THE UNIVERSITY OF SYDNEY

Understanding Data Breach Information: How Lay Individuals Interpret Breach Notifications

A thesis submitted in fulfilment of the requirements for the degree of

Master of Philosophy

By

Muqing Hu

Supervisors

Professor Jane Andrew

Professor Max Baker

Discipline of Accounting, governance and regulation

The University of Sydney Business School

May 2025

STATEMENT OF ORIGINALITY

I hereby affirm that this submission represents my original work. To the best of my knowledge, it contains no materials previously authored or published by another individual, nor does it include content that has been substantially used to obtain any other academic qualification at the University of Sydney or any other educational institution, unless appropriately cited within this thesis.

Contributions from others, whether with whom I have worked at the University of Sydney or elsewhere, have been explicitly acknowledged herein. This study also has acquired confirms from the University of Sydney on Ethical Conduct in Human Research with project identifier: 2023/HE000879.

I also declare that the intellectual content of this thesis is solely the outcome of my own work, except where assistance has been acknowledged in the design, conception, process, stylistic presentation, or linguistic refinement of the project.

During the preparation of this thesis, I did not use generative AI for writing but only used relevant software (e.g. Grammarly) as a grammar-checking tool. After the use of the AI program, I independently reviewed and edited the content to ensure the accuracy and coherence of this thesis. I, as the author, assume full responsibility for the final content of the thesis and its publication.

Muqing (Snow) Hu

November 2024

ACKNOWLEDGEMENTS

My deepest gratitude to everyone who has encouraged and supported me throughout these past two challenging yet rewarding years. First and foremost, I am profoundly grateful and greatly indebted to my supervisors, Professor Jane Andrew and Professor Max Baker, for their generous commitment of time and effort. Your unwavering guidance, substantial support, and dedicated help play an important role in shaping my ideas, thesis, and academic outlook. Thank you for providing me with the opportunity to embark on this research journey. Your inspirational insights and support not only enriched this thesis but also ignited a genuine passion in me when I felt lost and confused. This transformative experience has truly opened doors for my future academic endeavours.

I would like to extend my sincere gratitude to all the interview participants in this research. Your kindness, assistance, and invaluable contributions have significantly shaped the direction of this work. I am especially grateful to all the academics in the Discipline of Accounting, especially Dr. Neal Athur, who generously dedicated time to help me approach interviewees, Dr. Simon Tan for his guidance in finalising ethics approval, Professor John Roberts and Dr. Cary Di Lernia for their insightful suggestions during the preliminary thesis defence. And I am also deeply grateful to my reviewers, Dr. Sendirella George and Dr. Annemarie Conrath-Hargreaves, for their thoughtful and constructive feedback on my thesis, and to Associate Professor Demetris Christodoulou for his meticulous emendation suggestions.

I would like to express special thanks to Casey Huang, a senior PhD candidate, whose experiential advice and emotional support carried me through this journey. Without her guidance, completing this thesis would have been much more difficult. I am equally thankful to my HDR cohorts and friends for their camaraderie and encouragement along the way.

Finally, my deepest gratitude is reserved for my family. Their unwavering love, selfless devotion, and steadfast belief in my decisions have been a constant source of support. And to my grandfather, who I believe is watching proudly from heaven, your influence continues to inspire and support me. A special thanks to Qirun Jin, who has been by my side through every high and low of this journey. Your patience, encouragement, and understanding have been my greatest source of strength. I could not have achieved this milestone without your unconditional love and support.

ABSTRACT

This thesis investigates how lay individuals interpret and respond to current data breach notifications (DBNs). By demonstrating DBN as a new form of accounting information, this thesis calls for "rethinking expertise" (Collins & Evans, 2019) in accounting information use and extends the current literature from professional users to lay users in the context of data breaches. Central to this research is the question of how ambiguities within current DBNs exacerbate the vulnerability and interpretation challenges that lay individuals face. Drawing on Ellsberg's ambiguity aversion theory (1961), this thesis employs phenomenological interviews to capture nuanced subjective interpretations and qualitative experiments to further assess lay individuals' preferences in the face of ambiguity in DBNs. Findings reveal that current DBNs are largely ineffective, characterised by substantial ambiguities that hinder lay individuals' interpretation. As a result, lay individuals prefer to adopt a rational "protective" strategy to prioritise clarity over negativity in breach information. Moreover, the thesis identifies a "power dynamic" (Carr & Beck, 2022) between DBN providers (breached organisations) and recipients (lay individuals), highlighting the critical need to amplify lay individuals' voices in breach disclosure practices. Based on empirical insights, the thesis provides practical recommendations for individuals, organisations, and policymakers to reduce ambiguity in current DBNs and proposes a framework for more effective breach disclosures that empower lay users and promote greater accountability in the aftermath of data breaches.

Key Words: data breach; accounting information; disclosure; breach notifications; lay individual; interpretation; phenomenology; ambiguity aversion; power dynamic

LIST OF ABBREVIATIONS

ACSC	**Australian Cyber Security Centre**
AFP	**Australian Federal Police**
APP(s)	**Australian Privacy Principle(s)**
ASX	**Australian Securities Exchange**
CEO	**Chief Executive Officer**
CISA	**Certified Information Systems Auditor**
CISSP	**Certified Information Systems Security Professional**
DBL(s)	**Data Breach Letter(s)**
DBN(s)	**Data Breach Notification(s)**
IAR	**Interpretative Accounting Research**
NDB	**Notifiable Data Breach**
OAIC	**Office of the Australian Information Commissioner**
OPC	**Office of the Privacy Commissioner**

LIST OF TABLES AND FIGURES

TABLE OF CONTENTS

CHAPTER 1 - INTRODUCTION

1.0 Introduction

This chapter provides an overview of the research, outlining the primary issue under investigation, as well as the contexts, motivations, and the overarching research question that guide the study. It also presents a comprehensive structure of the thesis, offering a detailed roadmap for the analysis and discussions in the following chapters.

1.1 Context of Data Breach

In recent years, a series of notable data breach incidents occurred in Australia, including those affecting Medibank (2022), Optus (2022), and Latitude Financial (2023), which aroused people's deep concern over information security. According to the OAIC (Office of the Australian Information Commissioner) report (2023), 483 data breach notifications[1] were received between July and December 2023, with "a steady increase in notifications received month by month" – peaking at 97 notifications in December 2023. This upward trend continued into 2024, with the OAIC receiving 527 data breach notifications between January and June, marking the highest number reported since late 2020 and reflecting a 9% increase compared to the preceding six months (OAIC, 2024). In the face of the increasing number of data breaches, the current situation of information security in Australia is becoming increasingly grim.

A data breach is defined by OAIC (2024) as "unauthorised access to or unauthorised disclosure of personal information or a loss of personal information", which often results in significant harm to both organisations and affected individuals. From an organisational perspective, the loss of sensitive information usually leads to significant reputational damage and financial losses and even impedes the long-term stability of the organisation (Cheng et al., 2017). In terms of affected individuals, the loss of control over personal data can result in various forms of victimisation, with harms spanning financial, physical, and moral dimensions (Gibson & Harfield, 2023).

To mitigate these risks, the *Privacy Act 1988 (Cth)* serves as a key legislative framework to protect the handling of personal information. Amended in 2014 and 2017 to adapt to the evolving digital landscape, the Act outlines 13 Australian Privacy Principles (Apps) to set out entities' obligation for the management of personal information and stipulates the NDB (Notifiable Data Breach) Scheme to clarify requirements for notifying affected individuals and the commissioner in the case of certain data breaches (OAIC, 2024).

[1] Data breach notification refers primarily to the formal process through which an organisation informs affected individuals and relevant regulators that a data breach has occurred (OAIC, 2024). While data breach disclosure encompasses a broader range of communication activities, including formal notification as well as public announcements, press releases, public statements, investor reports and other forms of stakeholder communication. Given the conceptual overlap between the two terms, this study uses "data breach disclosure" and "data breach notification" interchangeably.

Under the OAIC regulations, the involved entities of data breaches are required to adopt mandatory disclosures with "reasonable methods" to notify individuals at risk of serious harm and provide a statement to the Commissioner "as soon as practicable" (OAIC, 2024). Besides, the Act also encourages voluntary disclosures, even when the breach is not considered material, to mitigate risks and manage public relations. However, the boundaries between mandatory and voluntary disclosure remain ambiguous. For example, breaches that do not meet the "serious harm" threshold or where remedial actions have mitigated potential harm are exempt from mandatory notification under the NDB Scheme. This ambiguity complicates compliance and transparency, raising concerns about whether the current breach notification framework adequately addresses the needs of affected individuals.

In terms of ambiguity, the NDB Scheme places significant emphasis on the "eligibility of data breaches" for notification. An effective data breach notification must detail the type of personal information involved, the overall circumstances of the breach (including the number of individuals affected, duration of the breach, and unauthorised access), and the potential harm resulting from the data breach. Entities obliged to make the notifications must balance the comprehensibility of their notifications with the resources required to notify affected individuals. In order to standardise the notification approaches, the OAIC (2024) provides three options for making disclosures: "Notifying all individuals", "Notifying only those individuals at risk of serious harm" and "Publishing notification", with the premise that the third one can only be used if the first two are not practicable.

Despite existing mechanisms, individuals remain the most direct and vulnerable victims of data breaches. In the second half of 2023, OAIC reported 26 breaches that affected over 5000 Australians, urging formulation and implementation of effective preventive measures. However, the current NDB Scheme has significant limitations. It stipulates mandatory disclosure only for breaches likely to result in "serious harm", which is defined as serious physical, psychological, emotional, financial, or reputational harm (OAIC, 2024). Breaches that do not meet this threshold, or where harm has been effectively mitigated through valid remedial actions, are exempt from mandatory notification. This gap raises concerns about the adequacy of the current framework in addressing the full spectrum of harm caused by data breaches and requires stronger regulatory guidance and improvements in the disclosure framework (Andrew et al., 2023).

Moreover, individuals often lack the expertise to fully comprehend the implications of a breach or take timely protective actions (Himick et al., 2016). As remediation is taken to eliminate the likelihood of subsequent harm, mandatory data breach disclosure serves as a critical mechanism for informing individuals of breaches and guiding them in taking protective measures. While existing research has explored the organisational impacts of data breach disclosures – such as economic, accountability, and decision-making implications – there is little understanding of how lay individuals interpret and respond to these disclosures (Albeshri & Thayananthan, 2018; Andrew et al., 2023; Huang & Wang, 2021).

Following such an argument, this thesis focuses on a specific breach incident – Latitude Financial data breach incident (2023) – and explores how data breach letter (DBL), a key breach disclosure measure used in Australia, is understood by individuals, particularly lay individuals who lack specialised knowledge of cybersecurity. Additionally, this thesis aims to propose further improvements to DBN frameworks, fostering greater clarity, accessibility, and trustworthiness in the breach disclosures.

1.2 Research Background, Motivations and Aims

In the past few years, a series of high-profile data breach incidents occurred in Australia, which aroused people's deep concern for information security. However, due to the lack of relevant professional expertise, breached victims often struggle to figure out what happened and how to protect themselves in a timely fashion. According to the OAIC (Office of the Australian Information Commissioner) statement (2023), mandatory stipulations were made by the *Privacy Act 1988 (Cth)* on notifying affected individuals and related government departments when a data breach may result in serious harm to personal information. As a convenient and effective approach, data breach letters then became the mainstream method for Australian companies to notify breached individuals and fulfil disclosure requirements.

Despite their widespread use, current breach notification letters often fail to effectively communicate essential information due to recipients' limited cybersecurity knowledge and expertise, which could lead to misunderstanding, unnecessary panic, and potential secondary damage. Furthermore, the *Privacy Act 1988 (Cth)* employs vague language to define the conditions under which notifications are required, limiting mandatory disclosure to breaches likely to cause "serious harm." Such legislative ambiguity has led to the predominance of voluntary disclosures in organisational reports, underscoring the need for clearer regulations and a standardised reporting framework. Consequently, proposing a robust mandatory disclosure framework in terms of data breaches is becoming an urgent research agenda (Andrew et al., 2023).

While extant studies have extensively explored the organisational implications of data breach disclosures, such as their economic, accountability, and decision-making impacts, little is known about the individuals' subjective understanding and preferences in breach disclosures (Albeshri & Thayananthan, 2018; Andrew et al., 2023; Huang & Wang, 2021). Given such a gap, this thesis specifically focuses on the 2023 Latitude Financial data breach incident and makes further investigations on how affected individuals, especially lay individuals without professional knowledge of cybersecurity and certain expertise, understand and respond to the DBLs they receive.

Meanwhile, motivated by the necessary need to standardise current breach notification practices (Andrew et al., 2023), this study seeks to uncover ways to improve the effectiveness of current DBNs

for non-expert recipients and aims to propose future avenues for enhancing breach disclosures. Given such context, this study addresses the overarching research objective: *To investigate the ways that lay individuals interpret the DBNs they receive.* This includes understanding how non-experts experience, interpret, and use breach-related information.

To achieve this, this study proposes a theoretical framework to analyse how often-overlooked lay individuals, different from professional users who have been well-studied in the existing literature, interpret accounting information in the context of data breaches (Himick et al., 2016). Using micro-phenomenology and qualitative experimental approaches, this research investigates lay individuals' preferences regarding less ambiguity in breach information. Grounded in Ellsberg's ambiguity aversion theory (1961), the study identifies lay individuals' preferences for prioritising clarity over negativity in DBNs as a rational "protective" strategy. As such, new light can be shed on the ineffectiveness of current DBNs, which could eventually impede lay individuals' actions in the aftermath of data breaches. Moreover, the ambiguity in current DBNs also reveals the "power dynamic" between notification providers (breached organisations) and recipients (lay individuals), further emphasising the vulnerability lay individuals face when navigating the uncertainty caused by data breaches (Carr & Beck, 2022). Drawing on the above empirical findings, this study finally provides practical recommendations to improve the overall accountability and transparency in DBNs and aims to inform policy reforms in future data breach disclosure practices.

1.3 Thesis Structure

This thesis mainly contains six chapters, and each chapter is structured as follows. Chapter 1 introduces the study background and the research context, explaining the practical and theoretical research motivations behind the inquiry. Chapter 2 reviews the existing literature on interpretative accounting research (IAR), accounting information use and users, data breach disclosure, and culminating in lay individuals' use of breach disclosures, providing a theoretical framework for understanding the current research on individuals' use of DBNs and highlighting the gap on lay individuals' interpretations of breach information. Furthermore, it also illustrates the rationale of the research and concludes with the overall research question. Chapter 3 outlines the research methodology, addressing the design, preparation, and execution of the study. It describes the pilot study process, emphasising how insights gained from mock interviews informed adjustments to the subsequent two formal interview phases. Chapter 4 presents the implications derived from the collected data, providing a comprehensive account of empirical findings. Chapter 5 extends the discussion on findings, making a deeper exploration of how lay individuals' interpretations of DBNs and their preferences related to ambiguity aversion informed by the relevant literature and theoretical framework. Finally, Chapter 6 concludes the thesis

by summarising the potential contributions to theory, methodology and practice, reflecting on the study's significance, limitations, and potential for future research.

CHAPTER 2 – LITERATURE REVIEW

2.0 Introduction

This chapter examines the extant literature on interpretative accounting research (IAR) and traces the evolution of accounting information use, highlighting the shift from a research focus on the use of accounting information by the users. Furthermore, this chapter explores the role of user expertise in accounting and establishes why DBNs constitute a novel form of accounting information. This chapter also addresses the existing research gap concerning lay individuals' interpretation of DBNs. By incorporating Ellsberg's ambiguity aversion theory (1961), this study investigates the significant effect of ambiguity on individual decision-making processes.

This review begins in Section 2.1 by discussing the IAR research, especially focusing on the phenomenological approach. Section 2.2 and Section 2.3 delineate the limited exploration of accounting information users and examine the role of expertise in its use. Section 2.4 and Section 2.5 trace the development of research on DBNs, justifying why it can be regarded as a form of accounting information. Section 2.6 narrows the research focus to lay users of DBNs, identifying key research gaps in the literature. Finally, Section 2.7 introduces Ellsberg's ambiguity aversion theory and its relevance to understanding lay individuals' interpretations of DBNs.

2.1 Interpretative Research in Accounting

Mainstream accounting research is grounded in three basic research paradigms: positivism, interpretivism, and critical theory (Chua, 1986). Commonly associated with empirical evidence and quantitative research, positivism emphasises objectivity in studies, with the belief that facts can be tested and proven, and therefore, positivists strive to minimise subjective interpretations and personal bias in scientific inquiries (Ryan, 2018). Critical theory, on the contrary, seeks to value modified subjectivity, it analyses complex social phenomena from multiple perspectives and advocates for the active engagement of challenging oppressive structures and pursuing social justice and liberation (Chua, 1986).

Compared to its counterparts, interpretivism is rooted in phenomenology and interpretive traditions (Mackenzie & Knipe, 2006; Ricoeur, 1976). It emphasises the significance of understanding the subjective interpretations that individuals attach to their social realities and experiences (Wilson, 2015). As discussed by Ricoeur (1976), interpretation acts as the link between language and lived experience. Interpretivism highlights the intersubjective nature of understanding and aims to provide an in-depth exploration of how individuals perceive, interpret, and make sense of social contexts (Ryan, 2018). From this perspective, interpretivists see reality as a dynamic, socially constructed phenomenon by

holding the point of view that individuals create their sense of social realities through their interactions and lived experiences (Buriro et al., 2021) and try to understand the lived experiences with subjective interpretation.

By emphasising the importance of understanding the subjective meanings individuals attribute to social reality, the interpretivism paradigm can be conceptualised as a societal initiative aimed at highlighting public interest and informing policymaking in accounting research (Wickramasinghe & Alawattage, 2017). This approach expands the previous domain of accounting by providing narratives, broadening its scope to encompass deeper societal and contextual considerations (Lehman, 2019). Within the interpretivism paradigm, *interpretative accounting research* (IAR), as illustrated by Chua (1986), was specifically applied in the field of accounting to constantly refine understandings of social reality and interpret accounting information by complex processes and structures. As it considers psychological, organisational, and societal contexts in its analysis (Hoque et al., 2017), IAR experienced long evolvement.

From the 1960s to the 1980s, following Argyris' (1952) seminal study on the effects of human behaviour, the behavioural accounting approach gradually entered IAR researchers' vision, drawing extensively on psychology and sociology. This shift challenged the conventional view of accounting as a purely technical discipline, expanding its scope to encompass broader social science practices (Hoque et al., 2017). Meanwhile, researchers began to recognise the necessity of engaging closely with research participants and conducting intensive field observations to achieve an in-depth understanding of individuals (Tomkins & Groves, 1983).

During this period, much of the emerging accounting research can be categorised under the label of IAR, with its initial focus on the process of 'making sense' of issues (Hoque et al., 2017). Later, scholars such as Hopper and Powell (1985) and Chua (1986) further expanded the theoretical underpinnings of IAR, situating it within a social constructivist epistemology and calling for new insights within organisational and societal contexts. Building on these developments, IAR evolved to concentrate on exploring people's subjective meanings and intentions, delving into the socially embedded understandings and behaviours within individuals' natural environments (Lukka & Modell, 2017).

In the 1990s, debates within IAR turned to various internal variants. Ethnographic and empirical approaches (Elharidy et al., 2008; Gurd, 2008; Parker & Roffey, 1997), such as grounded theory (Glaser & Strauss, 2017) and actor-network theory (Justesen & Mouritsen, 2011; Lukka & Vinnari, 2014), became prevalent in established IAR. However, as proposed by De Loo and Lowe (2017), these approaches often pay limited attention to people's subjective motivations, which departs from the prior social constructive epistemology associated with IAR.

Simultaneously, another variant of IAR leaned on established theoretical frameworks, such as Gidden's structuration theory (Boland, 1993) and institutional theory (Covaleski & Dirsmith, 1990), which keep

addressing the significance of empirical work and the socio-cultural dynamics for understanding accounting practices. Case research also gained traction, emphasising theory development over empirical analysis, with scholars like Ahrens and Chapman (2006) advocating for greater theoretical rigour and problematisation to advance IAR (Hoque et al., 2017).

An additional variant of IAR, labelled explanatory IAR, emerged in response to a radical shift in the concept of causality within the philosophy of science (Lukka & Modell, 2017). Moving beyond descriptive inventories of individuals' subjective understandings, explanatory IAR began probing the nature of explanation and interpretation as central research objectives (Lukka & Modell, 2017). This shift marked a significant expansion of interpretative boundaries, with researchers such as Macintosh and Scapens (1990) suggesting that management accounting systems serve as interpretative frameworks, standards, and facilities for managerial decision-making, leading the further research of IAR into a more micro-level utilisation process.

As an interpretative act, accounting involves multiple layers of interpretation. These processes include not only the preparation and presentation of accounting records and reports but also the interpretation of accounting information by its users (Boland, 1993). Since accounting is primarily used to provide information that facilitates decision-making (Young, 2006), interpreting accounting information serves as a fundamental prerequisite for making informed decisions. However, decision-making based on accounting information is not solely determined by the information itself but is also significantly influenced by users' individual interpretations, such as managers' understanding of reports and the contextual factors that shape those interpretations (Simon & March, 2015). This recognition has led to an increasing focus on understanding how individuals interpret accounting information in IAR.

Prior accounting research has adopted various approaches to examining individuals' interpretations, such as readability and understandability (Abu et al., 2010; Adelberg, 1979). These approaches explore the level of complexity in written texts and the extent to which readers can effectively comprehend them (Bailin & Grafstein, 2016). However, readability and understandability are grounded in objective perspectives, focusing on the degree of easiness with which a written text can be read and understood but often fail to account for the contextual background knowledge of specific reader groups or individuals, thereby largely neglecting the subjective dimensions of interpretations (Dale & Chall, 1949). This limitation led to the exploration of alternative theoretical frameworks better suited to capturing the nuances of subjective interpretation within IAR.

In response to the requirements of interpreting how individuals experience and make sense of accounting information, *sensemaking* and *phenomenology* then emerged as prominent philosophical frameworks within IAR (Maulana et al., 2022). Sensemaking is a cognitive process that individuals and groups use to interpret and assign meaning to their experiences, especially in situations characterised by complexity or uncertainty (Sandberg & Tsoukas, 2015). It involves making sense of ambiguous or

confusing information by constructing mental models, narratives, or explanations that provide coherence and understanding (Kapon, 2017). By understanding how individuals and groups make sense of their experiences, researchers and practitioners can facilitate more effective communication, problem-solving, and decision-making processes, helping individuals and organisations navigate complexity and uncertainty more successfully (Choo & Bontis, 2002).

Sensemaking has been widely applied in IAR to explore how individuals and groups interpret accounting information within complex and dynamic environments. For instance, Tillmann and Goddard (2008) investigated how sensemaking was carried out in strategic management accounting, focusing on management accountants' attempts to understand their past, present, and future environment. Similarly, Abdul-Khalid (2009) explored the interpretive processes involved in analysing qualitative data through a longitudinal study on the evolution of management accounting practices.

As an iterative process that involves adaptation and learning over time, sensemaking encourages individuals to engage with new information or experiences proactively (Giuliani, 2016). This process enables them to refine their knowledge and interpretations, incorporating new insights and feedback into their understanding of the world (Sandberg & Tsoukas, 2015). However, as Boland (1984) argues, sensemaking is inherently ambiguous and can only be comprehended in hindsight. It highly focuses on the process of constructing meaning (Zhang & Soergel, 2014), which limits its capacity to account for behaviours, reactions and subsequent reflection after initial understanding. These limitations have prompted the incorporation of phenomenology as a complementary concept in IAR.

Phenomenology, introduced by Husserl (1970), provides a philosophical framework for capturing consciousness and understanding how individuals make sense of the world. In the context of IAR, Schutz (1962) further advanced this idea by highlighting that social life is a coherent stream of lived experience, thus, this "stream of consciousness" aligns closely with phenomenology in understanding subjective experiences within a continuous social interaction.

Researchers also came to realise the importance of understanding interpretations from a phenomenological perspective, bringing studies such as understanding managers' interpretations of accounting texts and revealing auditors and auditees' satisfaction (Boland, 1993; Sigalingging et al., 2021). Moreover, Khan and Gupta (2023) utilised phenomenology to analyse social networks within the context of green accounting, while Dewi et al. (2022) applied a phenomenological perspective to examine household accounting practices. In a word, phenomenology provides a clear process for investigating individuals' lived experiences, combining both the "art and science" of interpretation (Ezzy, 2013, p.24) and the study of the essence of a phenomenon (Crotty, 1998). With the supplement of phenomenology, IAR will provide us with a better horizon of understanding the issues of by whom and in what ways the accounting information is interpreted.

Building on insights from social science literature, IAR has increasingly been used to facilitate "critical" interventions with an interpretive underpinning (Arrington & Francis, 1989, 1993; Lehman, 2019). While IAR transcends the mere documentation of subjective meanings, its core remains an interactive and transformational process focused on understanding and interpreting socially constructed meanings (Sword, 1999). This paradigm has allowed accounting studies to move beyond the traditional objective analysis of decision-making information quality and content (Chen et al., 2015) toward addressing a wider array of contemporary issues, such as sustainability (Chen et al., 2023; Tregidga et al., 2014).

Today, as accounting increasingly incorporates pressing social and environmental issues, the importance of further advancing IAR in accounting cannot be overstated. The interpretative research genre has evolved into a substantial and vibrant field, enriched by a diverse array of theories, methodologies, and approaches (Lukka & Modell, 2017). Given the inherently interpretive nature of human existence, where meaning is continually derived from daily interactions and activities (Boland, 1993), developing IAR offers a critical pathway for accounting research to engage meaningfully with the complex, socially constructed realities that shape modern commerce and society.

2.2 From Using Accounting Information to Users of Accounting Information

There is considerable discussion regarding the function of accounting in contemporary commerce and society. Accounting has primarily been viewed as a tool for providing "useful information" (Young, 2006) to users, facilitating decision-making and performance evaluation (Eierle & Schultze, 2013). In recent years, accounting has been widely recognised as an information system designed to collect, record, store and communicate high-quality information to decision-makers (Snavely, 1967). Through such a process, accounting information is primarily used to produce valuable insights for users to make decisions (Mock, 1971). Aligned with this overarching purpose, the *use* of accounting information addresses diverse user needs, giving rise to various research topics such as corporate governance, performance management, investment analysis and knowledge development (Bushman & Smith, 2001; Danos et al., 1989; Downie, 2010; Hall, 2010; Holmes & Nicholls, 1988). Regarding rich research on the *use* of accounting information, this section seeks to first make a detailed exploration of how accounting information has been used in both financial and non-financial contexts. Subsequently, this section will then shift to a discussion on the users of accounting information.

Financial accounting information pertains to data and reports produced through corporate accounting and reporting systems, which are primarily intended for external reporting purposes, providing stakeholders such as investors, creditors, regulators, and analysts with an overview of a company's financial performance and position (Bushman & Smith, 2001). Corresponding to the demand of the capitalist system, a consistent and trustworthy stream of financial accounting information holds

essential significance in making well-informed decisions, enhances transparency and accountability, supports regulatory compliance and enables stakeholders to access the financial health and performance of companies (O'Regan, 2015). With its enduring significance, rich discussions have been generated on the use of accounting information, especially in formulating financial strategies.

Studies on the use of financial accounting information can be broadly classified into three different distinct phases, representing inquiries in normative description and evaluation, interdisciplinary approach, and technological advancements. In the initial normative stage, researchers focus on documenting existing financial accounting practices, standards, and regulations and using empirical research to evaluate the effectiveness, efficiency, and fairness of accounting practices to examine related phenomena such as stock price, acquisition, executive compensation, performance evaluation and managerial decisions (Gamayuni & Dewi, 2018; Holmes & Nicholls, 1988, 1989; Lev & Ohlson, 1982; O'Regan, 2015).

Shortly afterward, with the influence of multiple disciplines such as psychology and sociology, researchers started to seek advanced understanding of financial accounting information such as investigating behavioural, biases, and other organisational factors or exploring topics in corporate governance and organisational behaviour (Ansari & Euske, 1987; Baker & Bettner, 1997; Danos et al., 1989; Lambert & Larcker, 1987). Furthermore, with the development of technology such as big data analytics and artificial intelligence, research is increasingly focused on exploring the collection, analysis, and utilisation of accounting data as well as their implications in financial reporting, auditing, and accounting information systems advancement (Abdallah, 2013; Safkaur et al., 2021).

Meanwhile, over the past two decades, a great trend shift has been witnessed in the increase of non-financial accounting information production (Arvidsson, 2011). Organisations produce a suite of extended performance-related information for external users, including information about sustainability, corporate social responsibility, ethical practices and corporate governance, which attracted people's attention to the significant role of the non-financial approach (Al-Shubiri et al., 2012; Bychkova et al., 2021; Christ et al., 2023; Schaper & Pollach, 2021; Tregidga et al., 2014). For example, Lin (2010) investigated the perceptions of both users and preparers of sustainability reports, aiming to evaluate their level of understanding towards the value and purpose of such disclosures. Similarly, Xiao and Shailer (2022) examined the factors influencing how users assess the credibility of sustainability reports.

Within the complex interplay of economic, social, technological, and regulatory influences, researchers are increasingly expanding their interest from exploring the use of dominant financial accounting information to the use of non-financial information (Baker & Bettner, 1997; Bushman & Smith, 2001; Danos et al., 1989; Lambert & Larcker, 1987). Non-financial accounting information was initially proposed as information related to company environmental, strategy, and management issues (AICPA,

1994; Tarquinio & Posadas, 2020), after continuing expansion, it has been generalised as a concept that provides insights into various non-monetary aspects of a company's activities and performance (Haller et al., 2017).

From operational data such as intangibles (Wyatt, 2008) to environmental issues (Dunk, 2005; Nikolaou & Evangelinos, 2012), sustainability reports (Tregidga et al., 2014), corporate social responsibility metrics (Al-Shubiri et al., 2012; Bychkova et al., 2021) and ethical practices such as statements on modern slavery (Christ et al., 2023; Schaper & Pollach, 2021), non-financial information is highly related to focal management accounting practices. Kurunmaki et al. (2003) extended the prior literature on health care to accounting information used in intensive care while others discussed the performance explanations of non-financial information in quality management (Aerts, 1994; Anderson & Sedatole, 1998; Broadbent, 1992). Furthermore, exploring the use of accounting information in communication and pedagogy also became a popular topic (Davison, 2011; Merkl-Davies & Brennan, 2017; Mitchell, 2002; Siriwardane & Durden, 2016). By providing a broader perspective on a company's performance and its impact on individuals, organisations, and societies, non-financial information presents close value relevance to financial information, which together improve companies' future transparency, accountability, and long-term sustainability (Amir & Lev, 1996; Simpson, 2010).

Despite extensive exploration of how accounting information is used, users of accounting information, as the subject of information utilisation, has also gained researchers' attention. Recognising the critical role of users, accounting research began to shift from the exploration on use of accounting information to the users themselves, emphasising the social implications of accounting as it relates to people (Bessieux-Ollier et al., 2023). This shift is particularly evident with the development of technology and the increased accessibility of information, which have empowered individuals to actively participate in social accountability, which has compelled organisations to address their social and environmental impacts more transparently, especially in their engagement with external users (Thomas et al., 2022). Information such as ESG disclosures (Cordazzo et al., 2020; Santamaria et al., 2021) and cyber security statements (Janvrin & Wang, 2022; Rosati & Lynn, 2021) are produced to better illustrate accounting's hidden capacity behind its creation and control force towards translating social realities into empowerment for individuals (Young, 2006).

However, as the voice of users is often referenced indirectly, the involvement of users in accounting research remains limited (Stenka & Jaworska, 2019). The existing literature on accounting users can be roughly categorised into two main perspectives: those examining accounting information users, such as financial statement users (Young, 2006) and accounting system users (Muda & Ade Afrina, 2019), and those discussing from the regulatory perspective, such as the role of users in the accounting standard-setting process (Eierle & Schultze, 2013).

In the context of accounting information systems and software, high user experience is always emphasised as a primary principle (Choe, 1998). Researchers have explored various aspects of user engagement, including users' satisfaction (Seddon & Yip, 1992), the effects of users' participation (Choe, 1998), and users' choice and behaviours (Bressler & Bressler, 2006), as metrics to evaluate the effectiveness and practicality of accounting systems. Concurrently, the needs and preferences of users are also recognised as essential considerations in the process of accounting standard-setting (Eierle & Schultze, 2013) and information production (van Helden & Reichard, 2019; Voinea & Dimitriu, 2014). However, the definition of "user" in current accounting literature remains inconsistent. Whether broadly defined by Choe (1998) as financial report users or specifically defined by Bressler and Bressler (2006) as entrepreneurs, there is a lack of consensus on the constitution of accounting information users.

As accounting is increasingly recognised as a social practice involving a wide array of participants, it is no longer solely viewed as "what accountants do" (Young, 2006). Instead, there is a growing emphasis on a broader spectrum of users with different backgrounds and levels of expertise in accounting knowledge. Following Young's critique of the disconnect between users and the selection of accounting practices, intense debates have emerged regarding the constitution of users in accounting information. Voinea and Dimitriu (2014) differentiated between users such as investors and other individuals seeking information from financial statements, while Eierle and Schultze (2013) highlighted the limited attention given to external users beyond investors. Additionally, van Helden (2016) subdivided the potential users of accounting information into more specific segments, including users of financial information and users of performance information, with a particular focus on politicians.

A noteworthy trend in recent research is the growing focus on users who lack expertise in accounting. These individuals, including those with limited financial literacy, disabilities, or those disproportionately affected by sensitive events, are particularly vulnerable in their ability to interpret and utilise accounting information effectively (Duff & Ferguson, 2011). This shift marks a departure from traditional accounting research, which predominantly concentrated on professional users, and underscores the need to reconsider the role of expertise in understanding and using accounting information.

2.3 Reformulating the Role of Expertise in Accounting Users

Accounting, as a professional activity, typically requires a certain level of expertise from its users (Power, 1997). Given historically understood as "what accountants do" (Young, 2006), accounting information use has led to a strong focus on accredited professional users, such as accountants, auditors, and managers (Himick et al., 2016). For example, Seddon and Yip (1992) explored the empirical evaluation of internal professionals, while Kochetova and Salterio (2003) examined professional firm

users such as managers, auditors, and investors. Later, as Choe (1998) broadened the scope of accounting information users, the concept of professional users seemed to be expanded to encompass all participants, both internal and external, in the accounting process with the required domain of expertise (Himick et al., 2016). This expansion aligns with the notion that professional users, by leveraging their expertise, could improve judgment and decision performance on accounting tasks, despite occasional differences in preferences (Kochetova & Salterio, 2003; Thottoli, 2020).

The role of expertise in accounting is also central to improving the quality of accounting practices (Garcia-Sanchez et al., 2017). Accounting research has historically relied on expert knowledge to ensure accuracy, reliability, and transparency in financial reporting (Sundby, 1997). Existing research has shown that accounting expertise can enhance audit quality (Dhaliwal et al., 2010) and mitigate the adverse effects posed by complex financial reports (Chychyla et al., 2019). However, similar to expert judgment in legal contexts, there is a tendency for individuals to be "overawed by experts' credentials" in the accounting profession (Sundby, 1997). Experts often act as a form of "delegated authority" (Collins & Evans, 2019), raising concerns about their transparency and accountability.

Earlier studies predominantly portrayed rational economic decision-makers as the primary users of accounting information, but this perspective overlooks the internal contradiction and unreliability rooted in accounting users (Young, 2006). Therefore, Young argues that the potential users of accounting information are rather multiple, conflicting, inconsistent, and uneducated. This has led to a growing call for accounting research on individuals who lack professional expertise or credentials. In response to this, scholars such as Himick et al. (2016) specified the concept of users in accounting as professionals and layman users, highlighting the importance of expertise in using and understanding accounting information.

Current accounting research has well explored the nature and implications of expertise, such as Sundby's (1997) work on expert testimony. However, while studies on professional users of accounting are well-established, they have largely overlooked the diversity of user positions (Stenka & Jaworska, 2019), with little exploration on users who lack specialised knowledge or expertise. The reliance on professional expertise in accounting research has prompted critical questions about the type of expertise that is truly useful for decision-making in contemporary accounting practices and underscores the need to reconsider and expand the role of expertise in accounting to address the varied needs of all users (Collins & Evans, 2019).

Given the different levels of professionalism in accounting information users, the concept of *lay expert* then originally emerged in the field of medicine, which refers to people who have acquired knowledge in a particular technical domain, but without credentialing (Kerr et al., 1998). This concept has since been extended to broader social and ethical domains to explore how boundaries around expertise are constructed and maintained (Prior, 2003). Later on, *lay expert* has been applied within the sociology of

health and illness to examine evolving representations of lay understanding in medical contexts. Subsequent research also investigated the role of patients and public as holders of "experiential expertise", recognising their contributions to health knowledge and participation in medical and health research, such as in the context of cancer studies (Thompson et al., 2012).

In the accounting context, the term *lay expert* is used to describe citizens who gain expertise in a technical domain without formal credentials (Himick et al., 2016). van Helden and Reichard (2019) expanded on this by categorising accounting information users into three groups: professional users (e.g., accountants, auditors), layman users (e.g., politicians, public sector managers, or employees), and hybrid group users. Compared to professional users, lay experts lack formal training and professional experience, which leads to their motivations for use being more driven by personal interests and experiences (Himick et al., 2016). However, research on lay experts has primarily focused on how they mimic experts and make relevant decisions (Himick et al., 2016; van Helden & Reichard, 2019), leaving the distinctions between experts and lay users somewhat ambiguous.

Lay users, who possess less expertise than lay experts, then attract the attention of researchers (van Helden & Reichard, 2019). While these individuals may have a general understanding of accounting concepts, they often face challenges in comprehending and interpreting complex financial information (Himick et al., 2016). Unlike professional users who prefer concise and lucid information, with lower "digestibility", lay users run the risk of becoming overwhelmed by technical details and thus are more conservative and short-sighted to risk in accounting information use (Govindarajan, 2011; van Helden & Reichard, 2019). Regarding the inherent vulnerability of lay individuals, this study focuses specifically on their engagement with DBN as a specific form of accounting information.

2.4 DBNs as Accounting Information

Over the past three decades, the scope of accounting has witnessed its rapid expansion in different contexts, including changes in business practices, advancements in technology, globalization, and evolving regulatory requirements (Andrew et al., 2023; Bushman & Smith, 2001; Tregidga et al., 2014). Based on the evolvement of the accounting information environment, additional value was urged to be added for generating comprehensive insights into a company's operation (Brecht & Martin, 1996). Emerging approaches, such as sustainability, corporate social responsibility, big data, and cybersecurity came into researchers' eyes (Al-Shubiri et al., 2012; Andrew et al., 2023; Chen et al., 2023; Tregidga et al., 2014). Widely recognised as a social practice (Hopwood & Miller, 1994; Potter, 2005), accounting has expanded its scope to encompass a broader range of services and responsibilities beyond traditional financial reporting, reflecting the evolving demands and anticipations of stakeholders in today's business landscapes. Such evolvement of accounting definition has led to increased specialisation,

interdisciplinary collaboration, and opportunities for accountants to contribute to organisational success and sustainability.

Although the nature of accounting information experienced a variety of changes, some key characteristics were retained. Snavely (1967) proposed two main purposes of accounting information use as rendering accountability and supporting decision-making, whereas Smith & Smith (1971) outlined the primary objective of accounting as conveying economic information regarding business decisions and events to ensure optimal comprehension by users, aligning the message with economic actuality. Disclosure, as the fundamental and obligatory process in accounting operations, has historically served as a valuable supplement for providing pertinent and material information to stakeholders, enhancing their understanding of businesses to a broader extent (Dye, 2001). Through comprehensive disclosures, companies enhance stakeholder trust, facilitate efficient capital allocation, and contribute to the integrity and transparency of financial markets (Snavely, 1967).

Similar to the evolution of research on accounting information use, the examination of accounting information disclosure has also experienced an extensive journey (Lee & Tweedie, 1975). Although the Financial Accounting Standards Board (FASB) has given primary guidance on disclosure states which outlines the principles and requirements for disclosures that accompany the financial statements, many researchers have proposed their own divisions of disclosure. Some researchers tend to directly define disclosure information as economic transactions and performance reporting (Kanodia, 2007; Marston & Shrives, 1991). For example, Craig and Diga (1998) elucidated corporate annual reports as the main disclosed information. Moreover, as outlined by Edmans and Gabaix (2016), only tangible data (like earnings) can be disclosed, and disclosing such concrete information alters managers' investment incentives by shifting the balance between tangible and intangible information.

However, accounting does not exist in a vacuum but rather deeply interacts with relevant social context (Christensen, 2010). Hence, other disclosed information should also be included in consideration while making accounting practices. Core (2001) concluded disclosure of information as news in general, and afterwards, researchers such as Goldstein and Yang (2019) broadened the range of disclosure to encompass external public information and internal price data. Just as Stocken (2013) suggested, disclosure should depend on the features of the corporate environment, as a result, it is no longer limited to the prior definition of financial information but rather a broader agenda that involves non-financial information including environmental, social, and governance (ESG) factors, corporate social responsibility (CSR) endeavours, and other non-monetary performance metrics.

While numerous studies have acknowledged the significance of non-financial information in disclosures, their comprehension of such data remains ambiguous and contradictory. Simpson (2010) defined non-financial information as a performance measure whereas Arvidsson (2011) mentioned it as

information related to intangible assets such as research and development (R&D), corporate social responsibility (CSR), and employee-related information. Particularly, in this era dominated by data, the swift rise of cyber threats and data breach incidents has captured the attention of the media, consumers, and regulatory bodies (Rosati & Lynn, 2021), driving organisations with growing pressure to disclose incidents of data security breaches promptly. However, few papers have noticed this problem, leading to the status quo that current studies on disclosures are still not keeping pace with changes in the business world (Wallman, 1995).

Given its significant impact, many countries stipulated regulations on organisations notifying affected individuals and related government departments after material cyber security incidents, such as the Australian *Privacy Act 1988 (Cth)*. Served as a new form of disclosure, DBNs provide stakeholders with crucial insights into the organisation's cybersecurity posture and risk management practices, thus, it could enhance corporate accountability and offer stakeholders informative disclosures related to economic and business performance issues (Andrew et al., 2023; Chen et al., 2023; Juma'h & Alnsour, 2020). Empirically, DBNs can also support individuals' entitlement to information and empower stakeholders to take appropriate actions to protect their interests (Jackson et al., 2019; Karyda & Mitrou, 2016). By promptly disclosing data breaches, organisations demonstrate their commitment to transparency and accountability, enabling stakeholders to evaluate the potential consequences of the breach on the organisation's operations, reputation, and financial position (Thomas et al., 2022). Similar to corporate disclosures such as environmental and sustainability reports, which emphasise societal issues, DBNs address critical concerns by fostering accountability and supporting decision-making (Snavely, 1967). Therefore, despite lacking a standard framework (Andrew et al., 2023), DBNs are increasingly recognised as a new form of accounting information.

However, in extant research, there is a widely acknowledged lack of comprehensive theory regarding mandatory disclosures, leading to limited understanding and unresolved questions about how users interpret mainstream disclosures, let alone breach disclosures (Schipper, 2007). As a new form of disclosure aiming at informing individuals about the unauthorised access or compromise of their personal or sensitive information, the features of DBN determine that its main audience should be external users without effective information protection measures (Zou & Schaub, 2019). Among them, lay users who lack certain awareness and knowledge are particularly vulnerable in terms of implementing effective responses to mitigate their risks (van Helden & Reichard, 2019). Therefore, it is crucial to make further exploration of DBNs as they pertain to being included in the new domain of accounting practices and contribute to the broader implications of stakeholder engagement and corporate social responsibility.

2.5 Current Research on DBNs

In response to the growing frequency and severity of cybersecurity incidents, DBNs have emerged as an important topic of scholarly inquiry across multiple disciplines. To provide a comprehensive overview of the extant literature, this section critically reviews key studies on DBNs within both accounting and non-accounting domains, with the aim of synthesizing existing knowledge and identifying salient gaps for future research.

Within the accounting literature, a prominent area of focus is the financial impacts of DBNs on organisational decision-making, disclosure practices, and corporate governance (Ashraf, 2022; Rosati & Lynn, 2021; Thomas et al., 2022). A substantial body of research has investigated the external market consequences of DBNs, particular their effects on stock market performance and investor behaviour. For instance, Avery (2021) analysed both short-term and long-term financial impacts of DBNs and explored the negative impacts that data breach events lead to the organisation's profitability. Similarly, Huang and Wang (2021) discovered that the severity of the data breach incident correlates with its effect on the company's financial status and reputation, suggesting that timely disclosure can serve as an effective mitigation strategy to reduce the financial fallout from such incidents.

Building upon this body of research, Foerderer and Schuetz (2022) demonstrated that DBNs often result in decreased market valuations, largely driven by diminished investor confidence and heightened perceptions of organisational risk. Their study also underscores the strategic nature of DBN timing, illustrating how organisations may actively manage the timing and framing of disclosures to mitigate potential adverse market reactions. Collectively, studies on the financial impacts of DBNs highlight their role as strategic instruments that shape investor perceptions, influence market dynamics, and inform broader financial reporting practices.

Beyond financial implications, DBNs also raise ethical and reputational concerns for organisations. Schwartz and Janger (2006) highlighted the role of notifications in mitigating post-incident harm and called for more comprehensive legal frameworks to address deficiencies in current disclosure regimes. Kuipers and Schonheit (2022) further compared various after-crisis initiatives and demonstrated that timely and transparent disclosure in organisations can mitigate reputational damage and restore stakeholder trust following a data breach.

Another critical strand of research focuses on the role of DBNs research in improving organisational transparency and accountability. Researchers such as Andrew et al. (2023) explored the current regulations and features of data breach disclosures, proposed a mandatory disclosure framework to enhance organisational accountability and strived to make clearer routines for stakeholders to assess data risks. Relatedly, by illustrating the little reflection of notification practices (Thomas et al., 2022), researchers identified the enablers and barriers to making effective notification initiatives and thus tried

to propose relevant approaches for a new regulation paradigm (Andrew et al., 2023; Karyda & Mitrou, 2016).

Additionally, recent research also started investigating how DBNs affect stakeholder perceptions regarding organisational trustworthiness and competence in managing cybersecurity risks (Chen & Jai, 2021). Findings suggest that effective disclosure practices can contribute to raising cybersecurity awareness, facilitating information sharing among stakeholders, and promoting a broader culture of cyber resilience within organisations. This is further supported by Mayer et al. (2021), who evaluated the efficacy of DBN mechanisms in enhancing cybersecurity resilience and promoting organisational accountability.

As an emerging area of inquiry, research on DBNs, both within and outside the accounting domain, frequently converges around common themes such as corporate governance, risk management, and shareholder response following cybersecurity incidents. For example, management research has also examined organisational reactions to data breaches, offering complementary insights to those found in accounting studies. Sen and Borle (2015), for instance, investigated the organisational drivers and barriers to effective DBN implementation, shedding light on firms' underlying motivations and decision-making processes in the aftermath of cybersecurity incidents. Similarly, Blakely et al. (2022) explored how notification practices contribute to improving internal control systems, implying that extant notification efforts often fall short of meaningfully strengthening organisational risk management.

In addition to these shared thematic concerns, non-accounting literature also placed extensive emphasis on the legal and regulatory dimensions of DBNs. Scholars have examined the evolution and divergence of DBN laws and regulatory frameworks across jurisdictions, highlighting variations in disclosure requirements, enforcement mechanisms, and the broader implications for organisational compliance (Daly, 2018; Nieuwesteeg & Faure, 2018). These analyses offer critical perspectives on the legal and institutional contexts that shape DBN practices. Furthermore, relevant studies also considered how firm-specific factors, including firm size, industry characteristics, and internal governance mechanisms, affect the adoption and effectiveness of DBNs (Albeshri & Thayananthan, 2018), Collectively, the non-accounting literature underscores the multidimensional nature of DBNs, positioning them as instruments of organisational governance, strategic risk management, and regulatory compliance.

Overall, existing research on DBNs has provided valuable insights into financial impacts, organisational accountability, regulatory landscape, and the effectiveness of notification mechanisms. However, the review on current research also reveals considerable overlap, with most of the studies addressing similar themes mainly from the organisational perspective. While some research has begun to examine individual perspectives, such as Gibson and Harfield's (2023) research on potential financial, medical and moral harms to data subjects, which initiated discussion on the efficacy of DBNs, there remains a significant gap in understanding how affected individuals perceive and interpret DBNs. This represents

a critical research gap, given that the effectiveness of DBNs ultimately depends on how they are understood and acted upon by affected parties. Accordingly, the following section will focus on individuals as recipients of DBNs and refine the research scope in light of the proposed research question.

2.6 Lay Users of DBNs

As an emerging form of accounting information, DBNs are utilised by individuals in different ways, influenced by their varying backgrounds. However, their effective understanding and use of DBNs are often impeded by a lack of relevant professional knowledge, resulting in unnecessary misunderstanding, panic, and potential secondary damage (Sundby, 1997). Given such limitations, this research focuses specifically on lay individuals – those who lack expertise in cybersecurity and are particularly vulnerable to the effects of sensitive breach incidents.

Nevertheless, the boundary between experts and lay users in the context of data breaches remains ambiguous (Himick et al., 2016; van Helden & Reichard, 2019), necessitating a clearer definition of "lay users" within the realm of data breach disclosures. The distinction between experts and lay individuals revolves around two key aspects: professional credentials and relevant experience (Cheng et al., 2017). Notably, "relevant experience" does not merely refer to initial personal breach experience, as subsequent breaches may still cause significant harm to lay individuals. Instead, it should be understood as professional working or training experience in cybersecurity.

Building on Collins and Evans' (2019) discussion on "rethinking expertise" from an outsider's perspective, both formal credentials and experience must be considered in defining expertise. Those recognised as experts in data breaches should possess formal training in cybersecurity and hold relevant cybersecurity certifications such as CISSP (Certified Information Systems Security Professional) or CISA (Certified Information Systems Auditor). These certifications represent a high level of professional expertise, or alternatively, significant professional working experience in cybersecurity or breach-related fields (The University of Adelaide, 2024).

Accordingly, in the context of this research, lay users of DBNs are defined as individuals lacking formal cybersecurity certifications, professional working and training experience, or supervisory roles related to information security (Whitler & Farris, 2017). Understanding how DBNs are used by these lay users is critical for organisations managing data breach incidents, as it influences both the rebuilding of organisational reputation and the effectiveness of organisations' overall crisis response (Cheng et al., 2017). Additionally, it provides valuable insights into how control mechanisms in data breach response are linked to broader accounting practices, influencing organisational processes such as labour relations and decision-making (Guo et al., 2023).

In recent years, there has been a growing body of research drawing on lay individuals. For instance, Himick et al. (2016) advocated broader participation by lay citizens in accounting standard-setting processes. They expanded the concept of lay individuals to both lay citizens and lay experts, questioning whether the latter often adopt or mimic the argumentative styles of experts rather than being mediators between lay citizens and professional experts. Furthermore, Ouda and Klischewski (2019) and van Helden (2016) called for increasing attention to lay users such as politicians, public sector managers, and employees, which highlighted the need for future research on vulnerable individual users who lack professional accounting knowledge or expertise. Despite this advancement, current research still struggles to fully capture the complexity and vulnerability of lay individuals in interpreting breach-related information. This gap underscores the critical need for further research that incorporates the perspectives of lay individuals, particularly in the context of their use and understanding of DBNs.

2.7 Applying Ellsberg's Ambiguity Aversion Theory in Lay Users' Interpretation of DBNs

As individual decision-makers, choices made under emergency situations, such as data breaches, are invariably accompanied by both risk and uncertainty (Al-Najjar & Weinstein, 2009). These two concepts are grounded in beliefs about probabilities. However, as Knight (1921) clarified, there is a crucial distinction between situations of probabilistic and non-probabilistic beliefs (Machina & Siniscalchi, 2014). According to LeRoy and Singell (1987), Knight's theory defines *risk* as situations where probability can be determined or theoretically deduced, while *uncertainty* refers to situations where such probabilities cannot be measured. Both terms, however, originally referred to objective probabilities in the standard sense.

Meanwhile, Knight (1921) also noted that under uncertainty, individuals tend to form subjective probabilities. In other words, an individual may assign a subjective "estimate" to the value of an opinion and "feel" as though it presents a probabilistic outcome, despite the absence of concrete evidence (Machina & Siniscalchi, 2014). This uncertainty, rooted in a lack of knowledge or incomplete information, leads to varying preferences and behaviours across individuals. As a response to the inadequacy of objective probabilities, Ramsey (1926) introduced the principle of expectation, which derives subjective probabilities based on personal beliefs about propositions or events. Despite these conceptual advancements, the clarification of uncertainty and its influence on individual preferences remains a complex and underdeveloped area (Machina & Siniscalchi, 2014).

To further address this gap, scholars such as Daniel Ellsberg began investigating *ambiguity* as a distinct form of uncertainty. As an ambiguous term itself (Weber & Tan, 2012), ambiguity encompasses both ambiguity over probabilities and ambiguity over outcomes (Camerer & Weber, 1992). It indicates the absence of critical information that complicates decision-making under uncertain conditions (Machina

& Siniscalchi, 2014). According to Ellsberg's (1961) definition, ambiguity arises from "the nature of one's information concerning the relative likelihood of events", with its scope determined by the quantity, type, reliability, and 'unanimity' of information available, ultimately influencing the level of "confidence" in estimating relative probabilities. In this sense, ambiguity reflects the limitations of classical decision theory, which assumes that uncertain beliefs can be fully represented by probabilities, and highlights the paradox inherent within rational choice models, wherein ambiguity challenges the traditional axioms of rationality and the application of standard decision-making models under uncertainty (Machina & Siniscalchi, 2014).

In ambiguous situations, it is believed that individuals' actual beliefs often deviate from rational expectations (Keynes, 2013). As a result, decision-making behaviour is not solely governed by mathematical expectations of utility or value but rather the "degrees of belief" (Ramsey, 1926). This paradox was most notably demonstrated by Ellsberg (1961) in his famous *Three-Color Ellsberg Paradox* experiment, in which participants were presented with two sets of bets based on the colour of a ball drawn from an urn containing 90 balls. The experiment revealed that individuals seem to prefer the known probability bet to the unknown probability, which is described by Ellsberg (1961) as *ambiguity aversion*. This preference for situations with known probabilities over ambiguous bets underscores individuals' discomfort with ambiguity.

Ellsberg's findings on ambiguity aversion were then widely confirmed through various subsequent experiments conducted among business owners, trade union leaders, managers, and executives, all of which demonstrated similar preferences for avoiding ambiguity (Becker & Brownson, 1964; Curley & Yates, 1989; MacCrimmon, 1968; Slovic & Tversky, 1974). Fox and Tversky (1995) later reinforced this observation by showing that decision-makers were ambiguity-averse on vaguer options than on explicit ones when comparing two options jointly. Moreover, Du and Budescu (2005) revealed that individuals were even willing to pay a premium to reduce ambiguity associated with outcome uncertainty, as opposed to probability uncertainty, further illustrating the profound effect ambiguity aversion has on individual decision-making.

A deeper understanding of individuals' preferences for information ambiguity, and their willingness to allocate resources and make decisions is also particularly relevant to disclosure policies (Du & Budescu, 2005). In ambiguous situations, such as the aftermath of a data breach, individuals are likely to prefer clearer, more certain information to guide their decision-making (Al-Najjar & Weinstein, 2009). In addition, more transparent disclosures could guide standard-setters in enhancing the inclusion of forward-looking and risk-related information in financial reporting (Hodder et al., 2001). Consequently, the ambiguity aversion perception further implies individuals' interpretation of data breach disclosures, which are often the most direct approach of information available to help them understand the nature of the breach and to take appropriate remedial actions.

As data breaches introduce various forms of uncertainty for affected individuals (Tchernykh et al., 2017), in contrast to professional users of accounting information who may apply their professional knowledge to make relatively rational decisions (Collier, 2015), lay users often exhibit multiple, conflicting, and inconsistent responses due to their lack of specialised expertise (Young, 2006). This limitation on acquiring additional information and limited experiences makes it more challenging for lay individuals to instantly understand data breach disclosures and make timely decisions (Himick et al., 2016). Unfortunately, the existing literature fails to specifically explore lay individuals' interpretation of DBNs under the ambiguous situation after data breaches. Facing such necessity, this study proposes the overarching research question: *Faced with a data breach incident, in what ways do lay individuals attempt to interpret organisational data breach disclosures they receive?* Following the question, this study aims to examine the breach experiences of lay individuals, amplify their often-overlooked voices and address their unique interpretative challenges in understanding DBNs.

In conclusion, this chapter has provided a comprehensive overview of the evolution of accounting research, transitioning from a focus on the use of information to the users of information. By demonstrating DBNs as a novel form of accounting information, this chapter underscores the pivotal role that DBNs play in shaping organisational reputation, transparency, accountability, and stakeholder trust (Andrew et al., 2023). Another key insight from the literature is the limited attention given to lay individuals, who lack specialised expertise and relevant experience, as a critical but often overlooked group of accounting information users compared to their professional counterparts. Therefore, drawing on the calls for "rethinking expertise", more detailed information about lay individuals' perceptions of DBNs, especially their preference under ambiguity, is required to explore. By introducing Ellsberg's (1961) ambiguity aversion theory, this chapter ultimately provides a theoretical framework to narrow down the research focus, concentrating on lay individuals' interpretations of and responses to DBNs. This framework lays the foundation for a deeper exploration of how to make current DBNs more effective and transparent.

CHAPTER 3 – METHODOLOGY

3.0 Introduction

The prior chapters established the theoretical framework for this study, highlighting the limited attention given to lay users' perspectives on understanding disclosed information, particularly in the context of data breaches. While some scholars have acknowledged the importance of considering non-expert users in accounting research (Himick et al., 2016; van Helden & Reichard, 2019), there remains a significant gap in understanding how these individuals interpret and respond to data breach notifications. To address such a gap, this study is designed to use semi-structured interviews as the primary method for collecting qualitative data.

This chapter begins with an introduction to the context of the Latitude Financial data breach and then transitions to the formal interview processes, which were outlined in two stages: the first stage employs phenomenological research with an interview method named micro-phenomenology, to gather detailed first-person accounts and subjective interpretations (Petitmengin, 2006) from an inductive approach. The second stage builds on insights from Phase One interviews with qualitative experimental interviews exploring the embedded preference of breached individuals from a deductive perspective.

More specifically, in phenomenological research, considering the challenges of conducting interviews, a pilot study was conducted as a preparatory measure for training, including a nuanced explanation of the micro-phenomenology method, which helped people better understand the processes of conducting micro-phenomenological interviews and refine the initial interview guidelines. Subsequently, this study follows a step-by-step illustration of Phase one interviews, including the recruitment process, interview structure, and relevant data collection techniques. Finally, the chapter concludes with a discussion of ethical considerations, including the process of ethics approval in each stage. Together, this chapter provides a comprehensive overview of the research approaches and methodologies, establishing the methodological foundation for analysing lay users' interpretations of DBNs.

3.1 Case Context: Latitude Financial Data Breach

Before implementing specific research methods, it is crucial to understand the context of the case selected for this study. This section provides a comprehensive overview of the Latitude Financial data breach, which serves as the primary case for my interview.

After deciding to focus on recent Australian data breach cases, I reviewed multiple high-impact incidents and identified a growing concern among individuals regarding financial harm. Compared to general data breaches, those involving financial institutions tend to elicit heightened sensitivity from

the public due to the potential for severe financial consequences. Hence, the Latitude Financial case was selected due to its recent and high-profile nature, which highlighted critical issues in data breach management and public communication.

Latitude Financial is a leading provider of sales finance and consumer lending services in Australia (Latitude Financial, 2023). After experiencing a significant data breach that affected approximately 14 million people, this incident is recognised as one of the most significant Australian data breaches in recent years. The latitude breach involved a sensitive personal information leak and attracted substantial media coverage. With its high-profile impact, the Latitude breach serves as an ideal case to explore lay users' interpretations, expectations, and concerns in response to DBNs. The subsequent sections offer a detailed account of the case, including a description of the incident, its aftermath, and Latitude's actions. Moreover, a detailed timeline of the Latitude Financial data breach and later responses has also been presented (see Appendix B).

3.1.1 What happened?

On 15 March 2023, Latitude Financial Services (briefly described as Latitude hereinafter), a prominent sales finance and consumer lending provider, disclosed a major cyber incident resulting in the theft of its customers' personal information (Latitude Financial, 2023). According to the Latitude report (2023), a malicious cyber-attacker used compromised login credentials, acquired from a third party, to infiltrate Latitude's network and obtain personal information in Latitude's database.

3.1.2 Cause of the breach

According to the Guardian (2023), the Latitude incident directly resulted in the leakage of approximately 7.9 million driver's license numbers, including name, address, telephone, and date of birth. Additionally, this incident also led to the loss of around 103,000 copies of driver's licenses or passports, approximately 53,000 passport numbers, and other personal details, including fewer than 100 monthly account statements; approximately 900,000 income and expense records were accessed to evaluate loan applications, along with around 308,000 bank account numbers (excluding passwords) for fund disbursement purposes and approximately 143,000 credit card or credit card account numbers (excluding expiration dates or 3-digit CVC) were accessed for debt consolidation of customers and applicants in Australia and New Zealand (Barrett, 2023).

3.1.3 Response of Latitude Financial

According to the OAIC statement (2023a), Latitude promptly notified relevant authorities and law enforcement bodies, including the Australian Cyber Security Centre (ACSC) and the Australian Federal Police (AFP). They also enlisted the support of external cybersecurity experts. On 16 March 2023, they informed the Office of the Australian Information Commissioner (OAIC) and the New Zealand Office of the Privacy Commissioner (OPC) about the incident and provided ongoing updates (OAIC, 2023b). Meanwhile, Latitude also claimed to notify affected customers by data breach email or letter, including compromised information and the support Latitude provided (Latitude Financial, 2023).

3.1.4 Subsequent effect of the incident

The Latitude incident is one of the major cyberattacks that occurred in Australia in 2023. According to *The Guardian*, the incident was later revealed to have affected 14 million customers, which is far worse than initially reported (Barrett, 2023). Besides, Latitude vowed not to pay ransom to hackers since they detected this would not result in further harm and would only encourage similar incidents. Soon afterwards, Latitude's share experienced a decline of more than 3% as traders considered the possible financial and reputational costs to the company (Barrett, 2023). This breach raised inquiries into companies' data storage and the phenomenon that many businesses keep on retaining old customer records.

As the impact of data breaches in Australia becomes increasingly severe, public awareness of breaches has also risen. According to the Australian Community Attitudes to Privacy Survey (OAIC, 2023a), 74% of Australians now view data breaches as a major privacy risk, with a 13% increase since 2020. Additionally, 62% of Australians consider the protection of their personal information a major life concern. However, the survey also revealed that while 82% of Australians are motivated to take action to protect their personal data, 57% remain unsure about the steps to take. Only 32% of Australians feel in control of their data privacy, and 84% desire greater control over the collection and use of their personal information.

All the above statistics highlight a significant gap in understanding how affected individuals perceive, interpret, and respond to breaches, leaving affected individuals feeling especially vulnerable and uncertain in the aftermath of breaches (Mayer et al., 2021). To address these gaps, this study intends to employ phenomenological research to capture nuanced, first-person interpretations and examine how lay individuals experience and react to a real-life data breach. The following sections detail the methodology and rationale for using multiple techniques to gain insights into lay users' interpretations.

3.2 Phenomenological Research

Building on an understanding of the current landscape of data breaches in Australia and their impact on individuals, the overall interview process for this study is divided into two phases: inductive phenomenological research and deductive experimental research. This section mainly focuses on the phenomenological methods employed in the pilot study and Phase One interviews. First, it explains the rationale behind choosing micro-phenomenology as the primary methodology, highlighting its relevance for capturing participants' conscious experiences and interpretations. Additionally, this section offers a step-by-step explanation of how the micro-phenomenological interviews were conducted, including the recruitment process, interview structure, and data collection techniques.

As one of the most significant and influential philosophical movements that emerged in the twentieth century, phenomenology opened up a new field of exploring experiences and acts of consciousness (Detmer, 2013; Husserl, 2012). With rigorous scrutiny of the nature of human existence (Koopman, 2018), phenomenology offers a framework for understanding real events by closely observing certain phenomena or engaging directly with individuals' experiences (Ridwan et al., 2021). It seeks to explain human consciousness by bracketing presuppositions about the phenomenon, thereby preserving the richness and complexity of individual experience (Karlsson, 1993; Lucas, 2000). Being a "science derived from experience", phenomenology considers experience as the primary "source" of human consciousness, aiming to investigate lived experiences as they are subjectively encountered (Koopman, 2018), which allows researchers to access the essential qualities of consciousness and maintain the integrity of individuals' lived experiences.

With the development of phenomenology theory, two primary approaches emerged: transcendental and hermeneutic, each representing a different account of human experiences (Neubauer et al., 2019). Transcendental phenomenology, grounded in Husserl's (1970) work, aims to understand experiences from an objective standpoint, employing a descriptive procedure that "brackets" the essence of experience without any bias from the researchers (Husserl, 1970). This approach seeks to capture the pure structure of consciousness as it presents itself, focusing on universal elements within experiences.

In contrast, hermeneutic phenomenology is rooted in interpretation, emphasising individuals' narratives to uncover meanings embedded within lived experiences and phenomena (Husserl, 1970; Neubauer et al., 2019). Influenced by Heidegger's (1962) argument that understanding is situated within cultural, historical, and social contexts, hermeneutic phenomenology draws on people's "lifeworld" to interpret certain phenomena. In both approaches of phenomenological examination, researchers seek to understand the essence or structure of a phenomenon as it appears in the lived experiences of individuals, which involves deep exploration and rich description suspending preconceptions and biases (Petitmengin, 2006).

Under the complex and changing social contexts, phenomenology offers another alternative to research methods (De Villiers et al., 2019; Maulana et al., 2022). With its richness of exploring individuals' experiences, phenomenology has been initially used in fields such as psychology and cognitive science. It enables researchers to investigate both reflective and unreflective aspects of participants' "lifeworld", uncovering their natural attitudes, such as values and norms, as well as their phenomenological attitudes shaped by immediate interactions with the surrounding environment (Koopman, 2018). Recognising these strengths, scholars across various disciplines, such as education, have embraced phenomenology as a valuable approach for examining individual experience, especially within qualitative research. For instance, Lucas (2000) applied phenomenological methods to study students' experiences within accounting curricula through qualitative interviews.

More recently, phenomenology has gained prominence in accounting research, which increasingly emphasises the social context and human experience underlying accounting practices. Dewi et al. (2022) utilised a phenomenological approach to capture shared life experiences related to household accounting, while Dianati Deilami and Qanit (2022) explored accounting practices in Afghanistan through a phenomenological perspective. Such studies underscore phenomenology's effectiveness in understanding human experience and interpreting the underlying rationale of certain phenomena, especially in qualitative research.

As experience is a complex interplay of events that contains both external data and inherent assumptions, states of awareness and conditions of existence are deeply embedded in consciousness (Koopman, 2018). Given that interpretation involves an empirical understanding shaped by diverse subjective experiences, a phenomenological approach allows for an in-depth exploration of the varied contexts influencing the comprehension of accounting-related information. Therefore, this research, which aims to understand how lay individuals interpret DBNs, finds phenomenology a particularly fitting methodology to unveil the embedded social dimensions of experience. To systematically and rigorously advance the study of first-person experiences and interpretations of data breaches, micro-phenomenology, as a specialised branch of phenomenology methods known for its structured interview techniques and detailed phenomenological analysis, especially effective for untrained participants (Valenzuela-Moguillansky & Vásquez-Rosati, 2019), were employed in this study. The next section will further elaborate on the concept of micro-phenomenology and explain its suitability for my study.

3.2.1 Micro-phenomenology

The concept of micro-phenomenology was introduced by a French researcher named Claire Petitmengin initially as a psychological method designed to explore and document detailed first-person experiences. Being a rich and systematic research method, micro-phenomenology provides rigorous analysis procedures, unfolding specific first-person experiences through an iterative approach (Petitmengin et al., 2019a). Unlike traditional phenomenological approaches, micro-phenomenology emphasises human experience through a cognitive paradigm shift, analysing subjective experience from a micro-level perspective (Valenzuela-Moguillansky & Vásquez-Rosati, 2019). This makes micro-phenomenology a powerful method for obtaining and analysing detailed descriptions within implicit contexts.

As demonstrated previously, in accounting research, little attention has been given to examining how affected individuals, particularly lay individuals, use and interpret disclosed information, especially in the context of data breaches. To address this gap, it is essential to begin with a thorough description of participants' experiences, capturing the nuances of their interpretative processes. Such an approach enables a deeper understanding of their interactions with disclosed information and the underlying dynamics of their interpretations. However, given that my focused participants are largely lay to data breach knowledge, eliciting their subjective experiences and guiding them to articulate these experiences in detail presents a challenge (Petitmengin, 2006). Traditional phenomenological interviews may fall short in assisting participants to access and describe their nuanced experiences effectively. Micro-phenomenology offers a solution to these challenges by providing structured interview techniques that guide participants in exploring and articulating their subjective experiences in detail.

In the following sections, further elaboration will be drawn on the principles of micro-phenomenology, review prior work in the field, introduce key concepts central to micro-phenomenology and outline how this approach will be applied in my study.

3.2.2 What is micro-phenomenology?

Micro-phenomenology, rooted in the *entretien d'explicitation* (interview for explicitation) which was developed by Pierre Vermersch in 1994, was further advanced by Claire Petitmengin (2006) in cognitive science to study subjective experiences in precise detail. Building on Husserl's transcendental phenomenology and Gadamer's hermeneutics phenomenology (1979), micro-phenomenology goes further in exploring and understanding an individual's subjective experiences in great detail

(Petitmengin, 2006). It involves conducting in-depth interviews and analysis to uncover the subtle nuances, temporal aspects, and structure of conscious experience, providing insights into the richness of human perception and cognition. This approach enables interviewees, even without formal training, to recognise, evoke and describe their lived experiences within a specific period (Petitmengin, 2006) and make further analysis of the generic structure of these experiences (Petitmengin et al., 2019a).

The micro-phenomenological interview uses a rigorous structure to guide participants toward recalling specific experiences, moving beyond theoretical or abstract responses to uncover authentic lived experiences. This process shifts participants' focus from immediate perception to reflective awareness, thereby unfolding nuanced aspects of cognition (Petitmengin, 2021). As a methodological innovation, micro-phenomenology is designed to systematically and rigorously examine the procedural dimensions of experience, with an epistemological framework that enhances both the authenticity and reliability of the data collected (Valenzuela-Moguillansky & Vásquez-Rosati, 2019). To provide a comprehensive understanding of micro-phenomenology, the following sections will explore its interview and analysis methods respectively, highlighting how these tools capture the intricacies of subjective experience.

3.2.3 Micro-phenomenological Interviews

Over a long period, empirical research is based solely on reproducible third-person data (Petitmengin, 2006), which was collected by an external objective observer. Nevertheless, with indirect transmission, the third-person data lack the precision and depth of a direct description. If researchers aim to explore cognition and subjective experience, they must expand beyond external data and consider the internal subjective dimension (Petitmengin, 2006). Therefore, micro-phenomenology was raised in response to the call for developing rigorous methods and specific kinds of expertise in terms of studies in subjective experience.

Nevertheless, capturing and describing consciousness is a tough process. As Petitmengin (2006) clarified, there are seven main difficulties in becoming aware of individuals' subjective experiences. The first difficulty is in stabilising attention, noting the quick dynamics of consciousness. With thoughts springing up, attention is hard to focus and nor do we be aware of this difficulty, which requires appropriate training and circumstances. The next two difficulties draw on the content of consciousness. On a given activity, people tend to concentrate more on the objective description of 'what' rather than 'how', addressing the issues that experience is hidden behind believed representations and easy to be absorbed by achieved results. Another two difficulties are the accuracy of description, pointing out the complex dimensions and the blurred definition of precision in describing an experience. The last two

difficulties focus on the accessing process, illustrating the uneasiness of getting real-time data and transforming it into a narrative.

Considering the above difficulties, eight techniques were proposed by Petitmengin (2006) to facilitate the micro-phenomenological interview process. The first one is called *stabilising attention*, which means using certain language skills such as *direct reference*, *regular reformulation,* and *context description* to maintain the interviewees' attention, lay down their burden, build rapport and bring them back from excursion. The second technique focuses on solving the prior *"what" to "how" question*. Interviewers should ask appropriate questions to help the interviewees turn their attention to the process of actions rather than the ultimate objective. Another question technique emphasises experience narrative, *shifting the description of general representation (theoretical knowledge) to a specific singular experience*. Besides, since the micro-phenomenology interview draws on evocation, interviewers must guide interviewees to *re-enact* or reflect on the experience, such as asking situational questions. Furthermore, micro-phenomenology also requires *containing different dimensions of experience*, such as emotional, visual, and non-verbal clues. As for the level of precision, two main dimensions- *synchronic* (non-temporal) and *diachronic* (temporal) - are highlighted to improve the depth of the description. In doing so, interviewers are required to ask "*content-free*" questions in order to avoid bias and stabilise the interviewees' attention to nuanced details. Last but not least, interviewers should also encourage the interviewees to find their own words and thus *provide a relaxed and trustful environment*.

Through certain prompts and questions, the large, unnoticed part of our experience will be triggered (Petitmengin, 2006). With its meticulous attention to the intricacies of first-person data, the micro-phenomenological interview offers a unique avenue for exploring and describing human consciousness with great precision (Heimann et al., 2023). It is an interview approach that pertains to unearthing the subtle and often overlooked aspects of interviewees' inner worlds, contributing to a deeper comprehension of their cognition and perception (Vermersch, 2012).

3.2.4 Micro-phenomenological Interview Analysis

According to Petitmengin (2021), similar to the interview method, the micro-phenomenological analysis method aims at unfolding experience with meticulous processes, therefore, its essential principle is to detect the structure of the experience through an iterative approach. Compared with traditional analysis methods, micro-phenomenology emphasises detailed data preparation and verbatim procedures for data cleaning. Subsequently, with specific top-down and bottom-up abstraction operations, the structural statements, particularly the temporal dynamics at micro-level are identified.

By doing such refinement, the reliability of the description is evaluated, and the hidden regularities of structures are detected and reorganised through disciplined access. Drawing the focus from the content of the experience to the generic structure, such processual criteria enable analysis procedures with high reproducibility, which also significantly reduce the bias from the interpretation by the researchers.

However, eliminating preconceptions is not an easy process, which requires rich experience and iterative unfolding. Just as Petitmengin et al. (2019b) mentioned, the structure only emerges gradually during the interview and is progressively identified in the analysis. As the structure unfolds, it constantly builds the awareness of the experience, and simultaneously, the analysis process enriches the researchers' understanding of questioning. Therefore, in micro-phenomenology, each interview has a crucial reflection on the subsequent one, and the interview protocol will be refined through an iterative process. In doing so, experience dimensions and questioning adjustments are explored through the heuristic abstraction operations and fine-grained understanding is completed in practice.

Overall, micro-phenomenology avoids the description of experience in general or in a depersonalised way and removes "satellite information" with pre-reflective theoretical knowledge, judgments, and biases, which bring people closer to the truth (Valenzuela-Moguillansky & Vásquez-Rosati, 2019; Vermersch, 2012). With rigorous interview description and analysis, micro-phenomenology uncovers the underpinning structures and categories within a certain subjective experience without the researchers' preconceptions. Meanwhile, it should be noted that the passive interview and analysis process has several uncertainties (Petitmengin et al., 2019a). Therefore, calls for conducting a pilot study to better understand the implicit dimensions and interpretations of a certain event are also emerging.

3.2.5 Important Concepts in Micro-phenomenology

To build up a clearer picture of micro-phenomenology studies, understanding key concepts of conscious experience (such as *epoche, synchronic, and diachronic*) is integral. These concepts serve to retrieve, re-enact, or evoke the very phenomenological (first-person) dimensions of an experience, allowing for a nuanced exploration of subjective consciousness (Petitmengin et al., 2019a). Following the general overview provided above, this section mainly introduces these fundamental concepts in micro-phenomenology to establish a foundational framework for further analysis.

Epoche

Epoche, also known as phenomenological reduction or bracketing, initially originated from Husserl's phenomenological universe as a method that aims at removing one's preconceived beliefs, assumptions, and judgments about a phenomenon under investigation (Husserl, 1970, 2012). This suspension of preconceptions allows for a more direct and unfiltered exploration of the phenomenon as it is experienced by the individual (Bednall, 2006). In doing so, it approaches the phenomenon with a fresh, open, and non-judgmental attitude.

In the context of micro-phenomenology, researchers and participants engage in epoche as a way to temporarily "bracket" or put aside their interpretations and focus on the consciousness of objects to access the essence of phenomena (Bednall, 2006). As a critical aspect of phenomenological research, it helps ensure that the researchers do not impose their bias onto the phenomenon being studied, thus maintaining the fidelity of the first-person perspective (Smith, 2013). In summary, in micro-phenomenology, epoche involves the intentional suspension of preconceived notions and judgments to explore and describe the lived experience of individuals with greater clarity and depth.

Synchronic and Diachronic

The most typical terms acquired to deepen the micro-level description in phenomenological studies should be *synchronic* and *diachronic* (Petitmengin, 2006; Valenzuela-Moguillansky & Vásquez-Rosati, 2019). Synchronic dimension mainly refers to the characterisation of the experience at a particular moment, which aims to describe an instant landscape, whereas diachronic dimension refers to the temporal change of an experience, which examines the evolution of consciousness over a specific period and explores how experiences change, develop, or transform from one moment to the next (Petitmengin et al., 2019a).

In micro-phenomenological analysis, the synchronic dimension particularly helps to anchor the moments in an experience and therefore make forward or backward diachronic retrospections. Both dimensions are used to unfold structural and experiential statements through specialised and generalised unfolding processes, which help to explicitly highlight the overall architecture of experiences. These two complementary approaches allow researchers to capture the intricacies of lived experiences from both immediate and longitudinal perspectives, enriching their understanding of subjective phenomena.

Intersubjectivity

Another concept that is often mentioned in micro-phenomenology studies is intersubjectivity. It refers to the shared understanding or mutual recognition that arises through social interaction and

communication between individuals. Unlike subjective experience, which pertains to the individual's unique perspective, intersubjectivity emphasises the relational aspect of human experience, highlighting how meanings, beliefs, and emotions are co-constructed and negotiated within social contexts.

In the context of micro-phenomenology, intersubjectivity is particularly relevant for understanding the dynamics of phenomenological reflection and analysis. While the method prioritises the exploration of individual subjective experience, it also acknowledges the inherently social nature of human consciousness. Participants in micro-phenomenological interviews are not isolated entities but are situated within a broader social and cultural milieu, shaping and shaped by their interactions with others (Valenzuela-Moguillansky & Vásquez-Rosati, 2019). Therefore, when tracing the analysis process, intersubjectivity is often used as a validation procedure to triangulate results (Petitmengin et al. 2019b).

3.2.6 Prior Work in Micro-phenomenology

Prior research in micro-phenomenology has made significant contributions to my understanding of the intricacies of psychology and anthropology. Under the umbrella of neuroscience, micro-phenomenology has employed rigorous qualitative methods to explore the nuances of lived experience at a micro level. Besides exploring interview implementation (Petitmengin, 2006; Petitmengin et al., 2019b; Vermersch, 2012), researchers have utilised techniques derived from micro-phenomenology, such as introspective interviews, descriptive phenomenological analysis, and first-person inquiry to uncover the subtlest aspects of human consciousness (Lind, 1993; Tewes, 2023).

Moreover, when studying the experience of meditation, micro-phenomenology also became a popular method to precisely collect the first-person data and therefore assess the effect (Petitmengin et al., 2019b; Petitmengin, 2006, 2021; Przyrembel & Singer, 2018). Meanwhile, researchers also tried to probe and expand the study on micro-phenomenology to objectless awareness during sleep (Alcaraz-Sanchez, 2023). Through this body of work, micro-phenomenology has shed light on diverse phenomena, ranging from bodily sensations and emotions to complex cognitive processes and knowledge sharing in change management (Benson, 2011).

With the gradual deepening of the study and understanding of micro-phenomenology, the investigations on micro-phenomenology have not only deepened the appreciation of individual subjectivity but also opened new avenues for its interdisciplinary applications. In Schoeller's paper, micro-phenomenology was reapproached as a philosophical method to reconnect the thinking process to the experiencing body, which contributed to the development and cultivation of embodied critical thinking through research and training (Schoeller, 2021). Coupé and Ollagnier-Beldame (2019) considered micro-phenomenology

as a method focused on the lived experience of intersubjectivity that contributed to healthcare practices. The rich tapestry of prior work in micro-phenomenology provides a foundation for continued exploration into the depths of human consciousness and the potential for transformative insights in various fields such as HCI (Human Computer Interaction) (Prpa et al., 2020).

3.2.7 Why is micro-phenomenology relevant to my project?

As outlined in previous chapters, this study aims to explore in what ways lay individuals understand, interpret and utilise data breach disclosures. Therefore, two main reasons should be clarified on why micro-phenomenology is relevant to this project. Methodologically, it facilitates participants' ability to articulate detailed first-person accounts, enabling lay individuals to accurately evoke and express their feelings related to data breaches. Besides, the process of epoche (phenomenological reduction) further enhances this method by allowing researchers to suspend preconceptions and assumptions, which allows researchers to approach the phenomena with a more authentic and unbiased view (Petitmengin, 2006). This openness enables a deeper and more precise understanding of the essence of participants' experiences. Additionally, micro-phenomenology's structured approach uncovers temporal development and transition in participants' perceptions, which is instrumental in tracking how their interpretations and reactions evolve before and after reading the data breach letters. By eliciting even minor, subjective impressions, the method seeks to reveal the nuanced ways in which participants engage with the data breach notification letters.

From the practical perspective, micro-phenomenology also provides a new approach to examining information interpretation that diverges from prior readability theories grounded in quantitative formulas. While readability formulas focus on text structure, micro-phenomenology considers the individual's subjective responses and intentions in interacting with the text, which is especially relevant in exploring comprehension among lay users (Gosselin et al., 2021; Petitmengin, 2006). Similar to tax forms and voting instructions, data breach notifications also have a responsibility to fulfil disclosure requirements by crafting texts that are intended to communicate information clearly to a broad audience (Bailin & Grafstein, 2016). By using micro-phenomenological interview methods, this study aims to uncover disclosure frameworks to improve the accessibility and effectiveness of data breach notifications, particularly for vulnerable lay individuals.

3.3 Pilot Interviews

Upon establishing the nature of the Latitude Financial data breach, it was identified that, in accordance with the *Privacy Act 1988 (Cth)* and the Notifiable Data Breaches (NDB) scheme, Latitude primarily relied on breach notification letters – either physical letters or emails – to disclose breach information. As these letters were the main form of communication with lay recipients, I initially chose to focus on interviewing breached individuals of Latitude to explore the clarity, interpretation and impact of these notifications.

Due to the rigorous methodological demands of micro-phenomenology, conducting effective interviews and analysis requires a well-organised protocol and substantial practical experience. Since I had limited prior exposure to this method, I encountered challenges in both the design and implementation of this approach. To address these issues and refine my interview techniques, my supervisor and I decided to conduct a pilot interview prior to initiating formal data collection. Coincidentally, one of my supervisors was also a victim of the Latitude breach, making her an ideal participant for this preparatory exercise.

Compared to the traditional pilot interview process, there are several methodological and practical advantages to including my supervisor as the interview participant. Interviewing a supervisor – similar to interviewing a friend or acquaintance – can make the interview process more accessible, efficient and targeted (Alam, 2024). As someone deeply familiar with the research topic, my supervisor was able to offer targeted feedback on the interview design and suggest ways to improve interview phrasing and topic sequencing. Furthermore, while traditional interviews typically maintain an "asymmetrical power relation" in which the interviewer holds most authority, involving a supervisor in this context introduced an "inversion of authority", which empowers the interviewee to take on a co-constructive role helping the interviewer start the discussion, emphasising key topics and managing the pacing of the interview (Kvale, 2003). In doing so, the interaction shifted from a one-way dialogue to a more dialogical and reflective exchange, thereby contributing meaningfully to the development of the interview framework (Brinkmann & Kvale, 2005).

Meanwhile, it is also important to acknowledge the potential ethical concerns associated with interviewing a supervisor during the pilot study, as this may primarily lead to hierarchical influence, conflict of interests and potential response bias (Brinkmann & Kvale, 2005). Given the inherent "asymmetrical power dynamic" of the researcher-supervisor relationship, there exists a risk that the supervisor might feel obliged to provide responses that are overly positive or influenced by their authority (Alam, 2024). To mitigate these risks, the interview with my supervisor was clearly framed as a mock interview. This distinction emphasised that the pilot interview was conducted solely for the purpose of testing the pre-designed micro-phenomenological interview questions and procedures. As

such, it served only to refine the interview protocol and did not aim to collect data for formal analysis, thereby minimising the ethical risks.

Additionally, as the pilot interview closely mirrored the format and procedure of the forthcoming formal interviews, informed consent was obtained orally, with clear clarification that participation was entirely voluntary and that my supervisor could withdraw at any time without affecting our professional relationship. The confidentiality of the mock interview data is also strictly maintained, and the pilot interview data was stored the same level of security as the formal interview data, ensuring the interviewee's privacy was fully protected. Taken together, we believe the above precautions could significantly reduce the ethical risks associated with interviewing a supervisor and help ensure the integrity of the research process.

After careful consideration of the ethical implications, the pilot interview was conducted via Zoom. During the session, the interviewee was asked to read and reflect on her breach notification letter, sharing her interpretations and emotional responses to both the disclosed information and the breach incident. This process enabled an evaluation of the preliminary interview protocol's flow, sensitivity and relevance in practice. A second mock interview was subsequently conducted to further solidify the procedures and improve the clarity of the interview questions.

Insights from the pilot study informed the final interview design, which continues to invite participants to share and read through their breach letter during interviews. Additionally, the pilot interviews provided valuable opportunities for me to practice micro-phenomenological interviewing techniques and confirm the appropriateness of the interview guidelines. Overall, findings from the pilot study significantly contributed to the subsequent formal interviews and informed broader methodological reflections.

3.3.1 Pilot Interview Processes

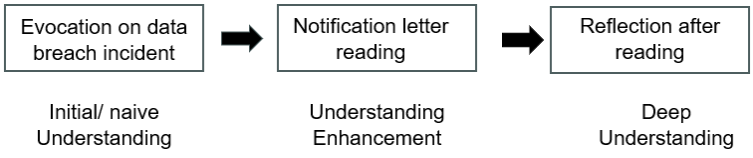
As Chua (1986) suggests, the interpretative process is a continuous social interaction and by no means linear. Through this continuous stream of consciousness, interpretation gradually deepened by the iteration of cognition and reflection (Petitmengin et al., 2019b) from a naïve understanding to a more in-depth grasp of the textual explanation, evolving from a partial comprehension to a holistic insight (Geanellos, 2000; Ricoeur, 1976). Accordingly, the interview processes of this study are structured based on the framework of a hermeneutic circle, with specific micro-phenomenological interview questions, to progressively deepen participants' interpretations across three stages: before, during, and after reading the breach notification letter.

First, before reading the breach notification letter, participants are introduced to the study through a prologue where we secure informed consent and provide a brief overview of the research. Premise questions are posed to stimulate recall and evoke participants' initial impressions of the Latitude data breach. For example, micro-phenomenological questions such as, "To the best of your knowledge, had you previously experienced a data breach?" and "How did you initially find out that you were breached by Latitude?" are designed to prompt participants to reflect on their awareness and understanding of the incident prior to engaging with the notification letter.

Subsequently, interviewees will be required to read the breach letter in sections with each portion followed by targeted questions that encourage them to engage deeply with specific statements or sentences in the letter. This guided, step-by-step reading enables participants to uncover underlying meanings or details they might have overlooked, fostering a layered understanding of the breach letter. As indicated in Appendix A, a typical breach letter includes components such as an introductory note from the CEO, a description of the incident, details of impacted information, steps the organisation has taken, recommended self-protection measures, and further resources. Questions are tailored to individual sentences that might elicit significant interpretative insights. After each interview, the transcription is promptly analysed to refine and adapt questions for subsequent interviews, enhancing the iterative nature of my approach.

Finally, after reading the breach letter, a reflection stage is also designed to explore participants' overall understanding of the breach and the notification letters. This phase focuses particularly on any shifts in interpretation and reaction prompted by the letter. Given the structured rigour required by micro-phenomenological interviews to capture the nuanced subjective interpretations (Petitmengin, 2006), I continually refine my interview questions based on insights gained through each iteration. The following figure (Figure 1) presents a direct overview of the iterative three-stage interview process, demonstrating how the interview structure assists the flow of understanding advance from naïve to in-depth.

Figure 11: Interview Process



Specifically, the micro-phenomenological questions are designed to systematically guide participants through their subjective experience before, during, and after reading a data breach letter (DBL). Unlike traditional interviews, the micro-phenomenological approach encourages participants to fully recall and examine overlooked experiences and details, facilitating a more profound engagement with their actions

toward breach incidents. In all three stages – pre-reading, reading, and post-reading – the participants' understanding is continually enriched through processes of retrieval, reflection, and description (Petitmengin et al., 2019b). This iterative return to the initial circumstances surrounding their receipt of the DBL enables participants to evoke and trace the evolving shifts in their perceptions and responses.

Generically, this interview process provides a systematic and iterative structure to individual interpretation, allowing for a deeper and more nuanced understanding of texts, experiences, and further reactions. This process assists participants, particularly lay people, in uncovering and articulating nuanced understandings that may have been unexpressed or previously unnoticed. Furthermore, through analysis of the initial mock interview, we established a preliminary generalised interview guideline, which facilitates refinement of the questions and enhances the exploration of experience in subsequent interviews. As part of the iterative process, a second mock interview was then conducted to review and further refine the questioning approach, ensuring that each element of the interview effectively supports an in-depth micro-phenomenological analysis.

3.3.2 Developing and Reorganising Pilot Interview Transcription

According to Petitmengin (2006), all kinds of information are valuable clues for evaluating the intensity of the evocation state and enhancing the authenticity of the descriptive statement. In contrast to audio recording, video recording has the advantage of capturing paralinguistic cues such as variations in speech pace, pauses, hesitations, repetitions, stammering, and sound imitations, all of which can contribute to a more immersive interview experience (Valenzuela-Moguillansky & Vasquez- Rosati, 2019). Besides, due to the requirements of the interview design, the interviewees need to read the breach letter on-site to deepen their understanding of the incident. Therefore, after getting consent, we decided to use Zoom recording for keeping video documents and automatically generating transcriptions. Subsequently, following the analysis structures of Petitmengin et al. (2019), we proposed an initial data cleaning protocol, which involves reorganising the chronology and providing a fine mesh description.

Table 11: Initial Data Cleaning Protocol

Main Procedures	Specific Processes	Reasons
Preliminary cleaning	• Correct paragraphs' pauses and speakers. • Add punctuation. • Correct spelling and grammar.	• Enhance the readability of the transcription.
Advanced cleaning	• Numbering (questions). • Distinguish question quality.	• Identify the useful information. • Facilitate the subsequent phases of refinement (Petitmengin et al., 2019a).

Assessing data reliability	• Note singular verbal statements. • Note verbal, non-verbal and para-verbal statements (slowing down, pausing). • Detect descriptive and non-descriptive statements.	• Epoche (bracketing). • Distinguish the verbatim statements describing singular experience with the generic present (Petitmengin et al., 2019a). • Minimise inaccurate induction.
Chronological reorganisation	• Arrange the sequence of the statements.	• Provide a fine mesh description. • Construct an iterative structure of the transcription.

According to the protocol, after doing the basic preliminary cleaning, micro-phenomenology also asks to detect the "pure singular experience element". In doing so, following the prior work of Petitmengin et al. (2019) on discovering the structure of micro-phenomenology, several advanced procedures are proposed to better "bracket" the interviewees' singular experience.

Firstly, after getting the cleaned initial transcription, the content in terms of different questions should be distinguished in numbers and noted quality. In this procedure, "content-empty" questions or inductive questions should be specifically labelled, which enables the researchers to obtain fine-focused statements. Subsequently, indicators such as verbal (tone, metaphor), non-verbal (eye contact, gesture), and para-verbal (pause, distribution of speaking time, slowing down of verbal flow) should be labelled in order to prepare for the verbatim analysis. This procedure, proposed by Husserl (1970) as one of the most significant concepts in the phenomenology discipline, is the so-called epoche or bracketing, which aims at capturing the singular experience without pre-existing beliefs or bias. Besides, specifically, singular statements (such as reference to a specific moment using "I") should also be noted in this procedure compared to general statements such as "usually" or "always".

Last but not least, the final procedure for reorganising the transcription is to sequence the different questions chronologically, which could provide a better fine mesh description as well as help the researchers construct the iterative structure of the whole interview. In this procedure, researchers could also review the interview and particularly reflect on the interview questions, which could provide an iterative process for enhancing the quality of micro-phenomenology interview questions in later interviews.

3.3.3 Analysis of Pilot Interview Transcription

Compared with other qualitative and phenomenological analysis methods, micro-phenomenology focuses more on the structure of the experience, emphasising the concrete (structural) statement rather than the normal content (descriptive) statement (Petitmengin et al., 2019b). It requires the researchers to detect potential minimal indicators of structural features, or so-called descriptemes, and analyse data through processes of synchronic and diachronic structural unfolding by specialisation and fragmentation, which will minimise the researchers' interpretation as well as enhance the reproducibility

of the analysis results (Petitmengin et al., 2019b).

The micro-phenomenological analysis begins with “verbatim”, which is an important procedure to find the synchronic and diachronic abstraction elements. In doing so, structural statements should be differentiated from the traditional content statement, and both top-down and bottom-up abstraction operations are conducted. Category, sub-category and descriptemes are defined from a generic to a specific level. Additionally, based on the formalism of the semantic network proposed by Sowa (1984), the operation of abstraction is mainly divided into three steps: classification and instantiation, aggregation and fragmentation, generalisation and specialisation. However, just as suggested by Petitmengin et al. (2019), when analysing verbatim transcripts, beginning with a diachronic analysis might be advantageous, as it encompasses the temporal progression of an experience. By employing a segmentation approach, researchers can effectively break down the description of an experience into precise micro-actions and micro-processes, emphasising the subtle chronological nuances among the identified temporal segments. After making the abstraction operation, the last procedure in micro-phenomenological analysis is to combine both the synchronic and diachronic structure with the dynamic lines, which helps to present the dynamic evolution of an experience. Last but not least, structural unfolding by specialisation and fragmentation should then be conducted, which elucidates the reproducibility of the analyses.

3.3.4 Reflection on Pilot Interview

The reflection on my first mock interview mainly focuses on interview questions and skills. From a technical perspective, we found it difficult to consistently record the interviewee via Zoom recording, resulting in instances where the interviewee’s actions were missed if both the interviewer and interviewee spoke simultaneously. However, since we could still record the interviewee’s voice and it did not substantially affect the overall quality of the interview recording, we decided to continue using the Zoom recording in my following interview, acknowledging this as an unalterable source of bias.

Besides, the mock interview provided valuable insights into the nuances of micro-phenomenological interviews. For instance, the initial interview question in the mock interview asks the interviewee to think about how things were going on the day that they received the breach disclosure letter. This approach could not only help the interviewee be further aware of her subjective memory but also stabilise her attention towards the process and enter into a more relaxed rapport with the interviewers (Petitmengin, 2006), thus fostering a conductive interview environment. Moreover, techniques such as “direct reference” were also employed to encourage the person interviewed (Heimann et al., 2023) and help to build a better context for the micro-phenomenological interview.

After conducting the initial mock interview and receiving feedback from my supervisors, we kept advancing my interview questions and processes with a subsequent interview, in which we decided to specify my interview questions into different parts of the breach letter. Firstly, the prior interview questions mainly focused on breached individuals' initial reactions and interpretations but ignored their experiences before the breach. For example, one question asked by my supervisor is, "Had you been breached before this?", which generates a deeper investigation of the interviewees' prior breach experience. Furthermore, as addressed by Petitmengin et al. (2019), the micro-phenomenological questioning mode should be content-empty and structure-driven, which means that the interviewer should have no induction during the interview, however, one question asked by me about the harm is somewhat inductive. Thus, in the following interviews, I should be more careful about the way of ask questions.

Additionally, I also made significant changes to my interview focus after the mock interview. As the research aim requires to explore the interpretations of individuals, which includes not only thoughts but also reactions and how to use, compared to the original micro-phenomenological focus on feeling, emotion and non-verbal elements (Petitmengin, 2006), I decided to emphasise more on individuals' understanding. Therefore, different from the previous questions, my advanced questions try to avoid asking about feelings and emotions but rather attempt to delve into the perspectives of interviewees' thoughts and understanding. Furthermore, based on Ricoeur's interpretation theory (1976), we advanced my interview steps into three parts according to the progressive understanding process. Meanwhile, we also looked back at the content of the breach letter and decided to divide the interview into the different parts of a breach letter and generate specific questions in terms of some significant problems exposed in the mock interview. For instance, in the mock interview, my supervisor pointed out that the third part of the breach letter (*what kind of information has been breached*) was particularly misleading, which made it even harder for her to understand the situation. Therefore, in the modified protocol, we pay special attention to asking nuanced questions for some important sentences.

Last but not least, despite the initial intention to collect data from interviews with three companies (Optus, Medibank and Latitude Financial) data breach incidents, the mock interview experience prompted a reconsideration of the potential chosen cases. For instance, as mentioned in the mock interview "[…] *there are certain institutions that you have to engage with properly and identify yourself right, which is financial institutions, health* […]", people naturally become more cautious about their financial and medical related data. Thus, with the increasing difficulties of micro-phenomenological interviews and the rich content embedded in each interview, we determined to focus solely on the Latitude Financial data breach incident. Nevertheless, the prior plan to interview approximately 15 to 20 breached individuals remains intact.

3.4 Interviewee Recruitment

Following the pilot study, formal interviews were conducted, largely adhering to the initial interview processes established in the pilot study, with minor changes to specific interview questions. Initially, I intended to recruit genuine victims of the Latitude Financial data breach through passive snowball sampling within my network; however, this approach was not as effective as anticipated. To enhance the recruitment efforts, I then expanded the strategy by incorporating social media platforms. In doing so, a Facebook group was identified spontaneously formed by breached victims of Latitude Financial with around 800 members. After obtaining consent from the group administrator and receiving relevant ethics approval, I started to approach potential participants both within my network and through the Facebook community.

The initial recruitment strategy of this study involved posting a recruitment advertisement in the group and actively engaging with interested individuals who responded. Prospective participants were subsequently sent a formal invitation letter, along with a participant consent form and a participant information statement, explaining the purpose of the research, the study procedures, and the objectives of the attached documents. Upon receiving formal consent, interviews were scheduled via Zoom, during which oral consent was also recorded and research objectives clarified. Formal interviews were planned to last approximately one hour, although participants were offered the option of a shorter, 30-minute session if preferred. Despite these efforts, recruiting a sufficient number of relevant participants proved quite challenging, and ultimately, four interviews were successfully conducted during the first stage of recruitment.

To broaden the participant pool, I subsequently sought ethics approval amendments to recruit through additional social media platforms, including X (formerly Twitter) and Reddit. However, this expansion presented new challenges. The anonymity of Reddit users, for instance, made it difficult to verify participant identities and obtain formal consent. Similarly, X's privacy settings, which restrict direct messaging to individuals without prior interaction, limited my outreach to potential participants on this platform. In response to the recruitment difficulties, I adapted interview methods in the second stage of interviews. Building on the data and materials collected from the initial breach victims, Phase two interviews shifted focus and expanded beyond recruiting breach victims to include retired or largely retired individuals – a population particularly vulnerable to cybersecurity threats (Murthy et al., 2021). This adjustment facilitated my access to participants while maintaining the study's relevance to data breach disclosure interpretation.

3.4.1 Phase One Interview Processes

The recruitment process naturally divided the interviews into two phases. The Phase One interviews closely followed the structure established in the pilot interviews. Before each interview, participants were asked to share the breach letter(s) they received from Latitude. During the interviews, participants were first prompted to evocate their breach experience and then invited to read through their letter(s), where they were encouraged to share their immediate reactions and reflect on any shifts in their thoughts. This micro-phenomenological approach enabled me to capture real-time responses and evolving perspectives. Given the length of the breach letters, I only concentrated on critical sections, such as the CEO's statement, the "What happened" section, "What kind of information has been impacted", and "Steps we are taking to help you". After reading these sections, participants were asked several generic questions regarding their overall understanding of the breach notifications, including inquiries about whether they felt the severity of the risk was adequately communicated and whether the disclosures influenced their perceptions of future choices.

Although the Phase One interview size was limited, these initial interviews provided valuable insights and led to important refinements in the interview guidelines. One of the key adjustments was the inclusion of more practical questions, such as asking participants to define data breaches and gauge their cybersecurity knowledge level. This addition helped me establish a clearer understanding of participants' baseline awareness and perception of data breaches. The Phase One interview also revealed critical focal points from the participants' perspectives. For instance, participants frequently expressed emotional reactions to specific phrases, notably the statement, "If you choose to replace your driver's license," which prompted confusion and concerns. These reactions led to further refinement of the interview questions to probe participants' interpretations of ambiguous wording. Additionally, participants identified paradoxes within the breach letters, highlighting areas of ambiguity that required further exploration. Based on these findings, further exploration of participants' reactions and interpretations was conducted in Phase Two interviews.

Another significant finding from Phase One interviews was the variation in participants' responses to different versions of the breach letters. While some participants received the standard lengthy and vague notification letter, others received a much shorter and more explicit version. These differences elicited distinct emotional and cognitive reactions, suggesting that letter style significantly impacts user interpretation and satisfaction. As micro-phenomenological interviews primarily focus on the subjective experience within a single text, it is insufficient to fully capture comparative understanding across letter styles. To address this limitation, Phase two interviews were also designed to broaden the methodological approach and further investigate how individuals understand and respond to different disclosure formats. By supplementing micro-phenomenological interviews with additional qualitative

methods, this research aimed to uncover more insights into participants' understanding and preferences, ultimately contributing to a richer assessment of DBN effectiveness.

3.5 Experimental Research

The findings from Phase One interviews established a foundational understanding of how breached individuals initially engage with and interpret breach notifications, which informed the design and focus of the Phase Two interviews. Leveraging these insights, Phase Two interviews conducted a method known as "qualitative experiment", initially proposed by Barlett (1932), to explore lay individuals' preferences regarding notification content and other features. In this phase, twelve semi-structured interviews were conducted, during which participants made a comparison of two notification scenarios captured from Phase One interviews, allowing for a deeper exploration of their preferences and responses.

This section begins by reviewing the context and theoretical foundations of qualitative experiments, explaining how this method differs from traditional qualitative and experimental approaches and why it is particularly suited for this study. Following this, this section then outlines the Phase Two interview processes in detail, which involved presenting participants with two distinct Latitude breach notification letters collected from Phase One participants. By comparing these scenarios, Phase Two interviews enabled a more in-depth exploration of how various notification elements affect individuals' understanding and responses. Through this deductive approach, Phase Two interviews seek to reveal patterns in interpretation and behaviour that may not have been fully articulated in Phase One interviews.

3.5.1 Qualitative Experiment

In Phase One interviews, the micro-phenomenological approach was conducted to capture nuanced descriptions of subjective experiences. While micro-phenomenology implies a close relation to phenomenology, it has been subject to extensive debate regarding its applicability (Heimann et al., 2023). For instance, researchers have noted that micro-phenomenology may not be ideally suited for exploring narrative structures, such as biographical or developmental trajectories (Sparby et al., 2023). Consequently, after applying micro-phenomenological interviews to identify the generic structures underlying certain types of experiences (Heimann et al., 2023), further hypotheses concerning lay individuals' preferences were generated. To substantiate the hypotheses, it is necessary to complement micro-phenomenology with additional methods. Thus, Phase Two interviews incorporate a method named "qualitative experiment" that builds upon the initial approach by integrating experimental

elements. Unlike traditional qualitative methods, such as in-depth interviews or focus groups, qualitative experiments provide a distinct approach to data collection, enabling the identification of patterns or processes that participants may find difficult to articulate explicitly (Steils, 2021). This complementary approach is intended to enhance the understanding and validation of the phenomena under the Phase One study.

First introduced by Bartlett (1995) to explore experimental elements in social psychology studies, the qualitative experiment method combines traditional qualitative approaches with structured experimental features (Steils, 2021). Unlike quantitative experiments, which focus on measurable outcomes, qualitative experiments are more "exploratory and heuristic" in nature (Kleining, 1986). Qualitative experiments also differ from traditional observation methods, which rely on discovery and introspection (Kleining & Witt, 2001), allowing for more controlled and systematic analyses of patterns (Robinson & Mendelson, 2012). Since Bartlett's (1995) pioneering experiments on memory, qualitative experiments have been further developed and applied to other disciplines. For example, Walter and Pronzato (1990) used this approach to design experiments for phenomenological models, while Garau et al. (2008) explored the concept of "breaks in presence" using qualitative interviews. In a word, qualitative experiments are especially effective for identifying qualitative relationships, including structures, processes, or changes within those structures (Kleining & Witt, 2001; Wagoner, 2015).

What distinguishes qualitative experiments is their open and interpretive approach to investigation and analysis (Robinson & Mendelson, 2012). In qualitative research, validity is attained by balancing methodological rigour with innovative exploration. (Whittemore et al., 2001). Compared to traditional in-depth interviews, the qualitative experiment method offers greater interpretive validity and rigour, making it a valuable approach for future research as well as authentically reflecting participants' experiences and the meanings they attach to them while conducting qualitative analysis (Lincoln, 2001; Sandelowski, 1996). By integrating experimental strategies into a qualitative framework, researchers can gain a deeper understanding of individual behaviours and decision-making processes, especially those that participants may find difficult to articulate (Steils, 2021). This method is particularly effective for identifying structures, processes, and other qualitative relationships, making it well-suited for studying complex phenomena in the social sciences (Kleining & Witt, 2001; Wagoner, 2015). Ultimately, the qualitative experiment enhances both the validity and interpretive depth of the study, providing a more robust framework for analysing lay users' interpretations of data breach disclosures (Steils, 2021).

In accordance with the qualitative experiment method, twelve "within-subject experiments" were conducted (Steils, 2021) as phase-two interviews. Following the adapted interview protocol iterated from the pilot study and preliminary interviews, each of these qualitative experiments employed a

traditional qualitative approach (in-depth interview) using the micro-phenomenological approach to capture the nuanced expressions and shifts in interviewees' feelings and thoughts as well as experimental sections including two scenarios for participants to choose which was selected from the breach disclosures materials captured from the preliminary interviews. This qualitative experimental approach not only added depth to the research but also increased its validity by controlling for extraneous factors, such as participant characteristics (e.g. retired or largely retired lay individuals with limited experience of data breaches), while allowing for flexible, participant-driven discussions. Consequently, the qualitative experimental approach conducted in Phase Two interviews facilitated a comparative analysis of individuals' interpretations and responses across different disclosure contexts.

3.5.2 Phase Two Interview Processes

In line with the qualitative experiment framework, the semi-structured interviews in Phase Two basically follow the guidelines established in Phase One interviews, with experimental elements added after participants fully read the breach notification letters. This phase involved enhancements to both participant recruitment and interview procedures.

Given the challenges in recruiting individuals directly affected by the Latitude breach, the participant pool was broadened to include non-breached individuals, particularly targeting retired or largely retired individuals since they lack cybersecurity knowledge and are especially vulnerable to data breaches (Murthy et al., 2021). Utilising the passive snowball sampling, I finally approached and interviewed twelve participants in the second interview phase, and each of the interviews lasted around thirty minutes.

Meanwhile, I refined the procedures for conducting Phase Two interviews. Adopting a within-subjects experiment (Steils, 2021), I believe that qualitative experiments could help me identify behavioural patterns and interpretive processes that participants might struggle to articulate explicitly. Drawing on notification materials collected in Phase One, I summarised the most common circumstances faced by breached victims of Latitude, detailing how people have chosen to use Latitude Financial services and how the breach occurred. This was used as consistent information provided at the beginning of each interview to help non-breached participants understand the Latitude breach context. With the offered background information, participants were then asked to imagine themselves as Latitude breach victims. To maintain consistency and control for the absence of further updates, interviewees in the second phase were also informed that the presented breach notification was the only letter they had received. This approach helped ensure consistency in participants' understanding of the data breach context.

Furthermore, Phase One interviews revealed that while breach notification letters are largely standardised, variations still exist in the affected personal information disclosed to different individuals. Based on this observation, I categorised the breach notification letters gathered into two distinct scenarios for comparison in Phase Two interviews. Each participant was first invited to read a real Latitude breach letter, including standard sections of the CEO statement and incident overview. Following this, participants were required to review two different scenarios describing the type of personal information affected and the support provided. This setup allowed me to explore participants' preferences for notification content and to assess how the varying formats influenced their understanding. Finally, participants were also asked to share their overall impressions and understanding of the breach notifications, providing insights into their interpretations and reactions. The following section is a detailed introduction to the two notification scenarios selected, illustrating the rationale I chose them.

3.5.3 Introduction of scenarios in Phase Two interviews

The breach notification letter chosen for scenario one is described by Phase One participants as "generic and vague" (see Figure 2), listing all potential categories of affected personal information and making assurance that without further update, some information has not been affected. My observation from Phase One interviews indicated that most Latitude victims received similar statements. Many participants found this type of statement confusing, with its length and ambiguity appearing to lead to contradictory interpretations. Given its typicality and prevalence, I selected this type of statement as the scenario one notification to examine how participants respond to a "generic and vague" breach notification.

Figure 22:Scenario One Breach Notification (Derived from collected DBLs)

What kind of information was affected?

We have so far identified that the attack resulted in the following kinds of your personal information being compromised. This information was collected from you at the time you applied for credit from Latitude or our predecessor companies.

Unless we have explicitly notified you, images of your identification document(s) have **not** been compromised.

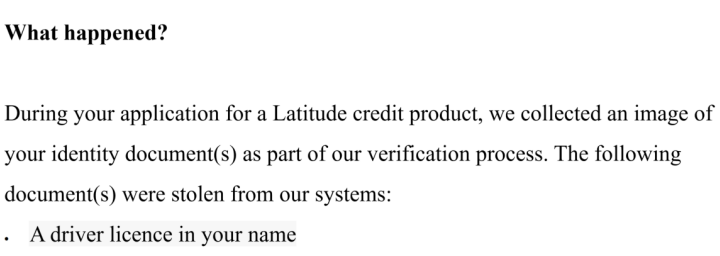
- The licence number on the driver licence you provided us as part of your application.
- The personal information you provided us as part of your application which, where applicable, included your full name, address, date of birth and phone number.

If we identify any other of your personal information has been compromised, we will notify you as quickly as possible.

The breach letter selected for scenario two (see Figure 3) is a highly specific and explicit statement, in

contrast to the more generic notifications discussed above. This unique notification letter is obtained from a Phase One participant and directly informs in clear, concise language that the driver's license information has been compromised. Since this is the first instance of a breach notification featuring such targeted specificity, I chose it as scenario two to explore how participants respond to a more direct and explicit notification style.

Figure 33: Scenario Two Breach Notification (Derived from collected DBLs)



What happened?

During your application for a Latitude credit product, we collected an image of your identity document(s) as part of our verification process. The following document(s) were stolen from our systems:

- A driver licence in your name

3.6 Ethical Consideration

The ethics approval of this study has been updated in accordance with methodology modifications in three stages. Initially, I employed a passive snowball sampling technique to identify and approach breached individuals of Latitude for interviews. However, it soon became apparent that this approach alone was insufficient to recruit an adequate number of participants. To overcome this limitation, I expanded the recruitment strategies to include social media platforms, starting with a Facebook group comprised of approximately 800 members, spontaneously gathered by Latitude breach victims. After obtaining consent from the group administrator, I posted a recruitment advertisement, inviting group members to participate in the study. This led to the first modification of my ethics approval.[2]

Despite these efforts, the sensitive nature of the breached individuals and issues such as ongoing class actions posed significant challenges. Many potential participants in the Facebook group were suspicious of my identity and responded coldly to the recruitment attempts. Consequently, I made an amendment to prior ethics approval to contact potential participants via other social media platforms, such as X (former Twitter) and Reddit. However, new challenges arose, including X's (former Twitter) privacy settings, which prevent direct messaging to individuals without prior interaction and the anonymity of Reddit users, which made it difficult to verify identities and secure consent.

After successfully conducting four interviews with genuine victims of the breach, I struggled to recruit additional participants. Given these constraints and the observation that lay individuals' interpretations

[2] This study has received the human research ethics approval from the University of Sydney with project identifier: 2023/HE000879.

of breach experiences were generally similar, I expanded the sample to retired or largely retired individuals, regardless of whether they had been breached, reverting to the original passive snowball sampling method. This adjustment significantly simplified the recruitment Process.

3.7 Concluding Comments

This chapter provided an overview of the methodological framework of this study, with a detailed account of the data collection processes. Specifically, it first offered a comprehensive introduction to the Latitude Financial breach case context, illustrated the process and findings from the pilot study, and then described the subsequent execution of the formal interviews in two distinct phases. Both phases highlight the specific methodologies employed and the concrete interview processes undertaken. Additionally, this chapter outlined the steps taken to obtain ethics approval for the study, along with the ongoing adjustments made to accommodate methodological refinements throughout the research process. This ensured that the study maintained ethical integrity while allowing for necessary adaptations to optimise the research design.

CHAPTER 4 – EMPIRICAL STUDY

4.0 Introduction

This chapter presents an in-depth analysis of the empirical data captured from the two-phase interviews, examining the further implications of DBNs for lay individuals' interpretations and preferences. Building on the data collection process outlined in the previous chapter, this chapter provides a comprehensive overview of the procedures followed in coding and analysing the collected data. Through detailed analysis, this chapter aims to uncover lay individuals' experiences with interpreting DBNs and explore their preferences regarding the content and structure of these notifications. After presenting findings from each interview phase separately, this chapter also aims to draw a picture of the lay users of DBNs, highlighting the distinct characteristics of lay users of DBNs in contrast to traditional professional users of accounting information.

4.1 Analysis of the Collected Breach Letters

During the empirical study, DBLs were ultimately collected from six Latitude victims (including my supervisor). A notable characteristic of these breach letters is the standardised structure, with several fixed sections. Each letter typically begins with a statement from the CEO, which includes an apology for the breach, an outline of the letter's content, and instructions for contacting Latitude Financial. This is followed by a "What happened" section, which provides a summary of the breach, its cause, and the immediate actions taken, such as notifying relevant authorities. Subsequent sections vary based on the individual's circumstances but commonly include "What kind of information has been impacted" and "Steps we are taking to help you." The former specifies the compromised personal data, while the latter offers guidance on mitigation steps for affected individuals.

Although the breach letters are generally standard, differences were observed in their content, issuance dates, and the number of letters received by different individuals. These differences influenced recipients' interpretation of the breach notification and their understanding of the incident. To provide a comprehensive overview, the letters were systematically compared based on the above differences. The detailed findings are outlined in the table below:

Table 22: List of Collected DBLs

	Breached Information	Letter/s Received	Date of first letter received	Date of second letter received	Date of third letter received
Victim 1	Driver's license (Vague statement)	1	5/4/2023	-	-
Victim 2	Driver's license (Vague statement)	2	17/3/2023	31/3/2023	-
Victim 3	Driver's license	3	17/3/2023	20/3/2023	31/3/2023
Victim 4	Driver's license (Vague statement)	1	31/3/2023	-	-
Victim 5	Driver's license & financial information	3	17/3/2023	20/3/2023	24/4/2023
Victim 6	Driver's license & financial information	2	20/3/2023	5/2023	-

The comparison reveals that the content and number of breach letters received by affected individuals are closely related to the severity of the data breach they experienced. Individuals who suffered more significant impacts, particularly those whose financial information was compromised, tended to receive additional letters providing further explanations. In contrast, the initial disclosures, sent shortly after the breach was detected, were generally vague and lacked specific details about the compromised personal information but only promised further updates. However, most breach victims did not receive any follow-up email. For instance, while victim 5, whose financial data was breached, received two follow-up emails, the majority of participants received only one or two notifications. Notably, only one victim (victim 3) received a third letter explicitly stating which of his personal information (driver's license) had been stolen.

Meanwhile, although most initial breach letters were sent in a timely manner, there was a noticeable delay between Latitude disclosures to relevant organisations, such as the ASX, and the time when breached individuals received the disclosures. Furthermore, breached individuals did not receive any further updates from Latitude regarding the investigation after legal firms (Gordon Legal and Hayden Stephens Associates) became involved, even regarding critical subsequent issues such as the ransom demand required by the attackers and how Latitude Financial responded to it. No additional breach letters were sent after May 2023, presenting a shortfall in the company's disclosure practices.

4.2 Coding Processes

The coding process for this study involved a systematic approach to analysing interview data, utilising

both manual and software-assisted techniques. The initial step in the process involved using the auto-generated transcriptions provided by Zoom. These transcriptions, while helpful in capturing the basic content of the interviews, required substantial manual review and correction to ensure accuracy. This was essential in maintaining the integrity of the data, especially given the nuanced nature of the participants' experiences in the context of breach notifications.

Once the transcriptions were thoroughly reviewed and corrected, the coding process proceeded with the use of NVivo, a qualitative data analysis software designed to assist in organising and analysing large datasets. NVivo facilitated the structuring and categorisation of the data, allowing for a more efficient and organised approach to identifying key themes and patterns (Welsh, 2002). Given the two-phase interview design, transcripts from each phase were coded independently. The coding from the first stage allowed for the identification of emerging themes, which informed the subsequent analysis and manual coding of the second-phase interviews.

A two-cycle coding method was employed throughout the analysis, in line with the guidelines set forth by Johnny Saldaña (2012). This method, consisting of both first-cycle and second-cycle coding, enabled a deeper exploration of the data by refining the initial codes into more meaningful categories (Saldaña, 2014). In the first cycle, a combination of descriptive coding and in vivo coding was conducted to label and capture the essential ideas directly from participants' language and experiences. This phase was critical in staying close to the participants' perspectives and understanding their unique interpretations of the breach notification letters (Saldaña, 2012).

Given the two phases of the interviews, coding was conducted in distinct stages. Each stage was coded separately to ensure that the specific focus and nature of each interview phase were preserved. This approach provided the opportunity to observe the evolution of participants' thoughts and experiences across the different stages of the study. In the second cycle of coding, pattern coding was employed to group the initial codes into more abstract themes and relationships (Saldaña, 2014). This process allowed for the identification of recurring themes and patterns across the various interview phases. The second-cycle coding was particularly useful in synthesizing the data, enabling a clearer understanding of how participants' trust, emotions, and responses to breach notifications developed over time (Saldaña, 2012).

By utilising a two-cycle coding process, this study ensured a robust and thorough analysis that captured both the immediate, surface-level reactions of participants as well as the deeper, more complex patterns underlying their experiences. This structured approach to coding allowed me to generate a comprehensive understanding of how lay individuals process and interpret breach notifications, contributing to the further exploration on analysing the implicit rationale of the phenomenon.

4.3 Phase One Interviews Analysis: Interpretations from Breached Individuals

Phase One consisted of four semi-structured interviews, each lasting approximately one hour. The primary focus of these interviews was to examine the breach letters provided by the participants, eliciting detailed accounts of their experiences.

This approach allowed me to gain a comprehensive understanding of the general circumstances faced by Latitude Financial breach victims while also refining and validating the interview questions initially developed from the pilot study. A summary of Phase One interview is provided in the table below.

Table 33: List of Phase One Interview

	Evocation in data breach	Response to breach & breach letter/s	Actions after breach	Key insights after reading	Evaluation on breach letter
Interviewee 1	**Little recollection** *("I can't remember", "The whole thing was just confusing for me because I didn't. And to be honest, I thought it was some kind of a scam or spam."*)	**Distrust & Indifferent** *("I didn't know that I had a Latitude. I didn't do anything. I didn't change my license. I mean, I don't know what I'm supposed to do. It gives me a lot of instructions here, but I didn't read it. And I didn't… I just didn't. I didn't care.")*	**No Action**	**Losing connection with Latitude** *("I'm much more concerned about being phished than I am about this loss of information." "The difficulty is getting me to read past the first paragraph, because you haven't connected with me.")*	**Redundancy** *("Just make it shorter and get to the point")*
Interviewee 2	**Little recollection** *("I think the Latitude send me 3 emails regarding this cyber-attack. But I think I missed all of this email last year. So, I just check this year and just find this information.")*	**Indifferent** *("I think for customers, we can't do too much." "I think no one can escape this attack (breach).")*	**No Action**	**More sensitive to financial information loss** *("[…] until this (got money stolen), maybe I'll close the account." "I think every month I check my bills")*	**Generic** *("I think everyone got an email like this.")*
Interviewee 3	**Little recollection** *("I couldn't remember. Now that's been very long time since I became their customer." "I remember seeing it (Latitude breach) on TV, and I remember seeing it in my inbox.")*	**Indifferent** *("So, now that I'm looking at that and I'm thinking that's just like a strategic ambiguity. But I'm sure when I read it first time, I just thought, well, it's just not written clearly, and I moved on with my life.")*	**No Action**	**Miscommunication** *("This is a disaster in communication. You might as well not communicate. It will be better than miscommunicating, because then I can interpret it in any way I want and then regret and think bad about my own behaviour, and about my own perception of what you're saying.')*	**Generic** *("I think it's quite generic.")*
Interviewee 4	**Strong recollection** *("I remember there was some kind of correspondence in the first phase […], where they were identifying to their consumers that there had been a breach. And then it went quiet, and it ended up all over the news. And I saw on social media. You know, the algorithms were kind of showing me more about latitude and how it fluctuated through the processes. And then I got the follow-up letter that I was impacted.")*	**Disappointed; Dismissive; Vague instructions and explanation** *("It's just so disappointing that businesses of such vast access to vulnerable people to sell their services like this letter to me, it's not tapping into clear conversation points to their consumers […]." "The language that they've used in my personal opinion is so youthful and dismissive." "It hurts to read it (breach letter) because they're not giving me a clear indication of what was stolen if I was impacted and how they're going to maintain a connection with me […]")*	**Participated in the class action and replaced driver's license.**	**Financial illiterate** *("[…] doing your people justice by letting them continue to be financially illiterate. We need stronger financial literacy capabilities for our people and our consumers. But it doesn't stop there with being financially literate. You need to understand what you're doing. You need to read the policy and back to the elderly.")*	**Nonsense** *("I think it's absolute nonsense. They've tiptoed on the water. They haven't provided enough […]")*

4.3.1 Reflection on Phase One Interviews

DBNs, as mandatory disclosures to the public, are supposed to be clear and easily understandable complying the *Privacy Act 1988 (Cth)* (OAIC, 2024). However, findings from the Phase One interviews revealed recurring expressions in the transcripts that highlight significant interpretation challenges faced by affected individuals in understanding both the breach incident and notifications. These challenges paint a picture that individuals interpret breach notifications in ways that differ greatly from the expectations of their original intention and what lay individuals need does not seem to be satisfied. Based on empirical materials, I derived three representative expressions that can best describe what participants in Phase One interviews understand and require to see in breach notifications.

"I don't care"

The primary question guiding my inquiry is whether mandatory data breach notifications effectively fulfil their intended purpose. Unfortunately, the findings suggest that current DBNs are largely ineffective. Participants displayed a limited understanding of the breach itself and expressed indifference toward the notifications. Many participants had minimal recollection of the breach or its notification, with some admitting they even didn't open the letter initially, only learning about the breach later through media coverage or conversations with friends and family. For instance, Interviewee 1 reflected:

"[…] So, when that Latitude email came in saying that my identity had been breached, my immediate assumption was that was some kind of a phishing scam or some. And so, I ignored it, you know, as it turns out, it was a real incident, so it probably would have been better for me to be more aware of the vulnerability of my identity and the loss of my information."

With phrases like "I ignored it" and assumptions that the breach notification email was a scam suggest that current breach notifications are ineffective in their design. Perceived as "lacking personal touch and urgency" (Interviewee 1) these messages often fail to communicate the severity of the risk or prompt individuals to take appropriate protective actions. Additionally, several factors contribute to this weak awareness of data breaches among lay individuals. First, although the notifications aim to inform, ambiguous or overly general language may lead recipients to overlook the significance of the breach. This lack of clarity can result in an underestimation of the associated risks. Second, a lack of expertise and experience in handling breaches may lead to further disengagement and ignorance of the breach for lay individuals (Himick et al., 2016). Finally, participants were primarily sensitive to financial data; once they realised financial information was unaffected, many opted not to pursue additional actions.

"I'm confused"

The expression "confused" was also frequently noted in the interviews, underscoring a key challenge for lay individuals in interpreting breach notifications. Complex terminology, ambiguous language, and contradictory statements within the breach notifications often left recipients perplexed and dissatisfied. For example, wording like "*if you choose to replace your license*" not only left participants unclear about what "license" specifically referred to but also gave the impression that the responsibility of taking actions was being shifted back from the company. Just like Interviewee 3 shared:

"[…] Because that's where I go. Got completely confused. What does that mean? What did they exactly steal? And what do I have to be now worried about, so compromised was, I suppose, what stood out here."

Such confusion on disclosure language and details can foster a vicious cycle of indifference, as recipients who feel increasingly vulnerable and powerless may become less likely to engage with future DBNs. These interpretative challenges pose a significant barrier to lay individuals' ability to understand DBNs, impeding the communication of actionable information and potentially amplifying the psychological impact of the breach. Moreover, the ambiguous language also erodes trust, with some participants questioning the transparency and intentions of the breach organisation. To enhance the effectiveness of DBNs, organisations must prioritise clarity and precision, empowering individuals to take informed protective actions and reducing the risk of disengagement and mistrust.

"It's not a letter to me"

An interesting finding from the interviews was the general impression participants had of the breach notifications. Many noted that the letter followed a standard format, making it feel impersonal and generic rather than tailored to their specific circumstances. This perceived lack of personalisation led some recipients to feel that the notifications were routine, and sent indiscriminately to everyone affected, which significantly reduced their interest in and patience for reading the content in full. As a result, the efficacy of breach notifications appeared low, as recipients expressed a stronger desire for information directly addressing the personal implications of the breach rather than broad explanations about the incident. For instance, Interviewee 4 observed:

"[…] this part is basically telling me that they did everything that they had to do when these criminals did what they did. I still don't know anything about me. […] I suppose what they're saying here is that some third party is to blame and that they did everything afterwards. And now it's with Australian Federal Police and good luck. I don't know… So, you know, what is this helping me through the process?"

Another significant insight was that participants felt the notification letter lacked a strong, direct connection to them. This disconnect led several recipients to skim the letter or ignore it altogether, instead learning about the breach through external sources, such as news reports or conversations with friends and family. As a result, some recipients failed to recognise the severity of the situation in a timely manner, further limiting the breach letter's intended impact. Interviewee 4 expressed this feeling of detachment:

"[…] And it should tell me also how they know it's me. It's not. Oh, we're Latitude, and we're very sorry. You know. We're sorry you've been impacted. They need to tell me why they know me, because I don't know them."

Additionally, many interviewees expressed dissatisfaction with the utility of the contact information provided, such as phone numbers or website links, indicating that these resources did not effectively support their needs. Overall, individuals expressed multiple dilemmas in interpreting current breach notifications. Facing such challenges, a pertinent question then arises: *What do lay individuals most want to see in breach notifications?* Insights from Phase One suggest that current DBNs seem to be ineffective. Instead, breach victims are chiefly concerned with information directly related to their personal data, while general explanations appear secondary. These findings highlight the need for a more personalised, clear, and engaging approach to breach disclosures – one that informs recipients about specific risks and empowers them to take immediate, appropriate action.

Based on these findings, the subsequent phase of interviews focused on exploring the specific preferences and needs of lay individuals, delving deeper into the important characteristics that Phase One interviews indicated. This exploration aims to identify practical improvements in disclosure practices to better meet individuals' expectations.

4.4 Phase Two Interviews Analysis: Further Exploration on Interpretations

From the Phase One interviews, I gained an initial understanding of how lay individuals interpret current Latitude breach notifications – with multiple challenges to understanding, people describing them as ambiguous, generic, and lacking meaningful content. According to OAIC (2024), data breach notifications are intended to reduce the likelihood of harm to individuals. However, the current notifications fail to achieve that objective, leaving individuals' needs unmet and, in some cases, exacerbating their sense of vulnerability. Furthermore, participants expressed that their voices and concerns were largely unheard in the notification process.

This disconnect highlights an "expectation gap" among notification providers, breached individuals, and policymakers (Ruland & Lindblom, 1992). Based on this observation, the Phase Two interviews

aimed to expand the research focus by exploring what lay individuals prioritise in breach notifications, what information they seek and value, and how they interpret these notifications in ways that align with their personal needs and concerns.

4.4.1 What do lay individuals prioritise in breach notifications?

As revealed in Phase One, individuals do not want to receive a generic letter addressed to everyone. Instead, they prefer a notification tailored specifically to them. With a strong sense of self-identity, individuals are naturally most concerned about the section of the breach notification that discloses which of their personal information was compromised. Some participants explicitly mentioned that they would skip the initial parts of the letter and focus directly on the personal information section:

"[…] Well, at least that's identifying it is your personal information, it's the first time I've said yours, as in I've identified it's you. So, I would be jumping. Oh, my God! I'd be onto it straight away. First time I've seen the word "your", your personal information. Before it was very general. […]" (Interviewee 7)

The sensitivity of individuals to the type of personal information breached also varies significantly, with responses reflecting differing levels of concern. For instance, unchangeable or difficult-to-change information, such as birth dates or addresses, often elicits feelings of helplessness and indifference. Regarding the primary compromised information in the Latitude breach – driver's licenses – some participants indicated reluctance to replace their licenses. They cited the complexity of the process and the limited protection it offers, as only the license number can be changed, leaving other immutable information exposed.

In contrast, financial information breaches generate significantly heightened concern, with individuals expressing particular anxiety about the safety of their money. Some participants reported meticulously monitoring their bank accounts and bills daily to detect potential fraud. One participant (Interviewee 10) who continues to use Latitude's services explained:

"[…] Because the Medibank and the Optus happened before, and I think for customers, we can't do too much. Yeah. So, I only can do, maybe applying the credit ban. Maybe it can block the other people from stealing my financial information to get on the things. Maybe like stole my information to open new account or other things. Yeah, that's the only thing I think I can do."

Another critical concern for individuals is understanding what has happened to their personal information following a breach and the severity of the impact. Just as a participant (interviewee 14) stated:

"[…] it (the breach letter) is informative, but only to the extent that they're doing exactly what I would imagine the law requires them to do. […] I'm still uncertain as to the extent of the problem."

Participants also noted that the prevalence of scam messages and phishing emails following a breach has left them fatigued and increasingly distrustful. Just as one participant (Interviewee 11) pointed out:

"I find that they are potentially covering themselves that they've informed me… I don't know the seriousness of the problem unless I've been watching on the news."

After a breach, affected individuals are eager to know whether their personal information is secure and how the compromised data could potentially be misused. However, due to limited cybersecurity knowledge, lay individuals often find the information provided in breach notifications insufficient to address their concerns.

Additionally, lay individuals also express concerns about the actions taken by the breached organisation in response to the incident. Despite the challenges associated with interpreting breach notifications, I observed that some participants felt the information provided offered a degree of reassurance. This indicates that individuals care about the organisation's response and the steps it has taken. For example, when reading a statement detailing the cybersecurity organisations Latitude had contacted, one participant (Interviewee 7) remarked:

"That's comforting to know that. Look that last paragraph, you know, at least they've done the right thing. […]"

This sense of reassurance may stem from participants' relatively low expectations of breach letters, as they generally recognised these communications as standard disclosures rather than personalised communications. Most participants appeared to accept the generic tone and structure of the notifications, understanding that their purpose was to provide a broad explanation of the incident rather than personalised details. This information, though limited, offered some assurance and appeared to restore a degree of trust in the breached organisation.

4.4.2 What do lay individuals require to see in breach notifications?

Given the limitations of current breach notifications, this section builds upon the previous discussion of lay individuals' concerns regarding their personal information to further explore the three primary requirements that lay individuals expect to see in a breach notification.

The first and foremost requirement that lay individuals have for DBNs is ***clarity and definite expression***. Current breach notifications often fall short of meeting this standard, addressing relevant interpretation

challenges. For example, in scenario one, many participants (Interviewee 9) identified contradictions that created confusion about what personal information had been compromised:

"[…] But the first paragraph says, the following kinds of your personal information, then, it says, have not been compromised unless they… so are they telling you it's being compromised or not. That's confusing."

Such responses illustrate how the complexity and ambiguity of the language used in breach notifications can lead to misunderstanding. The reliance on standard templates and formal language in current breach notifications further exacerbates this issue, making it difficult for lay individuals – especially those lacking cyber-security knowledge or for whom English is a second language – to comprehend the key information in a breach letter. Therefore, in interviews, participants repeatedly expressed a need for clearer, more specific explanations presented in simple, plain language:

"Well, it's (Scenario one) sitting on the fence, the other one. […] As you get older, I had to say, we want definite. We haven't got time to be sitting on the fence. We could fall off a fence and die the next day. You know, we need definite. We need A and B. We haven't got time." (Interviewee 8)

This aversion to ambiguity reflects a broader preference for straightforward communication and highlights the detrimental impact of conditional or overly formal phrasing on the effectiveness of notifications. It underscores the importance of tailoring the language to ensure accessibility for all recipients, particularly those who may already feel vulnerable after a breach. These findings will be explored further in subsequent qualitative experiments to assess how clarity and specificity can enhance the effectiveness of breach notifications.

Another significant requirement identified by lay individuals is the ***need for ongoing updates***. Affected individuals consistently articulated a desire for receiving further information regarding the status of their personal information and the evolving consequences of the breach. However, most interviewed Latitude victims reported receiving no follow-up communication from the company. As noted by one interviewee:

"*It says we continue to update them on developments. So, they haven't said anything about updating me, and they haven't updated me, so I don't know what the outcome of this was. I don't know where… you know. I've received no further emails, but they didn't promise to send me any more emails. They said that they keep the OAIC. And the OPC and the ACSC, the AFP updated." (Interviewee 2)*

Due to the dynamic nature of breach situations and the continuous emergence of new findings during after-breach investigations, initial notifications are often perceived as insufficient to fully address individuals' concerns. Since alternative, reliable channels for obtaining updates on compromised personal data are often inaccessible or unverified, lay individuals are more likely to rely on breach notifications as a trusted source of information. Many participants described themselves as being in a state of "waiting" for an update, underscoring their expectation for continued engagement from the

breached organisation. Yet many organisations appear reluctant to issue follow-up disclosure, potentially to minimise reputational damage or avoid further scrutiny. This perceived disengagement or "silent treatment" (Le et al., 2019) can leave affected individuals in a prolonged state of uncertainty and emotional distress.

This finding highlights the critical responsibility of breached organisations to provide clear and ongoing updates about the status of breached personal information and the potential severity of its impact. Regular communication allows individuals to make informed, independent assessments of the potential risks and harms they may face (Andrew et al., 2023) and take appropriate actions, such as enrolling in credit monitoring services.

Notably, some participants interpreted the absence of further updates as an indication that the situation had not worsened. However, for many others, the lack of communication continuously heightened anxiety and confusion. This sense of abandonment led some individuals to seek redress and clarity through class actions, reflecting a broader loss of trust in the organisation's willingness to engage meaningfully post-breach.

The third critical requirement identified by lay individuals is ***making timely notifications***. This concept extends beyond organisations notifying affected individuals promptly after a breach is discovered but also encompasses ensuring that notifications are effectively delivered to the intended recipients without unnecessary delay. While participants generally acknowledged the inevitable gap between the discovery of a breach and the issuance of notifications, they highlighted additional factors – such as the breach letter's lack of connection with individuals, so that they did not trust the letter and did not open it – that can hinder the timely receipt of these notifications by certain individuals.

Furthermore, delayed notifications are often assumed to exacerbate the harm caused by breaches. One participant (Interviewee 11) remarked: *"I don't want to deal with it (the breach) because I think there is nothing can happen. The information is already stolen."* This sentiment underscores the passive position individuals often find themselves in following a breach, revealing their vulnerability and limited capacity to influence the situation. The combination of perceived powerlessness and restricted agency can foster feelings of indifference or resignation among affected individuals. To address these challenges, organisations must prioritise not only the prompt issuance of breach notifications but also the effective delivery of these communications. Ensuring that notifications are timely, transparent, and actionable can empower individuals to respond proactively, thereby mitigating the adverse effects of a data breach.

4.4.3 Why do lay individuals attempt to interpret breach notifications in these ways?

After examining individuals' concerns and their corresponding needs regarding breach notifications, this section aims to analyse the underlying factors contributing to the current state of breach notification effectiveness. These factors stem from both the design and content of the breach notifications themselves and broader societal issues, particularly the vulnerabilities and limitations of lay individuals.

Interviews reveal that current breach notifications are far from effective, leading to significant challenges in interpretation for recipients. These deficiencies not only impede understanding but also elicit unnecessary emotions such as mistrust and panic. First, one main reason that impeding the interpretation of breach notification is the ambiguity of the breach content. While current breach notifications often outline the types of personal information affected, their overall impact is weakened by vague and sometimes inappropriate language. For instance, participants highlighted dissatisfaction with phrases like *"if you choose to,"* arguing that such wording shifts responsibility to them rather than reflecting organisational accountability. Given the severity of data breaches, participants expected a more authoritative tone and clear, professional recommendations. They suggested alternative phrasing such as *"We highly recommend you..."* to emphasise the importance of taking specific actions and to instil a sense of urgency.

This lack of clarity is particularly problematic because the section addressing personal information is of paramount concern to affected individuals. Complex terminology and contradictory expressions further exacerbate the concerns, leaving laypersons confused about the implications of the breach notifications. This not only obstructs their ability to fully understand the situation but also disempowers them from taking timely remedial actions with confidence and urgency. By reducing ambiguity and adopting clearer language, breach notifications can enhance recipients' understanding, improve their response, and restore trust in the organisation's crisis management efforts.

Second, the structure of current breach notifications also undermines their effectiveness. While standardised formats lend a formal and authoritative tone and reduce the workload for breached organisations, they can feel impersonal to recipients. Some participants expressed that such letters lacked a personal connection, causing them to disregard the notification altogether or mistake it for phishing or scam letters. This disconnection significantly diminishes the intended impact of the notifications. To address these concerns, breach notifications must adopt a structure that is simple, clear, and engaging. A well-designed framework should capture recipients' attention quickly, communicate the seriousness of the issue, and build trust. Such a structure not only ensures that the recipients read and understand the notification but also maximises its efficacy by prompting timely and appropriate actions.

Meanwhile, it is also important to consider the inherent limitations and vulnerabilities of lay individuals

that impede their ability to interpret breach notifications effectively. During Phase Two interviews, two additional questions were introduced to explore participants' knowledge of data breaches: one asked them to define a data breach, and the other asked them to assess their level of cybersecurity knowledge. The findings revealed that most participants rated their understanding of data breaches as average or below average. Moreover, only half of the participants were familiar with key breach-related organisations, such as the Australian Cyber Security Centre (ACSC) and the Office of the Australian Information Commissioner (OAIC). These findings highlight a significant limitation in breach-related knowledge among lay individuals, emphasising their heightened vulnerability and the necessity for clarity and precision in breach notifications to ensure better comprehension.

Additionally, the interviews uncovered a general lack of awareness among participants regarding data breaches. Many individuals exhibited indifference toward breaches, resulting in a limited understanding of the severity and potential long-term harm. This lack of concern often led lay individuals to either disregard breach notifications entirely or initially perceive them as low risk, further limiting their ability to take protective measures against potential harm after a breach (Himick et al., 2016). The combined effect of insufficient knowledge and limited awareness presents a significant barrier to the effective interpretation of breach notifications. These factors not only reduce the likelihood of lay individuals understanding the gravity of a breach but also hinder their ability to respond appropriately. Addressing these challenges requires a dual approach: improving public education and awareness about data breaches and ensuring that breach notifications are accessible, straightforward, and actionable for lay individuals with varying levels of knowledge and concern.

The collective interpretations of lay individuals point to a general consensus that current breach notifications are largely ineffective and there is a specific "expectation gap" (Ruland & Lindblom, 1992) been the requirements of breach notifications provider (Latitude) and recipients (lay individuals). However, during the interviews, I found an alternative breach notification format – one that was short and clear. This format appeared to align more closely with the requirements of lay individuals discussed above. To further investigate individuals' preferences on breach notification, the Phase Two interviews concluded with an experiment presenting the Scenario Two statement. Participants were asked to evaluate their attitudes and preferences toward this alternative notification, enabling a deeper exploration of what, in the eyes of lay individuals, constitutes a more effective and less ambiguous breach notification.

4.5 Experiments on Lay Individual Preferences: Ambiguity Aversion

In the experiment, participants were asked to choose between two statements – one lengthy and vague, often perceived as contradictory, and the other specific and explicit, directly informing recipients that

their driver's license had been stolen – and the majority of participants (nine out of twelve) preferred the more specific and explicit statement (Scenario Two). Two participants expressed no particular preference, while one suggested a hybrid approach combining elements from both scenarios (more details is presented in Appendix C).

The choice of lay individuals in the designed qualitative experiments provides valuable insights into their underlying preferences regarding breach notifications. When participants were asked why they favoured Scenario Two, the majority emphasised its transparent and honest presentation of facts. In contrast, Scenario One was criticised for its vague and contradictory language, as well as its instruction for people to await further updates. Participants described this approach as *"sitting on the fence,"* reflecting their frustration with its lack of decisiveness and actionable information. Conversely, Scenario Two was praised for its specificity in detailing the breached information. As one participant noted (Interviewee 12), this level of clarity reassured them that other personal data was unaffected, enabling them to focus on taking immediate remedial actions:

"[…] because the other one (Scenario one) was all sort of vague, and it could be other things as well […] This is the only thing you have to worry about. But this is the thing. If you're going to fix something, just fix this. It is far more detailed. The other one was, was sort of vague and kind of left me thinking, what should I do? Should I do this, or should I do that? Oh, what should you do? There you go. Question!"

The straightforward and explicit nature of Scenario Two minimised ambiguity, alleviated participants' panic, and fostered a predominantly positive response. By clearly presenting the necessary information without unnecessary complexity and ambiguity, Scenario Two addressed participants' need for direct and honest communication, further validating its effectiveness as a preferred approach. This finding highlights the critical role of clarity and transparency in designing breach notifications that effectively engage and reassure recipients.

Meanwhile, an intriguing phenomenon also emerged during the qualitative experiments: although the scenario one statement is vaguer and more complex, as it lacks a definite conclusion about the breach impact, it implies that the ultimate consequence of the breach may be minimal. This suggests an uncertain outcome in which the individual's personal information remains uncompromised unless further disclosures are made. In contrast, the second scenario presents a clear negative outcome, explicitly stating that the driver's license has been stolen.

Analysing the preferences of lay individuals across the two scenarios reveals a consistent pattern: despite the first scenario's implication of a more favourable, or at least neutral outcome, participants were more comfortable with the certainty of the second scenario. They found the explicit and straightforward nature of Scenario Two disclosure more reassuring, even though it conveyed worse

news.[3] This finding highlights an important trend: given the limited information available in data breach notifications, lay individuals tend to prioritise clarity and directness over ambiguity, even if it means they need to pay more risks for negative outcomes (Du & Budescu, 2005).

The observed behaviour that participants appeared more comfortable with the certainty of a negative disclosure and prioritising disclosure clarity over a more favourable but more ambiguous result in the experiments aligns with Ellsberg's (1961) theory of ambiguity aversion, which posits that, when faced with uncertainty, individuals tend to prefer a definite outcome over an ambiguous alternative, reflecting ambiguity aversion a rational "protective" strategy under conditions of uncertainty and ambiguity (Al-Najjar & Weinstein, 2009). This tendency acknowledged evident among lay individuals, as they lack specialised knowledge and thus are more conservative and likely to place a higher value on transparency when limited information is available (Govindarajan, 2011). Such preference also aligns with the conventional assumption that accounting information users are "rational decision-makers" who make independent, value-neutral choices, and consistently select the optimal option for a clear objective (Young, 2006). A further illustration of the theoretical application of the "ambiguity aversion" theory will be made in Chapter 6.

Overall, this experiment reinforces the theoretical implications that DBNs should address the needs of lay individuals, who constitute the majority of disclosure recipients and avoid the ambiguity of the statement to a maximum extent. Providing clear, timely, and ongoing information – rather than ambiguous or incomplete disclosures – allows lay individuals to make informed decisions and take immediate remedial actions. By hearing the voices of lay individuals and reducing disclosure ambiguity, organisations can mitigate current "accountability failure", build trust with affected individuals, and provide a greater sense of after-breach control to affected individuals (Walker, 2005).

4.6 Analysis on Interviewee Demographics

Demographic characteristics are widely recognised as significant factors in shaping individuals' decision-making processes (Bulog, 2016). Accordingly, it is important to consider how different demographic factors may influence interviewees' interpretations of DBNs. Based on interview transcripts, several demographic factors were observed as potentially influential (see Table 4). However, due to the recruitment design, some factors were partially or fully controlled. First, by focusing exclusively on retired or semi-retired lay individuals, the study introduced homogeneity in demographic factors such as "data literacy" and "age". Second, the use of a passive snowball approach generated a

[3] The language used in Scenario One is notably ambiguous, leaving recipients uncertain about whether their information has been compromised until further updates are provided. In contrast, Scenario Two explicitly statement that individuals' driver's license has been stolen. As a result, the information in Scenario One is perceived as neutral, while the information in Scenario Two is perceived as definitively negative.

convenience sample largely drawn from specific social networks, limiting participant variation in socioeconomic status, particularly with regard to income and education, thus reducing the sample's representativeness (Wohl et al., 2017). Finally, for privacy and ethical reasons, factors such as educational background were not systematically collected unless voluntarily disclosed.

Given these constraints, the identified demographic factors were qualitatively categorised as having relatively high, medium, or low influence, based on two criteria: (1) whether the factor was explicitly mentioned by participants during interviews, and (2) whether the factor was implicitly controlled during recruitment. Factors frequently mentioned and not controlled (e.g., trust level) were classified as relatively high influence. Factors mentioned but to a certain degree controlled through recruitment (e.g., education) were considered to have a medium influence. Factors not mentioned were assessed as having relatively low influence on interpretation.

Although participants in this study shared broadly similar backgrounds – most from middle-class households with at least moderate levels of education, with several holding qualifications above the national average – many still struggled to interpret key sections of the breach notifications, particularly those containing ambiguous language. As noted in the pilot interview, *"And I'm highly educated. So again, when we read that part of the latitude statement about what was breached. It's actually really difficult. If you read that closely, it's difficult to understand what that means."* The difficulty in interpretation reinforces the study's central finding: current DBNs are not sufficiently accessible or effective for lay users. While the influence of demographic variation on individual interpretation requires further investigation, the consistent interpretative challenges across participants suggest these issues are widespread and not limited to specific social groups.

Nonetheless, it is important to acknowledge the limitations inherent in the empirical analysis. The partially controlled demographic profile of participants limits the extent to which the influence of specific demographic factors can be fully explored. Moreover, demographic factors may interact in complex ways; for instance, occupational background may directly influence participants' levels of data literacy, thereby shaping how they interpret DBNs. As such, future study is needed to engage with a broader and more diverse demographic spectrum to determine whether specific demographic factors significantly affect individuals' interpretation of DBNs, as well as the reciprocity among different factors. Subsequent studies would benefit from more representative sampling and a systematic investigation into how demographic characteristics shape individuals' understanding of DBNs and related decision-making processes.

Table 44: Demographic Factors and Influence

Interviewee Demographic Factors	Influence on DBNs Interpretation
Prior Breach Experience	Relatively High
Trust Level	Relatively High
Data Literacy	Medium
Education	Medium
Occupational Background	Medium
Income	Relatively Low
Gender	Relatively Low
Age	Relatively Low

4.7 Concluding Comments

This chapter presents the results and findings of the empirical study employing Petitmengin's (2006) micro-phenomenology interview and Steils' qualitative experiment (2021). Further, it has taken a critical approach to understand lay individuals' interpretation of DBNs and how they navigate the challenges facing the ineffectiveness of current breach disclosures. Moreover, this chapter provides novel perspectives on the real concerns and requirements of lay individuals in interpreting breach notifications, suggesting that while DBNs are often framed in standard and generalised language, the lack of clear, direct communication can hinder recipients' understanding and prompt confusion about the severity of the breach and the necessary actions they should take. Meanwhile, the qualitative experiment applied in this chapter indicates that lay individuals, who lack the specialised expertise to fully comprehend complex data breach disclosures, prefer the breach notifications that avoid relevant, unambiguous statements even when they convey more negative information. Finally, this chapter provides findings on challenges that lay individuals may face when interpreting data breach notifications, exploring potential improvements to develop a more effective breach notification framework.

CHAPTER 5 – DISCUSSION

5.0 Introduction

This chapter builds on the findings from the micro-phenomenological interviews and qualitative experiments that examine lay individuals' preferences to avoid ambiguity in DBNs. To better understand this preference, the theory of ambiguity aversion, as proposed by Ellsberg (1961), is employed to explore the reasons behind lay individuals' aversion to ambiguity in DBNs. Defined as a decision-maker's sensitivity to the lack of reliable information (Machina & Siniscalchi, 2014), ambiguity aversion highlights individuals' strong preference for information clarity over negativity. This tendency is particularly evident among lay individuals, as they lack specialised expertise, and thus are more short-sighted and conservative under uncertainty (Govindarajan, 2011).

The chapter commences in Section 5.1 by identifying five primary contributors to ambiguity in DBNs. Subsequently, Section 5.2 makes further articulation on why lay individuals prefer avoiding ambiguity in DBNs. It contrasts lay users with professional users of accounting information, emphasising how lay individuals' vulnerability and limitations make ambiguity aversion a rational choice in DBN interpretation (Gilboa & Schmeidler, 2001). This section also explores the "expectation gap" between lay individuals and organisations regarding disclosure efficacy (Ruland & Lindblom, 1992) and examines the "power dynamic" in disclosure practices (Carr & Beck, 2022). In addition, Section 5.3 extends to practical applications, offering insights into how ambiguity aversion theory can inform the design of more effective DBN frameworks. Finally, Section 5.4 provides the concluding remarks. By integrating theoretical analysis with practical recommendations, this chapter aims to contribute to the development of a clearer, more user-centred DBN framework that enhances individuals' ability to navigate the interpretation challenges posed by data breaches.

5.1 What causes the "ambiguity" in DBNs?

The empirical findings reveal that current DBNs are often too ambiguous to be effectively interpreted, thereby failing to adequately support affected individuals. However, the underlying factors contributing to this ambiguity remain insufficiently understood. According to Ellsberg's (1961) ambiguity aversion theory, ambiguity arises primarily from the absence of reliable information, which prevents individuals from forming confident beliefs (Al-Najjar & Weinstein, 2009). Building on an exploration of lay individuals' interpretations challenges in DBNs, this section examines five key reasons that contribute to the "lack of reliability" inherent in current breach notification information (Muzatko & Bansal, 2024). For each identified challenge, the discussion analyses the underlying factors that exacerbate these issues, providing a comprehensive assessment of the root causes of ambiguity.

5.1.1 Ambiguous Expression

DBNs are intended to "notify individuals at risk of serious harm" (OAIC, 2024) and prompt them to take necessary protective actions. However, the language used in current notifications often fails to meet this objective, creating one of the primary challenges for recipients: ambiguous expressions that hinder clear and effective interpretation. Although breach notifications can, to some extent, help alleviate panic (Chen et al., 2023), considerable confusion and interpretative challenges persist, which reinforce the ambiguity in DBNs.

One prominent source of this ambiguity in DBNs is the use of paradoxical statements. For instance, a notification section addressing compromised information began with, *"the following kinds of personal information have been compromised,"* but later followed by a contradictory statement stating that *"images of your identification documents have not been compromised."* Such contradictions create uncertainty about the specific data affected, leaving recipients ambiguous about the scope and severity of the breach. Furthermore, the use of complex terminology and overly lengthy phrasing adds to recipients' difficulties in understanding the information provided.

Instead of providing clarity, ambiguous expressions in current DBNs often heighten feelings of worry and distress among the recipients due to the unclear wording, undermining individuals' trust in the notification information. Such distrust further amplifies lay individuals' perceptions of the "lack of reliability" in the information presented (Muzatko & Bansal, 2024) and finally lead to their preferences on avoiding the ambiguity.

5.1.2 Unbalanced Disclosure

The empirical findings reveal that participants exhibited varied interpretations of DBNs: some criticised the notifications as overly lengthy and complex, finding it difficult to identify critical information amidst dense text, while others found them as excessively standardised and lacking the specific details necessary to address their concerns. This preference divergence in content and level of details underscores another key challenge for DBNs: achieving an optimal balance between clarity, relevance, and comprehensiveness in disclosures.

As stated in the existing literature, optimising the informativeness of disclosure remains a persistent challenge (Chen et al., 2023). Notifications that overwhelm recipients with excessive complexity can obscure essential information, leading to frustration and, in some cases, causing individuals to disregard the breach letter entirely. Conversely, notifications that lack sufficient detail often leave recipients dissatisfied, forcing them to seek clarification through additional inconvenient steps, such as contacting customer service. Both excessively detailed and overly simplistic DBNs undermine the opportunities for organisations to rebuild trust with affected individuals and repair their reputations by providing clear

and reliable information (Guo et al., 2023).

Additionally, the absence of ongoing updates about compromised personal information also contributes to the ambiguity of current breach notifications. Lay individuals expect timely and continuous notifications, and the lack of follow-up disclosure exacerbates the uncertainty stemming from insufficient information, heightening some recipients' anxiety and confusion.

For lay individuals, unbalanced disclosure can raise their concerns about potential unreported harm and further diminish their confidence in the organisation's information transparency. With the eroded public trust in the organisation, the ambiguous and unreliable breach notifications make it hard to form individuals' confident beliefs in the provided information (Al-Najjar & Weinstein, 2009), which further leads to lay individuals' preference for avoiding ambiguity in DBNs.

5.1.3 Standard Form

An overly standardised structure is also a significant factor contributing to ambiguity in DBNs. A common complaint raised during interviews was that current DBNs were perceived as *"too generic."* While the *Privacy Act 1988 (Cth)* does not mandate a specific structure for DBNs, organisations often spontaneously adhere to a standardised format, which led some participants to feel that the DBLs lacked a personalised connection. As one participant (Interviewee 2) noted, the breach notifications felt like *"a letter to everyone"* rather than a targeted letter designed to inform and assist him specifically. This generic approach undermined the credibility of the breach notifications, causing lay individuals to feel confused or even disregard the information provided.

More concerningly, lay individuals tend to be more sensitive and sceptical after experiencing a data breach. One participant (Interviewee 1) even noted that the generic language used in the DBLs led him to question the legitimacy of it, perceiving the breach notification as a potential scam email. This reaction highlights a critical limitation of current standardised notifications: instead of providing reassurance and clarity, standardised disclosures can inadvertently heighten recipients' sense of vulnerability and distrust, thereby increasing ambiguity in notification information.

5.1.4 Weak Consciousness

Ambiguity also stems from lay individuals' limited knowledge and awareness of data breaches and privacy issues. According to the *Australian Community Attitudes to Privacy Survey (OAIC, 2023a)*, while 90% of Australians recognise the importance of protecting their personal information – a notable increase from 85% in 2020 – only 21% rate their privacy knowledge as "very good" or "excellent". Although many Australians take basic precautions on their personal information, such as verifying email

and text links and using unique passwords, a substantial 57% report caring about data privacy but feeling uncertain about how to act on that concern. Furthermore, despite 84% expressing a strong desire for greater control over their personal information, half feel they have no meaningful choice when accepting the data policies of service providers. This data highlights the weak awareness of data breaches among the majority of lay individuals.

Insights from interviews further underscore this challenge. Many participants exhibited limited understanding of cybersecurity knowledge and weak awareness of data breaches, leaving them particularly vulnerable to associated risks. This lack of awareness often led participants to underestimate the severity of a breach or fail to recognise that they had been affected until informed by external sources such as news outlets or social media.

What is even more concerning is that DBLs often serve as the primary, and sometimes the only, source of formal information about a breach for lay individuals. Unlike professional users who can easily apply their expertise to understand DBNs and seek additional information (Kochetova & Salterio, 2003), most lay individuals passively rely on information provided in the notifications to understand the breach situation and obtain further instructions. However, given the ambiguity of current breach notifications, this reliance often results in feelings of helplessness and uncertainty. This sentiment was poignantly illustrated by one participant (Interviewee 6) in the interviews, describing her experience of contacting Latitude using the phone number provided in the breach letter:

"I advised whoever I had on the phone that I could not get through to them. Sorry we can't help you. You just have to refer to your (breach) letter and just wait to see what happens or try this number again."

Compared to expert users of DBNs, lay individuals are particularly vulnerable due to their limited knowledge and lack of access to additional resources. When interpreting DBNs, the internal contradiction and unreliability (Young, 2006) rooted in lay users not only hinder their ability to comprehend breach notifications but also impair their capacity to effectively use the provided information to make informed decisions and take appropriate protective measures. This further amplifies the inherent ambiguity of DBNs, as lay individuals with weak awareness are less equipped to interpret and act on the information provided effectively.

5.1.5 Ineffective Support and Accountability

The empirical findings also reveal a significant deficiency in the efficacy of support and accountability mechanisms provided by current DBNs. Although breach letters are designed to offer comprehensive instructions, such as links to relevant websites, customer service contacts, and, in some cases, compensation for document replacement, many participants reported not utilising these resources. This

low engagement stems primarily from a loss of trust in the organisation following the negative breach event (Guo et al., 2023), leading lay individuals to avoid the services provided in DBNs altogether. Some other breached individuals were discouraged by the perceived complexity of replacing compromised identity documents, ultimately choosing to take no action. These findings underscore the vulnerability and sense of abandonment experienced by lay individuals in the aftermath of a data breach, further amplifying the ambiguity of current DBNs.

Additionally, breach notifications often include conditional language such as *"if you choose to...,"* which suggests that breach organisations tend to shift remedial responsibility onto affected individuals rather than actively supporting them. Such phrasing risks reinforcing the perception that the organisation is using the breach notification to "evade accountability", exacerbating individuals' sense of isolation and distrust (Busco et al., 2006). As a result, current DBNs often fail to achieve their intended purpose of providing reliable information and support to affected individuals (OAIC, 2024). The lack of meaningful support and clear accountability leaves many individuals feeling ignored, increasing the ambiguity and ineffectiveness of current breach information.

Overall, ambiguity in DBNs arises from the inherent uncertainty and risks associated with insufficiently reliable information, making it difficult for recipients to fully understand the breach situation and make informed decisions (Ellsberg, 1961; Machina & Siniscalchi, 2014). This ambiguity heightens feelings of incompetence among lay individuals compared to more knowledgeable groups, such as professionals, further reinforcing their preference to avoid ambiguity in DBNs (Fox & Tversky, 1995). However, the underlying reasons behind this ambiguity aversion preference remain insufficiently explored. Therefore, in the next section, more illustrations will be drawn to explore why lay individuals prefer to avoid ambiguity in DBNs, even when clearer notifications may convey more negative information.

5.2 Why do lay individuals prefer to avoid ambiguity?

As demonstrated by OAIC (2024), the core objective of breach disclosures is to communicate effectively with affected individuals by providing clear, actionable information about the breach and reducing the likelihood of harm. However, the ambiguity presented in current breach notifications impairs lay individuals' ability to form confident beliefs and make informed decisions (Al-Najjar & Weinstein, 2009), exacerbates their vulnerability and heightens the risk of harm, prompting a natural inclination to avoid ambiguity. To further contextualise this response, this thesis draws on Ellsberg's (1961) theory of *Ambiguity Aversion* to further demonstrate lay individuals' tendency to avoid ambiguity of DBNs.

Different from lay users, professional users of accounting information are inherently less vulnerable to uncertainty as their expertise enables them to strategically utilise limited information to make rational

decisions (Himick et al., 2016). For instance, in the context of Enterprise Risk Management (ERM), experts demonstrate a strategic appetite for risk in terms of corporate governance (Allan et al., 2013). Their higher level of "risk tolerance" arises from the need to manage both risks and opportunities, integrating uncertainty into decision-making to achieve long-term value creation (Rittenberg & Martens, 2012). In corporate governance, risk appetite is a central element of strategy formulation, as professionals integrate risk as part of broader organisational goals (Govindarajan, 2011). Therefore, professional accounting information users are adept at navigating uncertainty and employ risk intelligence to balance potential threats with rewards, reflecting a proactive attitude to risk and ambiguity (Allan et al., 2013).

Unlike experts who can rely on their skills and expertise to acquire additional information, lay individuals face significant limitations due to their lack of specialised knowledge (Himick et al., 2016). This limitation is particularly evident in the context of data breaches, where uncertainty is heightened by unprecedented risks and constrained access to reliable information (Guo et al., 2023). Consequently, lay individuals become more vulnerable and acutely sensitive to ambiguous information in DBNs, which impedes their ability to accurately interpret and respond to the breach effectively. Furthermore, ambiguity aversion is driven by feelings of incompetence, often exacerbated by comparisons with individuals possessing greater knowledge, such as professionals (Fox & Tversky, 1995; Fox & Weber, 2002). As a result, the dominant ambiguity and ineffectiveness of current DBNs leave lay individuals with little choice but to adopt ambiguity aversion as a rational "protective" strategy when interpreting DBNs.

This finding first adds to the previous research that lay users tend to display multiple, conflicting, and inconsistent behaviours due to their lack of specialised knowledge and experience in using accounting information (Young, 2006). When interpreting DBNs, ambiguity aversion emerges as a rational and adaptive approach for lay individuals to mitigate uncertainty and minimise potential secondary harm (Gilboa & Schmeidler, 2001). Even when explicit notifications convey more negative information, lay users demonstrate a preference for clarity over ambiguity, viewing it as a means to protect themselves and stop future pitfalls (Du & Budescu, 2005).

Meanwhile, the study also reveals an "expectations gap" between organisations and lay individuals in the context of breach disclosure (Ruland & Lindblom, 1992). Current DBNs are predominantly ambiguous, reflecting a divergence between what lay individuals need – clear and actionable information driven by ambiguity aversion – and what organisations prioritise – fulfiling the disclosure obligations mandated by the *Privacy Act 1988 (Cth)*. As one participant (Interviewee 9) discussed, breach letters often resemble a "protective letter" designed to safeguard the organisation rather than a "helpful guidance" for affected individuals. This divergence between organisations and lay individuals mirrors prior accounting research on accountants' conflicting responsibilities to comply with

professional standards while addressing public interest concerns, highlighting a broader contest of interest in the perception of "fair disclosure" (Ruland & Lindblom, 1992).

By using ambiguous language in DBNs, organisations strategically maintain a neutral stance, which mitigates their legal and reputational risks. This ambiguity appears to serve organisational interests by allowing them to avoid full integrity and accountability for the breach. As a result, current DBNs typically adopt a "legalistic" tone that implies "kicking back" the responsibility to victims (Interview 9), reflecting a "power dynamic" where organisational priorities overshadow the needs of lay individuals (Carr & Beck, 2022). Therefore, the ambiguity aversion preference among lay individuals reflects a "contest of interest" between organisations and stakeholders. Such an imbalance in disclosure underscores the critical need to give voice to lay users, who are often left disempowered and individualised. Recognising this power dynamic is essential for addressing the significant gap in trust and accountability between the discloser and recipients of breach notifications (Busco et al., 2006). Despite their stated intentions, empirical evidence suggests that organisations primarily act in their own interests, prioritising self-preservation disclosure over the needs of affected individuals.

Additionally, current disclosures are dominantly stipulated from expert perspectives (Collins & Evans, 2019). However, experts tend to marginalise and dismiss alternative perspectives, viewing them as biased or uninformed (Jasanoff, 2003), which can result in a limited understanding of the broader implications of disclosures. Also, despite the limited engagement, most accounting disclosures still rely heavily on the information provided by experts and lay individuals are getting used to following the suggestions of experts, which hide their own voices and requirements (Himick et al., 2016). As there is a lack of participation of lay users in accounting practices, little is known about their decision-making processes (Young, 2006). It is encouraged that more lay individuals should participate in the processes of accounting practices. This highlights the importance of amplifying the voices and concerns of lay individuals in accounting practices to ensure data breach disclosures are accessible and meaningful to all stakeholders.

In conclusion, avoiding ambiguity in breach notifications is not only vital for lay individuals to reduce harm but also serves as a foundational step toward fostering a more transparent and accountable disclosure framework (Andrew et al., 2023). While lay individuals' ambiguity aversion may initially appear as a rational strategy (Gilboa & Schmeidler, 2001), it highlights the inadequacy of current breach notification practices, where lay individuals are left to a "contest of interest" with breach organisations. This underscores the need to give voice to individualised recipients and prioritise clarity and transparency in future data breach disclosure frameworks. By providing clear, reliable, and comprehensive breach information, organisations can also establish new norms of accountability, empower lay individuals, rebuild the trust with their stakeholders and ultimately enhance the resilience of the digital environment (Andrew et al., 2023).

5.3 How to better avoid ambiguity under the current DBN mechanism?

While data breach regulations are evolving, the *Privacy Act 1988 (Cth)* does not strictly mandate the format or content of DBNs, leaving their structure and language largely to the discretion of organisations. This discretion leads to significant variation in the nature, scale, and timeliness of DBNs (Andrew et al., 2023). As revealed in the preceding analysis, the ambiguous language often used by organisations in DBNs hampers individuals' ability to accurately assess the risks of a breach, impeding their capacity to take appropriate action and eroding trust in the organisation. In both phases of the interviews, participants frequently expressed sentiments such as, *"I did not trust the company anymore."* These interpretations indicate how current DBNs, despite their original purpose to inform and support affected individuals, often fail to demonstrate sufficient transparency and accountability, ultimately rendering them ineffective.

Compounding this issue is the general lack of knowledge and awareness about data breaches among lay individuals. This knowledge gap renders them inherently vulnerable within the "power dynamic" (Carr & Beck, 2022) between lay individuals, professionals, and organisations. Moreover, organisations often prioritise their own interests, sometimes employing ambiguous language to obscure critical information from affected individuals, regulators, or the broader market. Although OAIC publishes aggregated and anonymised reports on data breaches for public access, there is no mandatory requirement for organisations to disclose breaches to the wider public. This regulatory gap limits disclosure obligations and prevents the development of a more robust accountability framework that could emerge if organisations were required to publicly disclose their data security performance (Andrew et al., 2023).

Overall, the empirical findings indicate that the ambiguous nature of current DBNs fails to address the unique needs of lay individuals, resulting in responses ranging from confusion and indifference to outright distrust. This lack of transparency and accountability significantly diminishes the protective function of breach notifications (OAIC, 2024), erodes organisational credibility, and marginalises the voice of lay individuals. To address these issues, this section tries to provide targeted recommendations to reduce ambiguity in current breach notifications. By adopting a distinct perspective from lay individuals, this study proposes potential improvements to develop a more effective breach disclosure framework.

First, to address lay individuals' preference for ambiguity aversion, organisations should, at a minimum, provide clear, explicit notifications immediately after the breach, along with actionable guidance to protect affected individuals from secondary harm. Effective DBNs should include straightforward explanations of the incident, specify the personal information compromised, and outline potential impacts. Given the inherent variability and limitations (Young, 2006), clarity and conciseness are essential to minimise misinterpretation and empower lay individuals to take appropriate protective measures. Meanwhile, organisations should reinforce accountability within breach notifications by

offering tangible assistance options, such as guarantees of support and direct contact information for dedicated personnel. A proactive approach that directly addresses individual concerns not only improves the perceived reliability of notifications but also helps mitigate breaches of trust (Guo et al., 2023).

Secondly, to address the ambiguity arising from standardised formats and enhance the informativeness of disclosures (Chen et al., 2023), breach notifications should adopt a more personalised approach to build trust and foster a stronger connection with affected individuals. Personalised content, with clear and relevant details, can reduce scepticism and enhance the effectiveness of breach notifications, ensuring lay individuals feel informed and supported rather than overlooked. Furthermore, as recipients may skim breach letters, DBNs should prioritise engaging content that captures attention and reinforces trust from the outset (Guo et al., 2023).

Third, similar to traditional accounting disclosures, it is crucial to calibrate the content of breach notifications carefully (Schipper, 2007). A potentially effective solution is to adopt a more targeted approach, tailoring DBNs to meet the specific needs of different individuals. For example, individuals whose data was unaffected could receive brief notifications disclosing the incident and reassuring them about the safety of their personal information, while those affected should receive more detailed notifications, including specific disclosures about compromised information and actionable guidance. Furthermore, ongoing updates on breaches should also be provided timely to alleviate uncertainty and keep individuals informed. According to the FASB Conceptual Framework, disclosures should provide useful information for users to make rational decisions. As a novel form of disclosure, DBNs should align with such an objective by offering targeted information that helps lay users reduce information ambiguity and better address their diverse informational needs.

Finally, facing the grim challenges to data privacy, despite organisations' proactive role in ensuring transparency and clarity in DBNs, raising public awareness of data breaches and their potential consequences is also very essential (Karyda & Mitrou, 2016). By fostering a culture of privacy education and encouraging responsible data practices, organisations and policymakers can equip broader lay individuals with the tools and knowledge necessary to navigate the aftermath of a breach (Ashraf & Sunder, 2023). In doing so, empowered lay individuals can better safeguard their personal information, respond effectively to data breaches, and ultimately enhance public resilience to the growing threats to data privacy (Mayer et al., 2021).

In conclusion, future breach notifications must prioritise clarity, transparency, and accountability to reduce ambiguity and build trust (Andrew et al., 2023; Guo et al., 2023). By adopting a more personalised, targeted, and informative approach, organisations can substantially improve the effectiveness of current DBNs while fostering greater public confidence (Ashraf & Sunder, 2023). Meanwhile, to mitigate the lack of individual lay voices, organisations should actively seek feedback from the public to better understand their specific needs and concerns. Incorporating such feedback

would facilitate the delivery of more targeted, accessible, and accountable support that directly addresses the challenges faced by lay individuals. Addressing the gaps identified in current breach notification practices requires the development of more accessible, trustworthy, and user-centred notification mechanisms to help lay individuals effectively navigate the challenges posed by data breaches.

5.4 Concluding Comments

This chapter provides a comprehensive discussion of the empirical findings on lay individuals' preferences for ambiguity aversion in interpreting DBNs, examining the origins, impacts, and implications of ambiguity aversion from the perspective of lay individuals. Drawing on Ellsberg's (1961) ambiguity aversion theory, this chapter not only explores the factors contributing to ambiguity in DBNs but also contextualises lay individuals' preference for ambiguity aversion through their inherent vulnerability when faced with limited information compared to expert users of DBNs (Guo et al., 2023). Moreover, this chapter further discusses the underlying "contest of interest" between the needs of lay individuals and what organisations provide in DBNs, emphasising the existing "power dynamic" in the context of data breaches (Carr & Beck, 2022). Finally, this chapter offers targeted recommendations to enhance transparency, clarity, and accountability in DBNs, contributing to the development of a more effective and user-centred DBN framework.

CHAPTER 6 – CONCLUSION

6.0 Introduction

This chapter concludes the insights of the study, highlights its contributions and limitations, and proposes potential directions for future research.

6.1 Conclusion and Contributions

This study explored lay individuals' interpretations of DBNs through in-depth micro-phenomenological interviews and qualitative experiments. By amplifying the often-overlooked voices of lay users, it offered novel insights into DBNs, as a new form of disclosure, and broadened the understanding of their communicative functions. The findings inform recommendations for future breach disclosure frameworks that prioritise transparency, clarity, and accountability, thereby better addressing the needs of lay individuals and offering practical guidance for organisations and policymakers.

The literature review examined the relevant extant studies on interpretative accounting research (IAR), tracing the evolution of accounting information studies from focusing on its use to users, and emphasising the need to "rethink expertise" in accounting information use (Collins & Evans, 2019). It also established the legitimacy of data breach disclosure as a new form of accounting information, highlighting gaps in extant research on data breach notifications, especially from the perspectives of lay individuals. By incorporating Ellsberg's ambiguity aversion theory (1961), this study finally narrowed down the focus on lay users' understanding of DBNs under uncertainty.

The methodology part introduced micro-phenomenology as a novel approach to capturing individuals' subjective interpretations and another method called qualitative experiment to assess lay individuals' preferences in the face of ambiguity in DBNs. Additionally, the empirical study analysed the embedded factors driving lay individuals' preferences on ambiguity aversion and further discussed the "power dynamic" between notification providers and recipients caused by current ineffective DBNs (Carr & Beck, 2022). Applying Ellsberg's ambiguity aversion theory (1961) to the empirical data, the study provided insights into designing a clearer, more user-centred framework for future breach disclosures.

This study makes contributions in three dimensions. Theoretically, it challenges the traditional focus on professional users of accounting information by calling for a "rethinking of expertise" in the use of accounting information (Collins & Evans, 2019). By addressing the substantial vulnerabilities lay individuals face due to limited knowledge and expertise compared to their professional counterparts (Himick et al., 2016), the research fills a critical gap in the literature on accounting information use from the perspective of lay users. By demonstrating DBN as a new form of disclosure, this study extends Ellsberg's (1961) ambiguity aversion theory into the context of accounting information interpretation

from a novel perspective of lay individuals. This study also provides theoretical insights into lay users' conservative "risk appetite" in the face of uncertainty, explaining their preference for clarity over negativity in breach information as a rational "protective" strategy, contrasting with the proactive attitude professional users possess to risk and ambiguity (Allan et al., 2013; Govindarajan, 2011). Finally, regarding the ambiguity in current DBNs, this study further reveals the "power dynamic" inherent in breach disclosure, identifying a "contest of interest" between breached organisations as the information providers and lay individuals as recipients (Ruland & Lindblom, 1992). By emphasising how ambiguity in DBNs can exacerbate these dynamics, the research underscores the need for greater transparency and clarity in DBNs, contributing to broader discussions on accountability and trust in disclosure practices.

Methodologically, this study introduces micro-phenomenology as an innovative interview method to better capture nuanced first-person accounts and subjective interpretations from an inductive approach (Petitmengin, 2006). Additionally, it employs qualitative experiments to further explore lay individuals' preferences on DBN interpretations through a complementary deductive approach (Heimann et al., 2023). By extending traditional qualitative methods, this study contributes to a more "exploratory and heuristic" nature of research methodology, which enhances both the validity and interpretive depth of findings (Kleining, 1986).

Practically, this study provides empirical evidence on how lay individuals interpret DBNs, offering valuable insights for individuals, organisations and policymakers. Findings first reveal a persistent knowledge gap between lay individuals and their professional counterparts, underscoring the need for disclosure frameworks that better address the needs of the majority of users. Given lay individuals' increasing sensitivity and vulnerability amid frequent cybersecurity incidents, current DBNs – often characterised by excessive ambiguity – fail to effectively engage or inform lay users. Consequently, participants consistently expressed a preference for clarity, specificity, and user-focused messaging over negative or vague disclosures. Therefore, drawing on principles from accounting disclosures practices (Schipper, 2007), this study recommends a calibrated approach for current DBNS: brief, reassuring notifications for unaffected individuals to minimise unnecessary panic caused by excessive interpretation, and detailed, consistent disclosures for affected individuals, outlining compromised information and providing actionable guidance to maximise the disclosure effectiveness and empower lay individuals to take appropriate protective actions.

For organisations, this study reveals that clear and explicit DBNs should be issued promptly following a breach. Organisations should also actively engage with affected individuals to better understand their needs, thereby ensuring that the DBNs they issue provide straightforward explanations, specify compromised data, and outline potential impacts. To overcome the limitations of standardised formats (Chen et al., 2023) and strengthen user trust, DBNs should adopt a more personalised approach,

delivering relevant and engaging content tailored to recipients' needs. Additionally, organisations should reinforce disclosure accountability by offering tangible support measures, such as guarantees of assistance and direct contact information for dedicated personnel. Furthermore, acknowledging that lay individuals often skim breach letters, notifications should prioritise concise, attention-grabbing content that reassures users and demonstrates organisational responsibility.

For policymakers, this study highlights critical regulatory gaps in the current dominant mandatory DBNs regimes, where disclosure practices remain largely at the discretion of breached organisations. Such discretion can significantly impede lay individuals' interpretation of DBNs, exacerbating transparency and accountability issues, and neglecting broader public interests. To address these shortcomings, it is imperative for policymakers to standardise disclosure frameworks, ensuring that DBNs are accessible, specific, and responsive to the needs of lay users. Additionally, policymakers could consider introducing incentive mechanisms to promote disclosure quality, such as recognising organisations for exemplary data breach disclosure practices, as seen in the OAIC's commendation of Redcross Lifeblood (OAIC, 2017). Beyond improving the quality of DBNs, fostering public awareness about data breaches and privacy risks remains essential (Karyda & Mitrou, 2016; Ashraf & Sunder, 2023). By advancing privacy education and responsible data practices, policymakers can empower individuals to better safeguard their information and enhance societal resilience against data breach threats (Mayer et al., 2021).

6.2 Limitations

While this study provides valuable insights into lay users' interpretations of DBNs, several limitations should be acknowledged. First, due to challenges in participant recruitment, the sample size was relatively small, consisting of only sixteen participants. Although the in-depth micro-phenomenological approach facilitated rich, nuanced insights into individual interpretations, the limited sample size constrains the generalisability of the findings. Furthermore, as discussed in Section 4.6, the recruitment design implicitly restricted the inclusion of diverse demographic groups. Consequently, some demographic factors – such as participants' occupational backgrounds and socioeconomic status– were not fully captured, and the reciprocity among different demographic factors remains underexplored. These limitations reduce the study's ability to reflect the full spectrum of public perspectives, thereby affecting the overall representativeness of its findings.

Second, the study focuses exclusively on DBNs issued by Latitude Financial. While this specific case provides a concrete and relevant context for exploring participants' interpretations toward one type of DBN, it may limit the applicability of the findings to other forms of DBNs. For example, alternative disclosures made via social media or those involving breaches of differing severity and visibility may

elicit different public responses from affected individuals. These variations in disclosure approach and situational context were not examined in the present study.

Finally, the study does not consider potential external influences, including media coverage, social networks, and expert advice, which may significantly shape individuals' interpretations of breach disclosures (Mayer et al., 2021). While such influences are likely to play a critical role in lay individuals' interpretations, they fall beyond the analytical scope of this research. Acknowledging these limitations, the following section outlines avenues for future research that could address these gaps and further contribute to the development of more effective and inclusive data breach disclosure practices.

6.3 Implications for Future Research

In light of the methodological limitations identified in this study, future research could first aim to expand the participant pool and adopt more inclusive recruitment strategies to capture a broader and more diverse demographic range. Specifically, incorporating participants from varied occupational, educational, and socioeconomic backgrounds would allow for a more comprehensive analysis of how these demographic factors, and their potential reciprocity, influence individual interpretations of DBNs. Future studies could also employ comparative designs to examine different types of breach disclosures, including those delivered via social media, organisational websites, or traditional media, as well as disclosures involving breaches of varying severity and public visibility. Such comparative work would help to uncover context-specific patterns in public interpretation and response. Moreover, future research could account for external influences, such as media narratives, social networks, and expert commentary, in shaping individuals' understanding of DBNs (Mayer et al., 2021). Addressing these areas would not only enhance the generalisability and representativeness of findings but also inform the development of more tailored, comprehensive, and effective data breach communication strategies.

Beyond methodological insights, this study also raises theoretical and empirical implications that enlighten future research. A recurring theme across interviews was the erosion of trust in the breached organisation. As said by one participant (Interviewee 10): *"Whatever they say at the moment, it's not going to win me back. I would never use them again."* This finding underscores the need to explore the dynamic interplay between individual trust and disclosure (Tomkins, 2001), particularly how individual trust evolves after data breaches. Conceptualised as "societal capital," trust sustains social structures by facilitating human interactions and relationships (Putnam, 1994). Within the accounting domain, it is widely regarded as an intangible asset critical to regulatory functioning and organisational legitimacy (Baldvinsdottir et al., 2011; Guthrie, 2001). Yet, in what Hardin (2006) characterises as an "age of distrust," trust remains inherently fragile (Kramer, 1999) and highly susceptible to erosion during periods of organisational crisis.

Following the global credit crisis, accounting scholars have increasingly examined the breakdown and repair of trust (Kim et al., 2004). While some studies, such as Guo et al.'s (2023) work on the effects of disclosure and trust after negative events in charitable sectors, highlight the potential of disclosure to facilitate trust repair, much of this literature still adopts a linear view centred on institutional actors (Hyndman & McConville, 2018). This framing often neglects the reciprocal dynamics between disclosure and trust, especially from the standpoint of lay individuals who may be more susceptible to "accountability failure" due to limited access to expertise or information (Walker, 2005). Although disclosures are frequently framed as mechanisms for repairing trust (Kim et al., 2004), the processes through which individuals interpret and respond to these efforts remain underexplored.

Building on the findings of this study, future research could also investigate how individual trust, functioning as a substitute for formal accounting mechanisms in reducing uncertainty (Tomkins, 2001), develops or deteriorates in response to DBNs. In addition, future studies could examine DBNs as strategic impression management tools used by breached organisations in crisis. As prior research indicates that organisations often minimise negative information while amplifying positive messaging through social media disclosures (Yang & Liu, 2017), future research could further explore the "power dynamics" between organisations and lay individuals by investigating the potential disjunction between organisational disclosure strategies and public expectations. Such inquiry would offer critical insights into the contested nature of trust and contribute to enhancing the communicative effectiveness of DBNs in mitigating perceived accountability failures (Walker, 2005).

6.4 Concluding Comments

This chapter concludes this thesis by summarising the findings and outlining its theoretical, methodological and practical contributions, alongside its limitations and future research avenues. By offering new insights into how lay individuals interpret data breach disclosures, the study advances understanding across multiple dimensions. Nonetheless, limitations such as recruitment challenges signal opportunities for methodological refinement. Drawing on the findings, the study advocates for the development of more direct, clear, and targeted DBN frameworks to better support affected individuals and restore trust. Several avenues for future research have also been proposed to deepen and extend this line of inquiry.

APPENDICES

Appendix A: Example of Latitude Financial Data Breach Letter

Dear xxx,

Latitude recently experienced a significant and malicious cyber-attack, which resulted in data being stolen from our systems. It is with deep regret that I am sharing with you that some of your personal information was compromised.

As Latitude's incoming CEO, I want to apologise for the impact that this incident has had on you. Know that we are committed to helping you through this process and hope that, in time, we are able to win back your trust.

This email explains what happened, the support we are offering you and the precautions we recommend you take to lower the risk of your information being potentially misused. Be assured, if you choose to replace your license, we will reimburse you.

Please take a moment to review the information below and contact us with any additional questions or concerns that you may have. Our dedicated customer service team is ready to help and can be reached on (AU) 1300 793 416 or (NZ) 0800 777 885, 9am – 6pm, Monday – Friday.

You can also stay up to date with the latest information on this matter by visiting our website: latitudefinancial.com.au/latitude-cyber-incident.

Again, please accept my sincere apology. Know that we are working around the clock to restore our systems safely and to ensure that you are supported throughout this process.

Sincerely,

Bob Belan

Chief Executive Officer (Designate)

Latitude Financial Services

What happened?

Latitude experienced a malicious cyber-attack that has resulted in a data theft.

Our investigation has identified that the attacker used compromised login credentials, obtained via a third-party, to access Latitude's network and steal personal information.

We immediately alerted relevant authorities and law enforcement agencies, including the Australian Cyber Security Centre (ACSC) and the Australian Federal Police (AFP), and engaged external cyber security specialists to work alongside our own teams.

This crime is now under investigation by the AFP.

We also notified the Office of the Australian Information Commissioner (**OAIC**) and the New Zealand Office of the Privacy Commissioner (**OPC**) about this incident on 16 March 2023, and we continue to update them on developments.

What kind of information has been impacted?

We have so far identified that the attack resulted in the following kinds of your personal information being compromised. This information was collected from you at the time you applied for credit from Latitude or our predecessor companies.

Unless we have explicitly notified you, images of your identification document(s) have **not** been compromised.

· The license number on the driver license you provided us as part of your application.

· The personal information you provided us as part of your application which, where applicable, included your full name, address, date of birth and phone number.

If we identify any other of your personal information has been compromised, we will notify you as quickly as possible.

Steps we are taking to help you.

Replacement of identity documents

Please visit our website latitude**financial.com.au/**latitude-**id-information** and go to the relevant identify document page for guidance on

what to do.

Please read the guidance carefully. In many cases, you may not need to replace your identity document.

We are working with government agencies/departments to streamline the process and avoid you being charged for any required replacement of your license.

If you choose to replace your license before this process has been set up, Latitude will reimburse you for the replacement cost. Please retain a copy of your payment receipt and we will advise you of the reimbursement process once our system functionality has been restored.

Latitude *Dedicated Contact Centre*

We have established dedicated contact centers which are available 9am – 6pm, Monday – Friday on (AU) 1300 793 416 or (NZ) 0800 777 885.

Our teams can help you understand the information provided in this letter. Please be aware that wait times may be much longer than we would like.

Support is available for customers who are in a uniquely vulnerable position as a result of this incident. Our dedicated contact center teams will be able to provide direct access to the support we have available.

IDCARE Support

Latitude has partnered with IDCARE, Australia and New Zealand's national identity and cyber support community service. They have expert Case Managers who can work with you in addressing concerns in relation to personal information risks and any instances where you think your information may have been misused. IDCARE's services are at no cost to you.

If you wish to speak with one of their expert Case Managers, please visit idcare.org or call (AU) 1800 595 160 or (NZ) 0800 121 068, Monday – Friday (excluding public holidays).

When engaging IDCARE, please use the referral code LAT23.

Mental Health Support Line

Mental Health and Wellbeing Support is also available free of charge through our Support Lines on (AU) 1800 808 374 or (NZ) 0800 808 374.

Steps you can take to protect yourself.

There are immediate precautions that you can take:

You can contact one of Australia's credit reporting agencies for a credit report to check if your identity has been used to obtain credit without your knowledge.

In New Zealand, you can check your credit record to confirm if your identity has been used to obtain credit without your knowledge. For further information, please refer to: govt.nz/browse/consumer-rights-and-complaints/debt-and-credit-records/check-your-own-credit-report.

You can also request the agencies to place a credit ban or suspension on your credit file via their website or by contacting them directly. Please be aware that you will not be able to apply for credit while the ban or suspension is in place.

Illion

AU 1300 734 806 or illion.com.au/credit-report-ban-request

NZ 0800 733 707 or illion.co.nz

Equifax

AU 138 332 or equifax.com.au/eform/submit/credit-ban

NZ 0800 692 733 or equifax.co.nz/credit-file-suppression.

Experian

AU 1300 783 684 or experian.com.au/consumer/request-a-ban

Centrix

NZ 0800 236 874 or centrix.co.nz/my-credit-score/suppress-your-credit-file.

You can find information on how you can protect yourself from the Australian Government at cyber.gov.au or the New Zealand Office of the Privacy Commissioner at privacy.org.nz/resources-2/protecting-yourself-from-a-privacy-breach.

Be alert for any phishing scams that may be sent via SMS, phone, email or post.

You should always verify the sender of any communications you receive to ensure they are legitimate.

You should never click on links contained in SMS or email messages unless you know they are from a legitimate source.

Be careful when opening or responding to texts from unknown or suspicious numbers.

Be careful when answering calls from private numbers or callers originating from unusual geographic locations.

You should regularly update your passwords and ensure they are strong. You should use multi-factor authentication where possible.

Further information

The latest information is available on our dedicated webpage: latitudefinancial.com.au/latitude-cyber-incident

You can also view Latitude's announcements to the ASX via the 'News Room' on our website: latitudefinancial.com.au/about-us/news-room

On behalf of the team at Latitude, I am very sorry that I have had to send you this email. Thank you for your understanding and patience.

Appendix B: Timeline of Latitude Financial Breach

- ***16 March 2023***

  Latitude Financial detected unusual activity and immediately informed the Australian Stock Exchange (ASX). The incident was described as a "sophisticated and malicious cyber-attack", believed to have originated from a major vendor used by Latitude. The attacker obtained Latitude employee login credentials, which were then used to access and steal personal information from two other service providers.

- ***17 March 2023***

  Affected customers began receiving breach notification letters from Latitude Financial.

- ***20 March 2023***

  Latitude Financial provided an update to the ASX, confirming the initial data loss.

- ***22 March 2023***

  Latitude Financial updated the ASX, stating that while no further data had been stolen since 16 March 2023, a forensic review revealed additional large-scale information theft, affecting customers and applicants in both Australia and New Zealand.

- ***27 March 2023***

  Latitude Financial disclosed to the ASX that approximately 7.9 million Australian and New Zealand driver's licence numbers had been stolen, of which around 3.2 million (40%) were issued in the last 10 years. In addition, approximately 53,000 passport numbers were stolen, and less than 100 customers had a monthly financial statement compromised.

- ***28 March 2023***

  Gordon Legal and Hayden Stephens Associates launched an investigation into the data breach. The investigation aimed to scrutinize the circumstances surrounding the cyber-attack, including the adequacy of Latitude Financial security measures and whether appropriate steps were taken to protect customers' personal information.

- ***11 April 2023***

  Latitude Financial informed ASX that it had received a ransom demand from the attackers. The company decided not to pay the ransom, aligning with the stance of the Australian Government.

Appendix C: List of Phase Two Interviewees

	Response to general part	Response to special part	Attitude	Insights on Scenario 1	Key insights after reading	Preference
Interviewee 5	General statement but a bit comforting.	More personally related, first time to see "your".	Might follow the letter and replace license.	Confused on what personal information has been impacted.	Stressed and worried; Old people especially want definite.	**Scenario 2**
Interviewee 6	A protective letter. All the information provided is below expectation but not helpful enough.	Strange wording and unsettling; More informed but don't know other personal information could be compromised.	Need more information (e.g. news) to make judgement.	Expect to have continuous reporting about the personal information situation of all the impacted people.	A letter for everyone. Uncertain as to the extent of the breach. People should also know how the loss of information can be used to fight against them.	**No preference.** Scenario 2 is what was implied in the scenario one
Interviewee 7	Feel vague about what happened. worry on what disclosed and even more concerned about what hasn't been disclosed.	The letter is unclear about the reimbursement process, and it doesn't ease the fact that information was breached.	Probably will call the company.	More uncertainty is created as the letter proceeds and the actual anger about what's happened hasn't been removed.	Disclosures only stop the possibility of future issues but do not prevent the occurrence of issues.	**Scenario 2** sounds better.
Interviewee 8	Half understand the letter.	Fairly clear. But still need all the affected information been affected included rather than generally included.	Waiting for the update.	Half-telling the information.	Wants to know the situation of all the other information.	**Scenario 2**
Interviewee 9	Panic but happier about the disclose of information.	Wondering what personal information has been provided.	Don't want a phone call.	Vague statement left stress.	Suspicious of emails especially after breach.	**Scenario 2**
Interviewee 10	Get used to the general statement.	Detailed and rather hard to understand. Confusing.	Don't want to make any actions.	General statement and assuming another explicit notification will be proceeded.	More price sensitive. But in terms of carefulness, assuming everything is safe.	**No preference.**
Interviewee 11	Wants to have more specific information about what happened.	Confused about what happened.	Be nervous in the future and not interested in trying the other products of the company.	Still wants the letter to be more detailed and specific.	Negative expressions (e.g. unless we notify you, your information has not been compromised) annoys people.	**Scenario 2** is more honest.
Interviewee 12	Standard statement. Very vague and generic.	Not entirely clear.	Choose not to replace anything.	Won't do anything until receiving definite instructions.	Offerings should be straightforward to the information compromised or it may cause confusion.	**Prefer a mixture of two** (both not entirely clear)

Interviewee 13	Not helpful at all.	The meaning is not clear.	No action. Waste of time.	Expression is incomplete, poorly drafted and confusing.	Start to worry about the company's overall internal control.	**Scenario 2**
Interviewee 14	"It is nothing in there that would give anyone confidence in their competence."	Confused.	Decide not to worry about things.	Hasn't used clear language.	The company is trying to put all the work on affected individuals. Older people need clarity.	**Scenario 2** (clear and in simple English)
Interviewee 15	Better than doing nothing but still expect more details.	Have some anxieties about the downstream risks.	Call the company and figure out the extent of the information been stolen.	Basically understand what they are saying.	Keep anxious and unhappy about what potential information can be used. Wants the facts.	**Scenario 2** (very specific)
Interviewee 16	Only introductory statement and would rather skim and turn to more serious information.	General letter, don't have enough information.	Will directly replace the license to save time.	Not complete and only giving examples.	The company didn't want to spend money, so they just sent a mass letter that is general and covers every possible option or most options.	**Scenario 2** (less vague from the first scenario)

REFERENCES

Abdallah, A. A. J. (2013). The impact of using accounting information systems on the quality of financial statements submitted to the income and sales tax department in Jordan. *European Scientific Journal*, 1(4), 41-48. Retrieved from https://scholar.google.com.au/scholar?hl=en&as_sdt=0,5&q=Abdallah,+A.+A.+J.+%282013%29.+The+impact+of+using+accounting+information+systems+on+the+quality+of+financial+statements+submitted+to+the+income+and+sales+tax+department+in+Jordan.+European+Scientific+Journal,+1%284%29,+41-48.&btnG=

Abdul-Khalid, S. N. (2009). Sensemaking in interpretive management accounting research: constructing a credible account. *International Journal of Qualitative Methods*, 8(1), 41-53. https://doi.org/10.1177/160940690900800104

Abu, B., Aishah, S., & Rashid, A. (2010). Readability of corporate social responsibility communication in Malaysia. *Corporate Social Responsibility and Environmental Management*, 18(1), 50-60. https://doi.org/10.1002/csr.240

Adelberg, A. H. (1979). A methodology for measuring the understandability of financial report messages. *Journal of Accounting Research*, 565-592. https://doi.org/10.2307/2490519

Aerts, W. (1994). On the use of accounting logic as an explanatory category in narrative accounting disclosures. *Accounting, organisations and society*, *19*(4-5), 337-353. https://doi.org/10.1016/0361-3682(94)90001-9

Ahrens, T., & Chapman, C. S. (2006). Doing qualitative field research in management accounting: Positioning data to contribute to theory. *Accounting, Organisations and Society*, 31(8), 819-841. http://dx.doi.org/10.2139/ssrn.816985

AICPA. (1994). Improving Business Reporting – a customer focus. Author. Retrieved from http://www.aicpa.org/InterestAreas/FRC/AccountingFinancialReporting/DownloadableDocuments/Jenkins%20Committee%20Report.pdf

Alam, M. K. (2024). Does the relationship between the interviewer and interviewee matter in qualitative research. *ICRRD Quality Index Research Journal*, *5*(1), 140-145. https://doi.org/10.53272/icrrd.v5i1.5

Albeshri, A., & Thayananthan, V. (2018). Analytical techniques for decision-making on information security for big data breaches. *International Journal of Information Technology & Decision Making*, *17*(02), 527-545. https://doi.org/10.1142/S0219622017500432

Alcaraz-Sanchez, A. (2023). Awareness in the void: a micro-phenomenological exploration of conscious dreamless sleep. *Phenomenology and the Cognitive Sciences*, 22(4), 867-905. https://doi.org/10.1007/s11097-021-09743-0

Allan, N., Cantle, N., Godfrey, P., & Yin, Y. (2013). A review of the use of complex systems applied to risk appetite and emerging risks in ERM practice: Recommendations for practical tools to help risk professionals tackle the problems of risk appetite and emerging risk. *British Actuarial Journal*, *18*(1), 163-234. https://doi.org/10.1017/S1357321713000135

Al-Najjar, N. I., & Weinstein, J. (2009). Rejoinder: The "ambiguity aversion literature: A Critical Assessment" *Economics & Philosophy*, *25*(3), 249-284. https://doi.org/10.1017/S0266267109990289

Al-Shubiri, F. N., Al-Abedallat, A. Z., & Orabi, M. M. A. (2012). Financial and non-financial determinants of corporate social responsibility. *Asian Economic and Financial Review*, 2(8), 1001. Retrieved from https://www.proquest.com/scholarly-journals/financial-non-determinants-corporate-social/docview/1417571919/se-2

Amir, E., & Lev, B. (1996). Value-relevance of nonfinancial information: The wireless communications industry. *Journal of accounting and economics*, 22(1-3), 3-30. https://doi.org/10.1016/S0165-

4101(96)00430-2

Anderson, S. W., & Sedatole, K. (1998). Designing quality into products: The use of accounting data in new product development. *Accounting Horizons*, *12*(3), 213. Retrieved from https://www.proquest.com/scholarly-journals/designing-quality-into-products-use-accounting/docview/208911591/se-2

Andrew, J., Baker, M., & Huang, C. (2023). Data breaches in the age of surveillance capitalism: Do disclosures have a new role to play? *Critical Perspectives on Accounting*, 90, 102396. https://doi.org/10.1016/j.cpa.2021.102396

Ansari, S., & Euske, K. J. (1987). Rational, rationalizing, and reifying uses of accounting data in organisations. *Accounting, Organisations and Society*, *12*(6), 549-570. https://doi.org/10.1016/0361-3682(87)90008-0

Argyris, C. (1952). Diagnosing defenses against the outsider. *Journal of Social Issues*, *8*(3), 24-34. https://doi.org/10.1111/j.1540-4560.1952.tb01615.x

Arrington, C. E., & Francis, J. R. (1989). Letting the chat out of the bag: deconstruction, privilege and accounting research. *Accounting, Organisations and Society*, 14(1-2), 1-28. https://doi.org/10.1016/0361-3682(89)90030-5

Arrington, C. E., & Francis, J. R. (1993). Giving economic accounts: accounting as cultural practice. *Accounting, Organisations and Society*, 18(2-3), 107-124. https://doi.org/10.1016/0361-3682(93)90029-6

Arvidsson, S. (2011). Disclosure of non-financial information in the annual report: A management-team perspective. *Journal of intellectual capital*, 12(2), 277-300. https://doi.org/10.1108/14691931111123421

Ashraf, M. (2022). The role of peer events in corporate governance: Evidence from data breaches. *The Accounting Review*, 97(2), 1-24. https://doi.org/10.2308/TAR-2019-1033

Ashraf, M., & Sunder, J. (2023). Can shareholders benefit from consumer protection disclosure mandates? Evidence from data breach disclosure laws. *The Accounting Review*, *98*(4), 1-32. https://doi.org/10.2308/TAR-2020-0787

Avery, A. (2021). After the disclosure: measuring the short-term and long-term impacts of data breach disclosures on the financial performance of organizations, *Information and Computer Security*, 29(3), 500-525. https://doi.org/10.1108/ICS-10-2020-0161

Bailin, A., & Grafstein, A. (2016). *Readability: Text and context.* Springer. https://doi.org/10.1057/9781137388773

Baker, C. R., & Bettner, M. S. (1997). Interpretive and critical research in accounting: a commentary on its absence from mainstream accounting research. *Critical Perspectives on Accounting*, *8*(4), 293-310. https://doi.org/10.1006/cpac.1996.0116

Baldvinsdottir, G., Hagberg, A., Johansson, I. L., Jonäll, K., & Marton, J. (2011). Accounting research and trust: a literature review. *Qualitative Research in Accounting & Management*, *8*(4), 382-424. https://doi.org/10.1108/11766091111189891

Barrett, J. (2023, March 27). Latitude financial cyber-attack worse than first thought with 14m Customer Records stolen. *The Guardian*. Retrieved from https://www.theguardian.com/australia-news/2023/mar/27/latitude-financial-cyber-data-breach-hack-14m-customer-records-stolen

Bartlett, F. C. (1995). *Remembering: A study in experimental and social psychology*. Cambridge university press. https://doi.org/10.1017/CBO9780511759185

Becker, S., & Brownson, F. (1964). What Price Ambiguity? or the Role of Ambiguity in Decision-Making. *Journal of Political Economy*, 72, 62–73. https://doi.org/10.1086/258854

Bednall, J. (2006). Epoche and bracketing within the phenomenological paradigm. *Issues in Educational Research*, 16(2), 123-138. Retrieved from https://iier.org.au/iier16/bednall.html

Benson, R. A. (2011). *A Phenomenological Study Exploring Change Management in Public General Aviation Airports.* [Doctoral dissertation, Walden University]. Retrieved from https://www.proquest.com/dissertations-theses/phenomenological-study-exploring-change/docview/915747529/se-2

Bessieux-Ollier, C., Nègre, E., & Verdier, M. A. (2023). Moving from accounting for people to accounting with people: A critical analysis of the literature and avenues for research. *European Accounting Review*, *32*(5), 1247-1271. https://doi.org/10.1080/09638180.2022.2052922

Blakely, B., Kurtenbach, J., & Nowak, L. (2022). Exploring the information content of cyber breach reports and the relationship to internal controls. *International Journal of Accounting Information Systems*, 46, 100568. https://doi.org/10.1016/j.accinf.2022.100568

Boland, R. J. (1984). Sense-making of accounting data as a technique of organisational diagnosis. *Management Science*, 30(7), 868-882. https://doi.org/10.1287/mnsc.30.7.868

Boland, R. J. (1993). Accounting and the interpretive act. *Accounting, Organisations and Society*, 18(2-3), 125-146. https://doi.org/10.1016/0361-3682(93)90030-A

Brecht, H. D., & Martin, M. P. (1996). Accounting Information Systems: The Challenge of Extending Their Scope to Business and Information Strategy. *Accounting Horizons*, 10(4), 16-22. Retrieved from https://www.proquest.com/scholarly-journals/accounting-information-systems-challenge/docview/208911919/se-2

Bressler, L. A., & Bressler, M. S. (2006). How entrepreneurs choose and use accounting information systems: it isn't what you think. *Strategic Finance*, 56-60. Retrieved from https://link.gale.com/apps/doc/A147302802/AONE?u=usyd&sid=googleScholar&xid=16b86810

Brinkmann, S., & Kvale, S. (2005). Confronting the ethics of qualitative research. *Journal of constructivist psychology*, *18*(2), 157-181. https://doi.org/10.1080/10720530590914789

Broadbent, J. (1992). Change in organisations: a case study of the use of accounting information in the NHS. *The British Accounting Review*, *24*(4), 343-367.https://doi.org/10.1016/S0890-8389(05)80044-7

Bulog, I. (2016). The influence of top management demographic characteristics on decision making approaches. *Ekonomski Vjesnik/Econviews-Review of Contemporary Business, Entrepreneurship and Economic Issues*, *29*(2), 393-403. Retrieved from https://hrcak.srce.hr/ojs/index.php/ekonomski-vjesnik/article/view/4142

Buriro, A., Ednut, N., & Khatoon, Z. (2021). Philosophical underpinning and phenomenology approach in social science research. *Asia-Pacific-Annual Research Journal of Far East & Southeast Asia*, *38*, 237-254. https://doi.org/10.47781/asia-pacific.vol38.Iss0.2526

Busco, C., Riccaboni, A., & Scapens, R. W. (2006). Trust for accounting and accounting for trust. *Management Accounting Research*, *17*(1), 11-41. https://doi.org/10.1016/j.mar.2005.08.001

Bushman, R. M., & Smith, A. J. (2001). Financial accounting information and corporate governance. *Journal of accounting and Economics*, *32*(1-3), 237-333. https://doi.org/10.2139/ssrn.253302

Bychkova, S. M., Karelskaia, S. N., Abdalova, E. B., & Zhidkova, E. A. (2021). Social responsibility as the dominant driver of the evolution of reporting from financial to non-financial: theory and methodology. *Foods and Raw Materials*, 9(1), 135-145. http://doi.org/10.21603/2308-4057-2021-1-135-145

Camerer, C., & Weber, M. (1992). Recent developments in modeling preferences: Uncertainty and ambiguity. *Journal of risk and uncertainty*, *5*, 325-370. https://doi.org/10.1007/BF00122575

Carr, M., & Beck, M. (2022). Accounting practices and hospital professional power dynamics during a crisis. *The British Accounting Review*, *54*(3), 101085. https://doi.org/10.1016/j.bar.2022.101085

Chen, H. S., & Jai, T. M. (2021). Trust fall: data breach perceptions from loyalty and non-loyalty customers. *The Service Industries Journal*, *41*(13-14), 947-963. https://doi.org/10.1080/02642069.2019.1603296

Chen, J., Henry, E., & Jiang, X. (2023). Is cybersecurity risk factor disclosure informative? Evidence from disclosures following a data breach. *Journal of Business Ethics*, 187(1), 199-224. https://doi.org/10.1007/s10551-022-05107-z

Chen, S., Miao, B., & Shevlin, T. (2015). A New Measure of Disclosure Quality: The Level of Disaggregation of Accounting Data in Annual Reports. *Journal of Accounting Research*, 53(5), 1017-1054. https://doi.org/10.1111/1475-679X.12094

Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 4(5), e1211. https://doi.org/10.1002/widm.1211

Choe, J. M. (1998). The effects of user participation on the design of accounting information systems. *Information & management*, 34(3), 185-198.https://doi.org/10.1016/S0378-7206(98)00055-X

Choo, C. W., & Bontis, N. (Eds.). (2002). The strategic management of intellectual capital and organisational knowledge. New York: Oxford University Press. https://doi.org/10.1093/oso/9780195138665.002.0004

Christ, K. L., Burritt, R. L., & Islam, M. A. (2023). Modern slavery and the accounting profession. *The British Accounting Review*, 55(3), 101174. https://doi.org/10.1016/j.bar.2023.101174

Christensen, J. (2010). Conceptual frameworks of accounting from an information perspective. *Accounting and Business Research*, *40*(3), 287-299. https://doi.org/10.1080/00014788.2010.9663403

Chua, W. F. (1986). Radical developments in accounting thought. *Accounting review*, 60(4), 601-632. Retrieved from https://www.jstor.org/stable/247360

Chychyla, R., Leone, A. J., & Minutti-Meza, M. (2019). Complexity of financial reporting standards and accounting expertise. *Journal of Accounting and Economics*, *67*(1), 226-253. https://doi.org/10.1016/j.jacceco.2018.09.005

Collier, P. M. (2015). Accounting for managers: Interpreting accounting information for decision making. John Wiley & Sons. Retrieved from https://sydney.primo.exlibrisgroup.com/permalink/61USYD_INST/12rahnq/alma991031517047305106

Collins, H., & Evans, R. (2019). *Rethinking Expertise*. University of Chicago Press. https://doi.org/10.7208/chicago/9780226113623.001.0001

Cordazzo, M., Bini, L., & Marzo, G. (2020). Does the EU Directive on non-financial information influence the value relevance of ESG disclosure? *Italian evidence. Business Strategy and the Environment*, 29(8), 3470-3483. https://doi.org/10.1002/bse.2589

Core, J. E. (2001). A review of the empirical disclosure literature: discussion. *Journal of accounting and economics*, *31*(1-3), 441-456. https://doi.org/10.1016/S0165-4101(01)00036-2

Coupé, C., & Ollagnier-Beldame, M. (2019). Epoché, verbal descriptions and corpus size in the conduct and analysis of explicitation interviews. *Constructivist foundations*, 14(2), 158-160. Retrieved from https://constructivist.info/14/2/158

Covaleski, M. A., & Dirsmith, M. W. (1990). Dialectic tension, double reflexivity and the everyday accounting researcher: on using qualitative methods. *Accounting, Organisations and Society*, 15(6),

543-573. https://doi.org/10.1016/0361-3682(90)90034-R

Craig, R., & Diga, J. (1998). Corporate accounting disclosure in ASEAN. *Journal of International Financial Management & Accounting*, 9(3), 246-274. https://doi.org/10.1111/1467-646X.00039

Crotty, M. J. (1998). *The foundations of social research: Meaning and perspective in the research process.* Routledge, 1-256. https://doi.org/10.4324/9781003115700

Curley, S., & Yates, F. (1989). An empirical evaluation of descriptive models of ambiguity reactions in choice situations. *Journal of Mathematical Psychology*, 33, 397–427. https://doi.org/10.1016/0022-2496(89)90019-9

Dale, E., & Chall, J. S. (1949). *The concept of readability*. Elementary English, 26(1), 19-26. Retrieved from https://www.jstor.org/stable/41383594

Daly, A. (2018). The introduction of data breach notification legislation in Australia: A comparative view. *Computer Law & Security Review*, *34*(3), 477-495. https://doi.org/10.1016/j.clsr.2018.01.005

Danos, P., Holt, D. L., & Imhoff, E. A. (1989). The use of accounting information in bank lending decisions. *Accounting, Organisations and Society*, *14*(3), 235-246. https://doi.org/10.1016/0361-3682(89)90025-1

Davison, J. (2011). Barthesian perspectives on accounting communication and visual images of professional accountancy. *Accounting, Auditing & Accountability Journal*, *24*(2), 250-283. https://doi.org/10.1108/09513571111100708

De Loo, I., & Lowe, A. (2017). "[T] here are known knowns… things we know that we know" Some reflections on the nature and practice of interpretive accounting research. *Accounting, Auditing & Accountability Journal*, 30(8), 1796-1819. https://doi.org/10.1108/aaaj-08-2015-2164

Detmer, D. (2013). Phenomenology Explained: From Experience to Insight. *Teaching Philosophy*, 37(2), 291-293. https://doi.org/10.5840/teachphil201437224

De Villiers, C., Dumay, J., & Maroun, W. (2019). Qualitative accounting research: dispelling myths and developing a new research agenda. *Accounting & Finance*, 59(3), 1459-1487. https://doi.org/10.1111/acfi.12487

Dewi, N. P. D. S., Suputra, I. D. G. D., Sudana, I. P., & Gayatri, G. (2022). Household accounting during the COVID-19 pandemic in phenomenology perspective. *Linguistics and Culture Review*, 6(S1), 449-479. https://doi.org/10.21744/lingcure.v6nS1.2078

Dhaliwal, D. A. N., Naiker, V. I. C., & Navissi, F. (2010). The association between accruals quality and the characteristics of accounting experts and mix of expertise on audit committees. *Contemporary accounting research*, 27(3), 787-827. http://dx.doi.org/10.2139/ssrn.1548766

Dianati Deilami, Z., & Qanit, S. Q. (2022). Phenomenology of the accounting situation in Afghanistan. *International Journal of Finance & Managerial Accounting*, *7*(24), 59-76. Retrieved from http://www.ijfma.ir/article_18063.html

Downie, N. J. (2010). The use of accounting information in hotel marketing decisions. *International Journal of Hospitality Management*, 16(3), 305-312. https://doi.org/10.1016/S0278-4319(97)00022-4

Du, N., & Budescu, D. V. (2005). The effects of imprecise probabilities and outcomes in evaluating investment options. *Management Science*, *51*(12), 1791-1803. https://doi.org/10.1287/mnsc.1050.0428

Duff, A., & Ferguson, J. (2011). Disability and the socialization of accounting professionals. *Critical Perspectives on Accounting*, *22*(4), 351-364. https://doi.org/10.1016/j.cpa.2010.12.009

Dunk, A. S. (2005). "Financial and Non-Financial Performance: The Influence of Quality of Information System Information, Corporate Environmental Integration, Product Innovation, and Product Quality", Epstein, M.J. and Lee, J.Y. (Ed.) *Advances in Management Accounting (Advances in*

Management Accounting, Vol. 14), Emerald Group Publishing Limited, Leeds, pp. 91-114. https://doi.org/10.1016/S1474-7871(05)14004-0

Dye, R. A. (2001). An evaluation of "essays on disclosure" and the disclosure literature in accounting. *Journal of* accounting and economics, 32(1-3), 181-235. https://doi.org/10.1016/S0165-4101(01)00024-6

Edmans, A., & Gabaix, X. (2016). Executive compensation: A modern primer. *Journal of Economic literature*, *54*(4), 1232-1287. https://doi.org/10.3386/w21131

Eierle, B., & Schultze, W. (2013). The role of management as a user of accounting information: implications for standard setting. *Journal of Accounting and Management Information Systems*, Forthcoming. http://dx.doi.org/10.2139/ssrn.1130162

Elharidy, A. M., Nicholson, B., & Scapens, R. W. (2008). Using grounded theory in interpretive management accounting research. *Qualitative research in accounting & management*, 5(2), 139-155. https://doi.org/10.1108/11766090810888935

Ellsberg, D. (1961). *Risk, ambiguity, and the savage axioms*. Cambridge University Press. https://doi.org/10.1017/CBO9780511609220.017

Ezzy, D. (2013). *Qualitative analysis*. Routledge. https://doi.org/10.4324/9781315015484

Foerderer, J., & Schuetz, S. W. (2022). Data breach announcements and stock market reactions: a matter of timing?. *Management Science*, 68(10), 7298-7322. https://doi.org/10.1287/mnsc.2021.4264

Fox, C. R., & Tversky, A. (1995). Ambiguity aversion and comparative ignorance. *Quarterly Journal of Economics*, 110(3), 585-603. https://doi.org/10.2307/2946693

Fox, C. R., & Weber, M. (2002). Ambiguity aversion, comparative ignorance, and decision context. *Organizational Behavior and Human Decision Processes*, 88(1), 476–498. https://doi.org/10.1006/obhd.2001.2990

Gadamer, H. G. (1979). The problem of historical consciousness. *Interpretive social science: A reader*, 103-160. https://doi.org/10.1525/9780520340343-005

Gamayuni, R. R., & Dewi, F. G. (2018). Usefulness analysis of accrual-based accounting information on local government financial statement: A qualitative study. *International Journal of Scientific & Technology Research*, 7(11), 10-21. Retrieved from https://www.ijstr.org/research-paper-publishing.php?month=nov2018

Garcia-Sanchez, I. M., Martínez-Ferrero, J., & García-Meca, E. (2017). Gender diversity, financial expertise and its effects on accounting quality. *Management Decision*, *55*(2), 347-382. https://doi.org/10.1108/MD-02-2016-0090

Geanellos, R. (2000). Exploring Ricoeur's hermeneutic theory of interpretation as a method of analysing research texts. *Nursing inquiry*, 7(2), 112-119. https://doi.org/10.1046/j.1440-1800.2000.00062.x

Gibson, D., & Harfield, C. (2023). Amplifying victim vulnerability: Unanticipated harm and consequence in data breach notification policy. *International Review of Victimology*, *29*(3), 341-365. https://doi.org/10.1177/02697580221107683

Gilboa, I., & Schmeidler, D. (2001). *A theory of case-based decisions*. Cambridge University Press. https://doi.org/10.1017/CBO9780511493539

Giuliani, M. (2016). Sensemaking, sensegiving and sensebreaking: The case of intellectual capital measurements. *Journal of Intellectual Capital*, 17(2), 218-237. https://doi.org/10.1108/JIC-04-2015-0039

Glaser, B. G., & Strauss, A. L. (2017). Theoretical sampling. In *Sociological methods* (pp. 105-114). Routledge. https://doi.org/10.4324/9781315129945-10

Goldstein, I., & Yang, L. (2019). Good disclosure, bad disclosure. *Journal of Financial Economics*, *131*(1), 118-138. https://doi.org/10.1016/j.jfineco.2018.08.004

Gosselin, A. M., Le Maux, J., & Smaili, N. (2021). Readability of accounting disclosures: a comprehensive review and research agenda. *Accounting Perspectives*, *20*(4), 543-581. https://doi.org/10.1111/1911-3838.12275

Govindarajan, D. (2011). Corporate risk appetite: Ensuring board and senior management accountability for risk (November 17, 2011). *ICMA Centre Discussion Papers: 2011 Series*. http://dx.doi.org/10.2139/ssrn.1962126

Guo, Z., Hall, M., & Wiegmann, L. (2023). Do accounting disclosures help or hinder individual donors' trust repair after negative events?. *Accounting, Auditing & Accountability Journal*, *36*(4), 1078-1109. https://doi.org/10.1108/AAAJ-08-2021-5409

Gurd, B. (2008). Remaining consistent with method? An analysis of grounded theory research in accounting. *Qualitative Research in Accounting & Management*, 5(2), 122-138. https://doi.org/10.1108/11766090810888926

Guthrie, J. (2001). The management, measurement and the reporting of intellectual capital. *Journal of Intellectual Capital*, 12(1), 27-41. https://doi.org/10.1108/14691930110380473

Hall, M. (2010). Accounting information and managerial work. *Accounting, Organisations and Society*, 35(3), 301-315. https://doi.org/10.1016/j.aos.2009.09.003

Haller, A., Link, M., & Groß, T. (2017). The term 'non-financial information'–a semantic analysis of a key feature of current and future corporate reporting. *Accounting in Europe*, 14(3), 407-429. https://doi.org/10.1080/17449480.2017.1374548

Hardin, R. (2006). *Trust* (Vol. 10). Polity. Retrieved from https://www.wiley.com/en-us/Trust-p-9780745624655

Heidegger, M. (1962). Being and time. *Wiley-Blackwell*. Retrieved from https://www.wiley.com/en-gb/Being+and+Time-p-9780631197706

Heimann, K., Boelsbjerg, H. B., Allen, C., van Beek, M., Suhr, C., Lübbert, A., & Petitmengin, C. (2023). The lived experience of remembering a 'good' interview: Micro-phenomenology applied to itself. *Phenomenology and the Cognitive Sciences*, 22(1), 217-245. https://doi.org/10.1007/s11097-022-09844-4

Himick, D., Brivot, M., & Henri, J. F. (2016). An ethical perspective on accounting standard setting: Professional and lay-experts' contribution to GASB's Pension Project. *Critical Perspectives on Accounting*, 36, 22-38. https://doi.org/10.1016/j.cpa.2015.12.002

Hodder, L., Koonce, L., & McAnally, M. L. (2001). SEC market risk disclosures: Implications for judgment and decision making. *Accounting Horizons*, 15(1), 49-70. https://doi.org/10.2308/acch.2001.15.1.49

Holmes, S., & Nicholls, D. (1988). An analysis of the use of accounting information by Australian small business. *Journal of small business management*, 26(2), 57. Retrieved from https://sydney.primo.exlibrisgroup.com/permalink/61USYD_INST/2rsddf/cdi_proquest_journals_220983823

Holmes, S., & Nicholls, D. (1989). Modelling the accounting information requirements of small businesses. *Accounting and Business Research*, 19(74), 143-150. https://doi.org/10.1080/00014788.1989.9728844

Hopper, T., & Powell, A. (1985). Making sense of research into the organisational and social aspects of management accounting: a review of its underlying assumptions. *Journal of management Studies*, 22(5), 429-465. https://doi.org/10.1111/j.1467-6486.1985.tb00007.x

Hopwood, A. G., & Miller, P. (Eds.). (1994). *Accounting as social and institutional practice*. Cambridge University Press. Retrieved from https://catalogue.nla.gov.au/catalog/670861

Hoque, Z., Parker, L. D., Covaleski, M. A., & Haynes, K. (Eds.). (2017). *The Routledge companion to qualitative accounting research methods*. Taylor & Francis. Retrieved from https://researchportal.northumbria.ac.uk/en/publications/the-routledge-companion-to-qualitative-accounting-research-method

Huang, H. H., & Wang, C. (2021). Do banks price firms' data breaches?. *The Accounting Review*, *96*(3), 261-286. https://doi.org/10.2308/TAR-2018-0643

Husserl, E. (1970). *The crisis of European sciences and transcendental phenomenology: An introduction to phenomenological philosophy*. Northwestern University Press. https://www.cambridge.org/core/books/husserls-crisis-of-the-european-sciences-and-transcendental-phenomenology/introduction/3DF23E2EC8E198E76C3D85831D8B8023

Husserl, E. (2012). *Logical Investigations Volume 1*. Routledge. https://doi.org/10.4324/9780203879054

Hyndman, N., & McConville, D. (2018). Trust and accountability in UK charities: Exploring the virtuous circle. *The British Accounting Review*, *50*(2), 227-237. https://doi.org/10.1016/j.bar.2017.09.004

Jackson, S., Vanteeva, N., & Fearon, C. (2019). An investigation of the impact of data breach severity on the readability of mandatory data breach notification letters: Evidence from US firms. *Journal of the Association for Information Science and Technology*, 70(11), 1277-1289. https://doi.org/10.1002/asi.24188

Janvrin, D. J., & Wang, T. (2022). Linking cybersecurity and accounting: An event, impact, response framework. *Accounting Horizons*, 36(4), 67-112. https://doi.org/10.2308/HORIZONS-2020-101

Jasanoff, S. (2003). (No?) Accounting for Expertise?. *Science and Public Policy*, 30(3), 157–162. https://doi.org/10.3152/147154303781780542

Juma'h, A. H., & Alnsour, Y. (2020). The effect of data breaches on company performance. *International Journal of Accounting & Information Management*, 28(2), 275-301. https://doi.org/10.1108/IJAIM-01-2019-0006

Justesen, L., & Mouritsen, J. (2011). Effects of actor-network theory in accounting research. *Accounting, Auditing & Accountability Journal*, 24(2), 161-193. https://doi.org/10.1108/09513571111100672

Kanodia, C. (2007). *Accounting disclosure and real effects*. Foundations and Trends® in Accounting, 1(3), 167-258. https://doi.org/10.2308/accr.2010.85.3.1119

Kapon, S. (2017). Unpacking sensemaking. *Science Education*, 101(1), 165-198. https://doi.org/10.1002/sce.21248

Karlsson, G. (1993). *Psychological qualitative research from a phenomenological perspective*. Almqvist & Wiksell International. Retrieved from https://psycnet.apa.org/record/1993-98834-000

Karyda, M., & Mitrou, L. (2016). Data breach notification: issues and challenges for security management. *Conference: 10th Mediterranean Conference on Information Systems (MCIS)*. Retrieved from https://www.researchgate.net/publication/309414062_DATA_BREACH_NOTIFICATION_ISSUES_AND_CHALLENGES_FOR_SECURITY_MANAGEMENT

Kerr, A., Cunningham-Burley, S., & Amos, A. (1998). The new genetics and health: mobilizing lay expertise. *Public understanding of science*, 7(1), 41-60. https://doi.org/10.1177/096366259800700

Keynes, J. M. (2013). *A treatise on probability*. Courier Corporation. Retrieved from https://www.gutenberg.org/files/32625/32625-pdf.pdf

Khan, S., & Gupta, S. (2023). Using a hermeneutic phenomenological approach to Twitter content: a social network's analysis of green accounting as a dimension of sustainability. *Qualitative Research in*

Financial Markets, *15*(4), 672-692. https://doi.org/10.1108/QRFM-02-2022-0031

Kim, P., Ferrin, D., Cooper, C., & Dirks, K. (2004). Removing the shadow of suspicion: the effects of apology versus denial for repairing competence-versus integrity-based trust violations. *Journal of applied psychology*, *89*(1), 104–118. https://doi.org/10.1037/0021-9010.89.1.104

Kleining, G. (1986). Das qualitative Experiment. *Kölner Zeitschrift für Soziologie und Sozialpsychologie*, 38, 724-750. Retrieved from https://nbn-resolving.org/urn:nbn:de:0168-ssoar-8631

Kleining, G., & Witt, H. (2001). Discovery as Basic Methodology of Qualitative and Quantitative Research. *Forum Qualitative Sozialforschung Forum: Qualitative Social Research*, 2(1). https://doi.org/10.17169/fqs-2.1.977

Knight, F. (1921). Risk, Uncertainty, and Profit. Houghton, Mifflin, New York. Retrieved from https://fraser.stlouisfed.org/files/docs/publications/books/risk/riskuncertaintyprofit.pdf

Kochetova, N., & Salterio, S. (2003). Judgment and Decision-making Accounting Research: A Quest to Improve the Production, Certification, and use of Accounting Information. In *Blackwell Handbook of Judgment and Decision Making* (pp. 547–566). Blackwell Publishing Ltd. https://doi.org/10.1002/9780470752937.ch27

Koopman, K. J. (2018). *A phenomenological investigation into the lived experience of selected Accounting teachers in the Western Cape Province* (Doctoral dissertation, Stellenbosch: Stellenbosch University). Retrieved from http://hdl.handle.net/10019.1/103513

Kramer, R. (1999). Trust and distrust in organizations: emerging perspectives, enduring questions, *Annual Review of Psychology*, 50, 569-598. https://doi.org/10.1146/annurev.psych.50.1.569

Kuipers, S., & Schonheit, M. (2022). Data breaches and effective crisis communication: A comparative analysis of corporate reputational crises. *Corporate Reputation Review*, 25(3), 176-197. https://doi.org/10.1057/s41299-021-00121-9

Kurunmaki, L., Lapsley, I., & Melia, K. (2003). Accountingization v. legitimation: a comparative study of the use of accounting information in intensive care. *Management Accounting Research*, *14*(2), 112-139. https://doi.org/10.1016/S1044-5005(03)00019-2

Kvale, S. (2003). Dialogical interview research—Emancipatory or oppressive. In *Keynote speech given at the 22nd meeting of the International Human Science Research Conference, Stockholm, Sweden*. Retrieved from https://sydney.alma.exlibrisgroup.com/discovery/openurl?institution=61USYD_INST&vid=61USYD_INST:sydney&url_ver=Z39.88-2004&rft.date=1996&rft.btitle=InterViews:%20An%20introduction%20to%20qualitative%20research%20interviewing&rft.title=InterViews:%20An%20introduction%20to%20qualitative%20research%20interviewing

Lambert, R. A., & Larcker, D. F. (1987). An analysis of the use of accounting and market measures of performance in executive compensation contracts. *Journal of Accounting research*, 85-125. https://doi.org/10.2307/2491081

Latitude Financial. (2023). Latitude cyber response. Latitude Cyber Incident | Information and support. https://www.latitudefinancial.com.au/latitude-cyber-incident/

Le, P. D., Teo, H. X., Pang, A., Li, Y., & Goh, C.-Q. (2019). When is silence golden? The use of strategic silence in crisis communication. *Corporate Communications*, 24(1), 162–178. https://doi.org/10.1108/CCIJ-10-2018-0108

Lee, T. A., & Tweedie, D. P. (1975). Accounting information: an investigation of private shareholder understanding. *Accounting and Business Research*, 6(21), 3-17. https://doi.org/10.1080/00014788.1975.9728662

Lehman, C. R. (2019). Reflecting on now more than ever: Feminism in accounting. *Critical Perspectives on Accounting*, 65, 102080. https://doi.org/10.1016/j.cpa.2019.04.001

LeRoy, S. F., & Singell, L. D. (1987). Knight on Risk and Uncertainty. *The Journal of Political Economy*, 95(2), 394–406. https://doi.org/10.1086/261461

Lev, B., & Ohlson, J. A. (1982). Market-Based Empirical Research in Accounting: A Review, Interpretation, and Extension. *Journal of Accounting Research*, 20, 249–322. https://doi.org/10.2307/2674685

Lin, I. (2010). *Users' and prepares' perception of sustainability reporting and corporate sustainability* (Doctoral dissertation). Nova Southeastern University. Retrieved from https://nsuworks.nova.edu/hsbe_etd/62/

Lincoln, Y. S. (2001). Varieties of validity: Quality in qualitative research. In *Higher Education: Handbook of Theory and Research,* 16. Retrieved from https://sydney.alma.exlibrisgroup.com/discovery/openurl?institution=61USYD_INST&vid=61USYD_INST:sydney&volume=16&date=2001&aulast=Lincoln&spage=25&auinit=YS&title=Higher%20Education:%20Handbook%20of%20Theory%20and%20Research%20%2F&atitle=Varieties%20of%20validity:%20Quality%20in%20qualitative%20research&sid=google

Lind, R. (1993). The case for micro-phenomenology. *The Journal of Aesthetics and Art Criticism*, 51(4), 622-625. https://doi.org/10.1111/1540_6245.jaac51.4.0622

Lucas, U. (2000). Worlds Apart: Students' Experiences of Learning Introductory Accounting. *Critical Perspectives on Accounting*, 11(4), 479–504. https://doi.org/10.1006/cpac.1999.0390

Lukka, K., & Modell, S. (2017). Interpretive research in accounting: Past, present and future. In *The Routledge Companion to Qualitative Accounting Research Methods* (1st ed., pp. 36–54). Routledge. https://doi.org/10.4324/9781315674797-3

Lukka, K., & Vinnari, E. (2014). Domain theory and method theory in management accounting research. *Accounting, Auditing & Accountability Journal*, 27(8), 1308-1338. https://doi.org/10.1108/AAAJ-03-2013-1265

MacCrimmon, K. (1968). Descriptive and normative implications of the decision-theory postulates. In *Risk and Uncertainty* (pp. 3–32). Palgrave Macmillan UK. https://doi.org/10.1007/978-1-349-15248-3_1

Machina, M. J., & Siniscalchi, M. (2014). Ambiguity and ambiguity aversion. In *Handbook of the Economics of Risk and Uncertainty* (Vol. 1, pp. 729-807). Elsevier Science & Technology. https://doi.org/10.1016/B978-0-444-53685-3.00013-1

Macintosh, N. B., & Scapens, R. W. (1990). Structuration theory in management accounting. *Accounting, Organisations and Society*, 15(5), 455-477. https://doi.org/10.1016/0361-3682(90)90028-S

Mackenzie, N., & Knipe, S. (2006). Research dilemmas: Paradigms, methods and methodology. *Issues in Educational Research*, 16(2), 193-205. https://sydney.primo.exlibrisgroup.com/permalink/61USYD_INST/2rsddf/cdi_proquest_journals_2393182114

Marston, C. L., & Shrives, P. J. (1991). The use of disclosure indices in accounting research: a review article. *The British Accounting Review*, 23(3), 195-210. https://doi.org/10.1016/0890-8389(91)90080-L

Maulana, B. H., Rohman, A., & Prabowo, T. (2022). Doing qualitative research of phenomenology in accounting, *Academy of Accounting and Financial Studies Journal*, 25(7), 1-07. Retrieved from https://www.abacademies.org/articles/doing-qualitative-research-of-phenomenology-in-accounting-13120.html

Mayer, P., Zou, Y., Schaub, F., & Aviv, A. J. (2021). "Now I'm a bit angry:" Individuals' Awareness, Perception, and Responses to data breaches that affected them. In *30th USENIX Security Symposium* (USENIX Security 21) (pp. 393-410). https://www.usenix.org/system/files/sec21-mayer.pdf

Merkl-Davies, D. M., & Brennan, N. M. (2017). A theoretical framework of external accounting communication: Research perspectives, traditions, and theories. *Accounting, Auditing & Accountability Journal*, *30*(2), 433-469. https://doi.org/10.1108/AAAJ-04-2015-2039

Mitchell, F. (2002). Research and practice in management accounting: improving integration and communication. *European Accounting Review*, *11*(2), 277-289. https://doi.org/10.1080/09638180020017087

Mock, T. J. (1971). Concepts of information value and accounting. *The Accounting Review*, 46(4), 765-778. Retrieved from https://sydney.primo.exlibrisgroup.com/permalink/61USYD_INST/2rsddf/cdi_econis_primary_47663654X

Muda, I., & Ade Afrina, E. (2019). Influence of human resources to the effect of system quality and information quality on the user satisfaction of accrual-based accounting system. *Contaduría y administración*, *64*(2). http://dx.doi.org/10.22201/fca.24488410e.2019.1667

Murthy, S., Bhat, K. S., Das, S., & Kumar, N. (2021). Individually vulnerable, collectively safe: The security and privacy practices of households with older adults. *Proceedings of the ACM on Human-Computer Interaction*, *5*(CSCW1), 1-24. https://doi.org/10.1145/3449212

Muzatko, S., & Bansal, G. (2024). It pays to be forthcoming: timing of data breach announcement, trust violation, and trust restoration. *Internet Research*, *34*(5), 1629-1663. https://doi.org/10.1108/INTR-12-2021-0939

Neubauer, B. E., Witkop, C. T., & Varpio, L. (2019). How phenomenology can help us learn from the experiences of others. *Perspectives on medical education*, 8(2), 90-97. https://doi.org/10.1007/s40037-019-0509-2

Nieuwesteeg, B., & Faure, M. (2018). An analysis of the effectiveness of the EU data breach notification obligation. *Computer Law & Security Review*, *34*(6), 1232-1246. https://doi.org/10.1016/j.clsr.2018.05.026

Nikolaou, I., & Evangelinos, K. (2012). Financial and non-financial environmental information: significant factors for corporate environmental performance measuring. *International Journal of Managerial and Financial Accounting*, *4*(1), 61-77. https://doi.org/10.1504/IJMFA.2012.044837

OAIC. (2017, August 7). *Donateblood.com.au data breach (Australian Red Cross Blood Service)*. OAIC. https://www.oaic.gov.au/privacy/privacy-assessments-and-decisions/privacy-decisions/investigation-reports/donateblood.com.au-data-breach-australian-red-cross-blood-service

OAIC. (2023a, October 6). *Australian community attitudes to privacy survey 2023*. OAIC. https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey-2023#section-main-findings

OAIC. (2023b, October 30). Statement on Latitude Financial Data Breach. https://www.oaic.gov.au/newsroom/statement-on-latitude-financial-data-breach

OAIC. (2024, October 1). *Notifiable data breaches report & Colon; January to June 2024*. OAIC. https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-january-to-june-2024

O'Regan, P. (2015). Financial information analysis: the role of accounting information in modern society. *Routledge*. https://doi.org/10.4324/9781315848372

Ouda, H. A. G., & Klischewski, R. (2019). Accounting and politicians: a theory of accounting information usefulness. *Journal of Public Budgeting, Accounting & Financial Management*, 31(4), 496–517. https://doi.org/10.1108/JPBAFM-10-2018-0113

Parker, L. D., & Roffey, B. H. (1997). Methodological themes: back to the drawing board: revisiting grounded theory and the everyday accountant's and manager's reality. *Accounting, Auditing & Accountability Journal*, 10(2), 212-247. Retrieved from https://sydney.primo.exlibrisgroup.com/permalink/61USYD_INST/2rsddf/cdi_proquest_journals_211251653

Petitmengin, C. (2006). Describing one's subjective experience in the second person: An interview method for the science of consciousness. *Phenomenology and the Cognitive sciences*, 5(3-4), 229-269. https://doi.org/10.1007/s11097-006-9022-2

Petitmengin, C. (2021). On the veiling and unveiling of experience: A comparison between the micro-phenomenological method and the practice of meditation. *Journal of phenomenological psychology*, 52(1), 36-77. https://doi.org/10.1163/15691624-12341383

Petitmengin, C., Remillieux, A., & Valenzuela-Moguillansky, C. (2019a). Discovering the structures of lived experience: Towards a micro-phenomenological analysis method. *Phenomenology and the Cognitive Sciences*, 18(4), 691-730. https://doi.org/10.1007/s11097-018-9597-4

Petitmengin, C., Van Beek, M., Bitbol, M., Nissou, J. M., & Roepstorff, A. (2019b). Studying the experience of meditation through micro-phenomenology. *Current opinion in psychology*, 28, 54-59. https://doi.org/10.1016/j.copsyc.2018.10.009

Potter, B. N. (2005). Accounting as a social and institutional practice: Perspectives to enrich our understanding of accounting change. *Abacus*, 41(3), 265-289. https://doi.org/10.1111/j.1467-6281.2005.00182.x

Power, M. (1997). Expertise and the construction of relevance: Accountants and environmental audit. *Accounting, organisations and society*, *22*(2), 123-146. https://doi.org/10.1016/S0361-3682(96)00037-2

Prior, L. (2003). Belief, knowledge and expertise: the emergence of the lay expert in medical sociology. *Sociology of health & illness*, 25(3), 41-57. https://doi.org/10.1111/1467-9566.00339

Privacy Act 1988 (Cth). Attorney-General's Department. (2024, September 12). https://www.ag.gov.au/rights-and-protections/privacy.

Prpa, M., Fdili-Alaoui, S., Schiphorst, T., & Pasquier, P. (2020). Articulating experience: Reflections from experts applying micro-phenomenology to design research in HCI. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1-14. https://doi.org/10.1145/3313831.3376664

Przyrembel, M., & Singer, T. (2018). Experiencing meditation–Evidence for differential effects of three contemplative mental practices in micro-phenomenological interviews. *Consciousness and cognition*, 62, 82-101. https://doi.org/10.1016/j.concog.2018.04.004

Putnam, R. D. (1994). Social capital and public affairs. *Bulletin - American Academy of Arts and Sciences*, 47(8), 5-19. https://doi.org/10.2307/3824796

Ramsey, F. (1926). Truth and probability. In: Ramsey, F. (Ed.), *Foundations of Mathematics and other Logical Essays*. https://fitelson.org/probability/ramsey.pdf

Ricoeur, P. (1976). Interpretation theory: Discourse and the surplus of meaning. TCU press. https://sydney.primo.exlibrisgroup.com/permalink/61USYD_INST/1c0ug48/alma991006214199705106

Ridwan, R., Indriasari, R., Mayapada, A. G., Djalil, N. M., Jurana, J., & Parwati, N. M. S. (2021). The Meaning of Fairness in Government Financial Statements: A Phenomenology Study. *Journal of*

Accounting Research, Organisation and Economics, 4(2), 164-172. https://doi.org/10.24815/jaroe.v4i2.21025

Rittenberg, L., & Martens, F. (2012). Enterprise risk management: understanding and communicating risk appetite. *American Institute of Certified Public Accountants (AICPA) Historical Collection.* https://egrove.olemiss.edu/cgi/viewcontent.cgi?article=1753&context=aicpa_assoc

Robinson, S., & Mendelson, A. L. (2012). A qualitative experiment: Research on mediated meaning construction using a hybrid approach. *Journal of Mixed Methods Research*, *6*(4), 332-347. https://doi.org/10.1177/1558689812444789

Rosati, P., & Lynn, T. (2021). A dataset for accounting, finance and economics research on US data breaches. *Data in Brief*, 35, 106924. https://doi.org/10.1016/j.dib.2021.106924

Ruland, R. G., & Lindblom, C. K. (1992). Ethics and disclosure: An analysis of conflicting duties. *Critical Perspectives on Accounting*, *3*(3), 259-272. https://doi.org/10.1016/1045-2354(92)90004-B

Ryan, G. (2018). Introduction to positivism, interpretivism and critical theory. *Nurse researcher*, 25(4), 41-49. https://doi.org/10.7748/nr.2018.e1466

Safkaur, O., Yanti, D., Fery, I., & Azwardi, P. C. (2021). The role of accounting information system afflication in reliability financial reporting. *Ilomata International Journal of Tax and Accounting*, 2(1), 97-112. https://doi.org/10.52728/ijtc.v2i1.208

Saldaña, J. (2012). *The coding manual for qualitative researchers* (2nd ed.). Sage Publications. Retrieved from https://sydney.primo.exlibrisgroup.com/permalink/61USYD_INST/12rahnq/alma991018028389705106

Saldaña, J. (2014). *Thinking qualitatively: Methods of mind*. SAGE publications. https://doi.org/10.4135/9781071909782

Sandberg, J., & Tsoukas, H. (2015). Making sense of the sensemaking perspective: Its constituents, limitations, and opportunities for further development. *Journal of Organisational Behavior*, 36(S1), S6-S32. https://doi.org/10.1002/job.1937

Sandelowski, M. (1996). Using qualitative methods in intervention studies. *Research in Nursing & Health*, *19*(4), 359-364. https://doi.org/10.1002/(SICI)1098-240X(199608)19:4<359::AID-NUR9>3.0.CO;2-H

Santamaria, R., Paolone, F., Cucari, N., & Dezi, L. (2021). Non-financial strategy disclosure and environmental, social and governance score: Insight from a configurational approach. *Business Strategy and the Environment*, 30(4), 1993-2007. https://doi.org/10.1002/bse.2728

Schaper, S., & Pollach, I. (2021). Modern slavery statements: From regulation to substantive supply chain reporting. *Journal of Cleaner Production*, 313, 127872. https://doi.org/10.1016/j.jclepro.2021.127872

Schipper, K. (2007). Required disclosures in financial reports. *The Accounting Review*, *82*(2), 301-326. https://doi.org/10.2308/accr.2007.82.2.301

Schoeller, D. (2021). Micro-phenomenology as a practice of critical thinking. *Constructivist Foundations*, 16(2), 195-197. Retrieved from https://constructivist.info/16/2/195.schoeller

Schutz, A. (1962). Phenomenology and the Social Sciences. In *Collected papers I*: (Vol. 11, pp. 118–139). Springer Netherlands. https://doi.org/10.1007/978-94-010-2851-6_5

Schwartz, P. M., & Janger, E. J. (2006). Notification of data security breaches. *Michigan Law Review*, 105(5), 913–984. Retrieved from https://sydney.primo.exlibrisgroup.com/permalink/61USYD_INST/2rsddf/cdi_gale_infotracacademiconefile_A160714672

Seddon, P., & Yip, S. K. (1992). An empirical evaluation of user information satisfaction (UIS) measures for use with general ledger accounting software. *Journal of information systems*, 6(1), 75-92. Retrieved from https://research.ebsco.com/c/ad2qx2/search/details/2ylchpvfcz?db=bsu

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. Journal of *Management Information Systems*, 32(2), 314-341. https://doi.org/10.1080/07421222.2015.1063315

Sigalingging, E. D., Abubakar, E., Iskandar, M. U. D. A., & Nedelea, A. M. (2021). Revealing Auditor and Auditee Satisfaction In The Evolution Of Accounting Software (Phenomenology Study In The Regional Government Of South Nias District). *Ecoforum Journal*, 10(2). Retrieved from https://www.academia.edu/98972977/Revealing_Auditor_and_Auditee_Satisfaction_in_the_Evolution_of_Accounting_Software_Phenomenology_Study_in_the_Regional_Government_of_South_Nias_District_

Simon, H., & March, J. (2015). Administrative behavior and organisations. In *Organisational Behavior 2* (pp. 41-59). Routledge. Retrieved from https://www.taylorfrancis.com/chapters/edit/10.4324/9781315702001-5/administrative-behavior-organizations-herbert-simon-james-march-herbert-simon

Simpson, A. (2010). Analysts' use of non-financial information disclosures. *Contemporary Accounting Research*, 27(1), 249–288. https://doi.org/10.1111/j.1911-3846.2010.01008.x

Siriwardane, H. P., & Durden, C. H. (2016). The communication skills of accountants: What we know and the gaps in our knowledge. *Accounting Education*, 23(2), 119–134. https://doi.org/10.1080/09639284.2013.847329

Slovic, P., & Tversky, A. (1974). Who accepts savage's axiom? *Behavioral Science*, 19(6), 368–373. https://doi.org/10.1002/bs.3830190603

Smith, D. W. (2013). *Husserl* (Second edition.). Routledge. https://doi.org/10.4324/9780203742952

Smith, J. E., & Smith, N. P. (1971). Readability: A measure of the performance of the communication function of financial reporting. *The Accounting Review*, 46(3), 552–561. Retrieved from https://www.jstor.org/stable/244524

Snavely, H. J. (1967). Accounting information criteria. *The Accounting Review*, 42(2), 223-232. Retrieved from https://www.jstor.org/stable/243928

Sowa, J. F. (1984). *Conceptual structures: Information processing in mind and machine*. Addison-Wesley. Retrieved from https://sydney.primo.exlibrisgroup.com/permalink/61USYD_INST/1c0ug48/alma991011828579705106

Sparby, T., Leass, M., Weger, U. W., & Edelhäuser, F. (2023). Training naive subjects in using micro-phenomenological self-inquiry to investigate pain and suffering during headaches. *Scandinavian Journal of Psychology*, *64*(1), 60-70. https://doi.org/10.1111/sjop.12858

Steils, N. (2021). Qualitative experiments for social sciences. *New trends in qualitative research*, *6*, 24-31. https://doi.org/10.36367/ntqr.6.2021.24-31

Stenka, R., & Jaworska, S. (2019). The use of made-up users. *Accounting, Organisations and Society*, *78*, 101055. https://doi.org/10.1016/j.aos.2019.07.001

Stocken, P. C. (2013). Strategic accounting disclosure. *Foundations and Trends® in Accounting*, 7(4), 197-291. https://doi.org/10.1561/1400000027

Sundby, S. E. (1997). The Jury as Critic: An Empirical Look at How Capital Juries Perceive Expert and Lay Testimony. *Virginia Law Review*, 83(6), 1109–1188. https://doi.org/10.2307/1073729

Sword, W. (1999). Accounting for presence of self: Reflections on doing qualitative research. *Qualitative health research*, 9(2), 270-278. https://doi.org/10.1177/104973299129121839

Tarquinio, L., & Posadas, S. C. (2020). Exploring the term “non-financial information”: an academics’ view. *Meditari Accountancy Research*, 28(5), 727-749. https://doi.org/10.1108/MEDAR-11-2019-0602

Tchernykh, A., Babenko, M., Chervyakov, N., Cortés-Mendoza, J. M., Kucherov, N., Miranda-López, V., Deryabin, M., Dvoryaninova, I., & Radchenko, G. (2017, August). Towards mitigating uncertainty of data security breaches and collusion in cloud computing. In *2017 28th International Workshop on Database and Expert Systems Applications (DEXA)*, 137-141. IEEE. https://doi.org/10.1109/DEXA.2017.44

Tewes, C. (2023). Microphenomenology as experientially based access to consciousness. *Journal für Psychologie*, 31(1), 239-263. https://doi.org/10.30820/0942-2285-2023-1-239

The University of Adelaide. (2024). The 6 best cyber security certifications to advance your career | online | university of Adelaide. https://online.adelaide.edu.au/blog/best-cyber-security-certifications.

Thomas, L., Gondal, I., Oseni, T., & Firmin, S. S. (2022). A framework for data privacy and security accountability in data breach communications. *Computers & Security*, 116, 102657. https://doi.org/10.1016/j.cose.2022.102657

Thompson, J., Bissell, P., Cooper, C., Armitage, C. J., & Barber, R. (2012). Credibility and the “professionalized” lay expert: Reflections on the dilemmas and opportunities of public involvement in health research. *Health (London, England : 1997)*, 16(6), 602–618. https://doi.org/10.1177/1363459312441008

Thottoli, M. M. (2020). Knowledge and use of accounting software: evidence from Oman. *Journal of Industry-University Collaboration*, 3(1), 2-14. https://doi.org/10.1108/JIUC-04-2020-0005

Tillmann, K., & Goddard, A. (2008). Strategic management accounting and sense-making in a multinational company. *Management accounting research*, 19(1), 80-102. https://doi.org/10.1016/j.mar.2007.11.002

Tomkins, C. (2001). Interdependencies, trust and information in relationships, alliances and networks. *Accounting, Organizations and Society*, 26(2), 161–191. https://doi.org/10.1016/S0361-3682(00)00018-0

Tomkins, C., & Groves, R. (1983). The everyday accountant and researching his reality. *Accounting, Organisations and Society*, 8(4), 361-374. https://doi.org/10.1016/0361-3682(83)90049-1

Tregidga, H., Milne, M., & Kearins, K. (2014). (Re) presenting ‘sustainable organisations’. *Accounting, Organisations and Society*, 39(6), 477-494. https://doi.org/10.1016/j.aos.2013.10.006

Valenzuela-Moguillansky, C., & Vásquez-Rosati, A. (2019). An analysis procedure for the micro-phenomenological interview. *Constructivist Foundations*, 14(2), 123-145. Retrieved from https://constructivist.info/14/2/123.valenzuela

van Helden, J. (2016). Literature review and challenging research agenda on politicians’ use of accounting information. *Public Money & Management*, 36(7), 531-538. https://doi.org/10.1080/09540962.2016.1237162

van Helden, J., & Reichard, C. (2019). Making sense of the users of public sector accounting information and their needs. *Journal of Public Budgeting, Accounting & Financial Management*, *31*(4), 478-495. https://doi.org/10.1108/JPBAFM-10-2018-0124

Vermersch, P. (1994). *L’entretien d’explicitation*, Paris, ESF. See Groupe de Recherche sur l’Explicitation: (GREX) http://www.grex2.com/#tabs-2

Vermersch, P. (2012). *Explicitation et phénoménologie : vers une psychophénoménologie*. Paris: Presses universitaires de France. Retrieved from https://www.expliciter.org/wp-content/uploads/2022/05/vers-une-psychophenomenologie-1-pierre-vermersch.pdf

Voinea, M. M., & Dimitriu, O. (2014). Manipulating user behaviour through accounting

information. *Procedia Economics and Finance*, 15, 886-893. https://doi.org/10.1016/S2212-5671(14)00552-8

Wagoner, B. (2015). Qualitative experiments in psychology: The case of Frederic Bartlett's methodology. *Forum: Qualitative Social Research*, 16(3). https://doi.org/10.17169/fqs-16.3.2367

Walker, D. M. (2005). Reclaiming public trust in the wake of recent corporate accountability failures. *International Journal of Disclosure and Governance*, *2*, 264-271. https://doi.org/10.1057/palgrave.jdg.2040057

Wallman, S. M. (1995). The future of accounting and disclosure in an evolving world: The need for dramatic change. *Accounting Horizons*, 9(3), 81. Retrieved from https://www.proquest.com/scholarly-journals/future-accounting-disclosure-evolving-world-need/docview/208915202/se-2

Walter, É., & Pronzato, L. (1990). Qualitative and quantitative experiment design for phenomenological models—a survey. *Automatica*, *26*(2), 195-213. https://doi.org/10.1016/0005-1098(90)90116-Y

Weber, B. J., & Tan, W. P. (2012). Ambiguity aversion in a delay analogue of the Ellsberg Paradox. *Judgment and Decision Making*, *7*(4), 383-389. https://doi.org/10.1017/S1930297500002734

Welsh, E. (2002). Dealing with data: Using NVivo in the qualitative data analysis process. *Forum: qualitative social research*, 3(2). Retrieved from https://sydney.primo.exlibrisgroup.com/permalink/61USYD_INST/2rsddf/cdi_doaj_primary_oai_doaj_org_article_b928460bb5fa4061b95c98833485ce47

Whitler, K. A., & Farris, P. W. (2017). The impact of cyber-attacks on brand image: Why proactive marketing expertise is needed for managing data breaches. *Journal of Advertising Research*, *57*(1), 3-9. https://doi.org/10.2501/jar-2017-005

Whittemore, R., Chase, S. K., & Mandle, C. L. (2001). Validity in qualitative research. *Qualitative health research*, 11(4), 522-537. https://doi.org/10.1177/104973201129119299

Wickramasinghe, D., & Alawattage, C. (2017). *Interpretivism*. In The Routledge *Companion to Critical Accounting* (pp. 17-32). Routledge. https://doi.org/10.4324/9781315775203-2

Wilson, R. M. (Ed.). (2015). *Accounting education research: prize-winning contributions*. Routledge. https://doi.org/10.4324/9781315690964

Wohl, A. R., Ludwig-Barron, N., Dierst-Davies, R., Kulkarni, S., Bendetson, J., Jordan, W., ... & Pérez, M. J. (2017). Project Engage: snowball sampling and direct recruitment to identify and link hard-to-reach HIV-infected persons who are out of care. *JAIDS Journal of Acquired Immune Deficiency Syndromes*, *75*(2), 190-197. https://doi.org/10.1097/qai.0000000000001312

Wyatt, A. (2008). What financial and non-financial information on intangibles is value-relevant? A review of the evidence. *Accounting and business Research*, 38(3), 217-256. http://dx.doi.org/10.2139/ssrn.1103443

Xiao, X., & Shailer, G. (2022). Stakeholders' perceptions of factors affecting the credibility of sustainability reports. *The British Accounting Review*, 54(1), 101002-. https://doi.org/10.1016/j.bar.2021.101002

Yang, J. H., & Liu, S. (2017). Accounting narratives and impression management on social media. *Accounting and Business Research*, 47(6), 673-694. https://doi.org/10.1080/00014788.2017.1322936

Young, J. J. (2006). Making up users. *Accounting, Organisations and Society*, *31*(6), 579-600. https://doi.org/10.1016/j.aos.2005.12.005

Zhang, P., & Soergel, D. (2014). Towards a comprehensive model of the cognitive process and mechanisms of individual sensemaking. *Journal of the Association for Information Science and Technology*, 65(9), 1733-1756. https://doi.org/10.1002/asi.23125

Zou, Y., & Schaub, F. (2019). Beyond mandatory: Making data breach disclosures useful for consumers. *IEEE Security & Privacy*, *17*(2), 67-72. https://doi.org/10.1109/msec.2019.2897834