of various aspects of the study to [80] can be summarised as:

(1) We recruited participants adhering to the relevant *essential attributes* of [80].

(2) The answers were a combination of choice based answers and free flowing text. The textual responses were analysed one participant at a time as outlined in *application* of [80].

(3) In Section 4.1, we outline how we achieved saturation. This is in line with the *essential attributes* [80].

(4) We present the findings of our study as per all the relevant *essential attributes* and some of the *desirable attributes* of [80].

(5) The survey text did not prompt the respondents to avoid any bias. This is in line with the relevant guideline under *essential attributes* of [80].

Table 5: Cyber Insurance Companies

1	HISCOX https://www.hiscox.co.uk/
2	PolicyBee https://www.policybee.co.uk/
3	MPR Underwriting https://www.mprunderwriting.com/products/cyber-incident-response-insurance/
4	AIG https://www.aig.com/home/risk-solutions/business/cyber
5	Chubb https://www.chubb.com/us-en/business-insurance/cyber-products.html
6	Zurich https://www.zurich.com/en/commercial-insurance/products/cyber
7	HSB https://www.munichre.com/hsbeil/en/products/cyber-insurance.html
8	AmTrust Financial https://amtrustfinancial.com/insurance-products/cyber-insurance
9	Travelers https://www.travelers.co.uk/products/cyber-insurance
10	AVIVA https://gcs.aviva.com/en-gb/classes-of-insurance/cyber/

B Survey Questions

When referring to an organisation, this means the organisation who was holding your data, which was breached.

Demographics

D1. Gender

D2. Age Range

D3. If a manager, how long

D4. Have you fallen victim to a data breach due to some organisation suffering a breach where your personal information was leaked? (Yes/No)

D5. When you commenced your relationship with the organisation, did they inform you of the contact details of a responsible person to get in touch with in the event of a data breach? (Yes/No/Don't Remember)

Questions for Victims:

V1. How did you learn of the breach? (Free Text)

V2. Did the organisation contact you about the breach? (Yes, as soon as they realised/Yes after delay/No)

V3. If Yes:

a. if you wanted to, were you able to get in touch with the responsible person? (Yes/No/I didn't want to/Couldn't remember)

b. Were you already aware of the breach before they contacted you? (Yes/No/Don't Remember)

c. When the organisation contacted you, did they mention any third party who they think was responsible for the breach? (Yes/No/Don't Remember)

d. When the organisation contacted you, did they re-direct you to a third party? (Yes/No/Don't Remember)

e. When the organisation contacted you, did they or a third party offer any compensation? (for example, covering the cost of identity theft insurance, cost to move bank account, or a cash sum to offset reputational damage) (Yes/No/Don't Remember)

f. Did the organisation (or a third party), mention any steps they are taking to notify all those who are affected? (Yes/No/Don't Remember)

g. Did the organisation (or a third party), mention any steps they are taking to contain the damages from the breach? (Yes/No/Don't Remember)

h. Did they (or a third party) ask YOU to take any steps to contain the damages from the breach? (Yes/No/Don't Remember)

i. Did they (or a third party) ask YOU to take any step to mitigate future breaches? (Yes/No/Don't Remember)

j. Did they (or a third party) clearly spell out the reasons for the breach? (Yes/No/Don't Remember)

k. Did the organisation ever apologise for the breach?

l. Did you yourself take any steps once you learnt about the breach? (Yes to me personally/Yes in the media/Yes to me and media/No/Don't Remember)

m. If Yes, What steps did you take? (Free Text)

n. Is there anything the organisation who had the breach could have done that they did not do? Please explain (Free Text)

o. How did you feel about how the organisation handled the aftermath of the breach. (Free Text)

V4. If No:

a. Do you think they should have contacted you? (Definitely not/I don't care/Definitely yes)

b. If Yes, what should they have told you? (Free Text)

c. If No, Given that you don't think they ought to have contacted you, please could you explain why not. (Free Text)

Non Victims:

NV1. If a data breach happens that leaks your personal information, how would you like to hear about it? (Free Text)

NV2. Imagine that a data breach of your personal information has occurred and the organisation contacts you, what would want the organisation to do (in an ideal world)? (Free Text)

NV3. Imagine that a data breach of your personal information has occurred and the organisation contacts you, Please indicate your agreement with the following statements (Strongly Disagree - Strongly Agree):

a. I would want them to tell me who they think was responsible for the breach.

b. I would want them to to re- direct me to a third party who lost my information.

c. I would want compensation.

d. I would want them to mention steps they are taking to notify all those who are affected.

e. I would want them to mention steps they are taking to contain the damages from the breach.

f. I would want them to ask ME to take steps to contain the damages from the breach.

g. I would want them to ask ME to take steps to mitigate future breaches.

h. I would want them to tell me why the breach happened.

i. I would want them to apologise for the breach.

j. I would take the steps the organisation advises me to take.

Managers:

M1. Does your organisation have cyber insurance? (Yes/No/Not Sure)

M2. Does your organisation use third parties to store your customer/staff personal data? (Yes/No/Not Sure)

M3. While you have been employed as a manager, did your organisation experience a data breach that leaked personal data? (Yes/No)

M4. If Yes:

a. Did your organisation apologise to customers whose data was breached in the aftermath? (Yes/No/Don't Remember)

b. *If insurance:* How helpful was the cyber insurance company? (Free Text)

c. How did you respond to your customers if any got in touch with you after the data breach? (Free Text)

d. *If third party used:*

(i) Given that you store your customers' personal data with third parties, is it your policy to reveal this to your customers once the breach has occurred? Please explain (Free Text)

(ii) *If third party used:* Did you refer your customers to the third party if it was the third party rather than yourselves who suffered the breach? (Yes/No/NA)

e. Did you (or your contracted third parties if appropriate) offer any compensation? (Yes, we did/Yes, 3rd party did/Yes we and 3rd party did/No/Unsure)

f. Did you explain the steps you (or your third party) are taking to contain the breach and mitigate future breaches? (Yes/No/Don't Know)

g. Did you explicitly ask your customers to take any steps to contain the fallout from the breach and to mitigate consequences? (Yes/No/Don't Know)

h. Did you expect them to carry out those steps? (Yes/No/Unsure)

i. Do you share results of any investigations with your customers? (Yes/No)

j. Who do you think should be responsible for managing the consequences of a breach? (Free Text)

k. Do you think users in general should shoulder some of the responsibilities to protect themselves against future breaches by organisations that hold their personal information? (Yes/No)
   (i) If Yes: Please say why and what you expect them to do? (Free Text)

M5 If No:

a. Should an organisation apologise to customers if their data is breached? (Yes/No/Don't Remember)
b. How should organisations respond to customers if they get in touch after a data breach? (Free Text)
c. If organisations store customers' personal data with third parties, should this be revealed to customers if a breach occurs? Please explain (Free Text)
d. Should organisations refer customers to a third party if it was the third party who suffered the breach? (Yes/No/NA)
e. Should the breached organisation or their contracted third parties offer any compensation if a breach occurs? (Yes we should/Yes 3rd party should/Both we and 3rd party should/No/Not Sure)
f. Should organisations explain the steps they are taking to contain the breach and mitigate future breaches to customers whose data has been breached? (Yes/No/Not Sure)
g. Should organisations explicitly ask their customers to take specific steps to contain the fallout from the breach and to mitigate consequences? (Yes/No/Don't Know)
h. Would you expect them to carry out those steps? (Yes/No/Some, not all)
i. Do you think organisations should share results of any investigations with customers whose data has been breached? (Yes/No)
j. Who do you think should be responsible for managing the consequences of a breach? (Free Text)
k. Do you think customers should shoulder some of the responsibilities to protect themselves against future breaches by organisations that hold their personal information? (Yes/No)
l. If yes: Please say why and how? (Free Text)
m. If no: who should? Please explain (Free Text)