ORGANISATIONAL LEARNING FROM CYBER SECURITY INCIDENTS

A thesis submitted to
The University of Kent
in the subject of Computer Science for the degree of PhD
by Clare Patterson 2025

Doctoral Committee:

Reader Jason R.C. Nurse
Senior Lecturer Virginia N.L. Virginia Franqueira

Clare M. Patterson
cmp54@kent.ac.uk
ORCID iD: 0000-0002-8480-406X

© Clare Patterson 2025

Classified: RMG – Internal

Declaration

This thesis is presented in accordance with the regulations for the degree of Doctor of Philosophy. It has been composed by myself and has not been submitted in any previous application for a degree. The research within this thesis was also conducted by myself. Parts of the thesis have been published or submitted as papers, and the list can be found in Publications section.

Word count: 85043

Abstract

As cyber security threats increase in frequency and sophistication, organisations must find more effective ways to learn from incidents in order to strengthen their defences and improve resilience. While industry guidance recommends post-incident reviews, recent research on this topic is limited, and much of the earlier work has focused narrowly on analysing causes rather than examining the entire learning process—from identifying which incidents to learn from to ensuring that lessons are implemented to improve security practices.

This thesis investigates how organisations currently approach learning from cyber security incidents and identifies key challenges in this process. Applying organisational learning theory and neo-institutional theory, the research highlights both internal and external pressures that shape learning practices. A pragmatic, mixed methods approach was employed to identify real-world challenges and offer practical recommendations to cyber security practitioners.

The study includes a systematic literature review following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) method, semi-structured interviews with 34 senior cyber security practitioners from large organisations operating in the UK, and thematic analysis. It synthesises current practices across disciplines and highlights common barriers, such as time pressures and cultural resistance, that impede effective learning. Practical recommendations were developed and then empirically validated through a two-round Delphi study involving over 20 expert practitioners, strengthening their credibility and applicability. This resulted in six endorsed recommendations to enhance organisational learning from incidents.

The overall findings indicate that, while all organisations studied conduct post-incident reviews, they have not consciously designed their learning practices. This supports the view from neo-institutional theory that organisational practices are often shaped by isomorphic pressures rather than deliberate efforts to ensure their effectiveness. Furthermore, despite recognising the importance of learning from incidents, organisations often focus on immediate technical issues, neglecting to explore underlying causes and systemic vulnerabilities. This aligns with organisational learning theory, where defensiveness can hinder effective learning. The empirically validated and practitioner-endorsed recommendations in this thesis provide strategies for overcoming these challenges.

This research contributes to cyber security practice by offering recommendations for organisations to improve their learning from incidents and build a more resilient cyber security posture. Theoretically, it extends the application of organisational learning and neo-institutional theories to a domain where these frameworks have been underutilised. Methodologically, it demonstrates the value of qualitative approaches—such as in-depth interviews and the Delphi method—in capturing practitioner perspectives. The thesis concludes with suggestions for future research inspired by this work.

Acknowledgements

This thesis would not have been possible without the support and encouragement of many individuals and organisations over the past three and a half years. I am deeply grateful for their kindness, guidance, and generosity throughout this journey.

First and foremost, I would like to express my sincere thanks to my supervisors, Dr Jason R. C. Nurse and Dr Virginia Franqueira. Their patience, insightful guidance, and unwavering support have been vital in shaping both this thesis and my development as a researcher. I am truly fortunate to have benefited from their expertise and encouragement.

I am also extremely grateful to my doctoral examiners, Professor Shujun Li and Professor Nathan Clarke, for their thoughtful feedback and constructive critique, which have greatly enhanced the quality of this work.

My thanks extend to the School of Computing and, in particular, the Institute for Cyber Security for Society, which welcomed me into its academic community and provided a supportive environment for my research.

This research would not have been possible without the participation of the many professionals who generously contributed to the fieldwork studies. While their anonymity prevents me from naming them individually, I want to acknowledge their valuable insights and the time they dedicated to supporting this research.

Finally, I wish to thank my husband, Michael Mee, along with my family and friends, whose constant encouragement and understanding have been a source of strength and motivation throughout this journey. I am especially grateful to Bia Bedria, Charlie Hosner, Christine Maxwell, and Anka Moraru, who generously served as sounding boards for my research ideas, offering thoughtful feedback and inspiring conversations that greatly enriched this work. A special thanks to my grandfather, Robert Gibson, whose curiosity, enthusiasm, and early encouragement sparked my interest in computers. His influence instilled in me a lifelong passion for learning and exploration in this field, shaping the path that led me to this research.

Publications

Details of this research have been disseminated through peer-reviewed academic journals detailed below:

- Patterson, C. M., Nurse, J. R.C., & Franqueira, V. N. L. (2023). Learning from cyber security incidents: A systematic review and future research agenda. *Computers & Security*, *132*, 103309. *Based on research in Chapter 2.*
- Patterson, C. M., Nurse, J. R.C., & Franqueira, V. N. L. (2024). "I don't think we're there yet": The practices and challenges of organisational learning from cyber security incidents. *Computers & Security*, *139*, 103699. *Based on research in Chapter 4.*
- A manuscript based on the research conducted in Chapter 6 is currently being prepared for submission to the *Computers & Security* journal. The paper will present the findings from the Delphi study and validate the recommendations developed to improve organisational learning from cyber security incidents.

In addition, presentations were given at two conferences:

- Patterson, C. M. (2023, Mar 8) Sometimes, the most important lessons are those we learn the hard way - How to learn the most from incidents, Industry and academic i4 Forum (paying members only access to the recording), Dubai. *Based on research in Chapter 4.*
- Patterson, C. M. (2024, Mar 24) From Aghh to Aha. Industry and academic IMPACT 2024 conference https://youtu.be/0_fK1gP8EJI?feature=shared. *Based on research in Chapters 4, 5 & 6.*

Table of Contents

GLOSSARY 10

INTRODUCTION 12

1.1 CONTEXT OF CYBER SECURITY INCIDENTS 12
1.2 CHALLENGES OF RESEARCHING CYBER SECURITY INCIDENTS 13
1.3 ORGANISATIONAL LEARNING FROM CYBER SECURITY INCIDENTS 15
1.4 WHY STUDY LEARNING FROM CYBER SECURITY INCIDENTS? 16
1.5 RESEARCH AIM AND QUESTIONS 17
1.6 SCOPE AND RESEARCH FRAMING 17
1.7 RESEARCH CONTRIBUTIONS 18
1.8 STRUCTURE OF THE THESIS 19

2 LITERATURE REVIEW 22

2.1 STANDARDS AND GUIDANCE ON LEARNING FROM INCIDENTS 22
2.2 RESEARCH INTO ORGANISATIONAL LEARNING FROM CYBER SECURITY INCIDENTS 26
2.3 RESEARCH FROM OTHER DOMAINS ON ORGANISATIONAL LEARNING FROM INCIDENTS 47
2.4 CHAPTER CONCLUSION 53

3 METHODOLOGY 55

3.1 RESEARCH PHILOSOPHY AND APPROACH 55
3.2 THEORETICAL FRAMEWORKS 56
3.3 RESEARCH DESIGN 61
3.4 RESEARCHER PERSPECTIVE 65
3.5 LIMITATIONS OF THE RESEARCH 66
3.6 ETHICAL CONSIDERATIONS 68
3.7 CHAPTER CONCLUSION 69

4 ORGANISATIONAL LEARNING FROM CYBER SECURITY INCIDENTS THROUGH AN EXPLORATORY POLL AND INTERVIEWS 70

4.1 EXPLORATORY POLL 70
4.2 PRACTITIONER INTERVIEWS 76
4.3 CHAPTER CONCLUSION 92

5 DEVELOPING PRELIMINARY RECOMMENDATIONS TO ENHANCE ORGANISATIONAL LEARNING FROM CYBER SECURITY INCIDENTS 94

5.1 APPROACH TO FORMULATING PRELIMINARY RECOMMENDATIONS 94
5.2 ANALYSIS OF THEMES, ASSOCIATED IMPLICATIONS AND PRELIMINARY RECOMMENDATIONS DEVELOPED 94
5.3 CHAPTER CONCLUSION 110

6 VALIDATION OF RECOMMENDATIONS THROUGH A DELPHI STUDY 112

6.1 DELPHI STUDY METHODS 112
6.2 DELPHI SURVEY RESULTS 119
6.3 DISCUSSION OF THE DELPHI SURVEY RESULTS 138
6.4 LIMITATIONS OF THE DELPHI STUDY 139
6.5 FINAL RECOMMENDATIONS 140
6.6 CHAPTER CONCLUSION 141

7 DISCUSSION 143

7.1 REFLECTING ON RESEARCH QUESTIONS 143
7.2 COMPARISON WITH INDUSTRY STANDARDS AND GUIDANCE 147
7.3 COMPARISON WITH EXISTING SCHOLARLY LITERATURE 147
7.4 COMPARISON OF FINDINGS WITH THEORETICAL FRAMEWORK 150
7.5 PRACTICAL IMPLICATIONS AND IMPLEMENTATIONS OF FINDINGS 151
7.6 LIMITATIONS 155
7.7 CHAPTER CONCLUSION 156

8 CONCLUSION AND FUTURE WORK 158

8.1 ADDRESSING THE RESEARCH QUESTIONS 158
8.2 CONTRIBUTIONS TO KNOWLEDGE 159
8.3 REFLECTIVE CRITIQUE OF THE RESEARCH 161
8.4 FUTURE RESEARCH DIRECTIONS 162

9 REFERENCES 164

10 APPENDICES 184

APPENDIX A – LITERATURE SEARCH QUERIES 184
APPENDIX B - EXPLORATORY POLL 185
APPENDIX C - INTERVIEW PARTICIPANTS 186
APPENDIX D - PRACTITIONER INTERVIEW PROTOCOL 188
APPENDIX E - INTERVIEW CODEBOOK AND THEMES 191
APPENDIX F - DELPHI SURVEY PARTICIPANTS 193
APPENDIX G - POTENTIAL FUTURE RESEARCH QUESTIONS 196

List of Tables

Table 1 *Screening criteria* 23
Table 2 *Incident management standards and guidance analysis* 24
Table 3 *Screening criteria* 29
Table 4 *Data items collected* 29
Table 5 *Geographical location where the analysed studies were conducted* 34
Table 6 *Research methods used by the articles analysed* 35
Table 7 *Research foundations used to frame the studies* 37
Table 8 *Coverage of the learning process by the articles analysed* 40
Table 9 *University of Kent Central Research Ethics Advisory Group (CREAG) approvals* 68
Table 10 *The organisations of interview participants by industry* 78
Table 11 *Roles of the practitioner interview participants* 78
Table 12 *Themes, associated implications and preliminary recommendations* 110
Table 13 *Delphi survey participant inclusion and exclusion criteria* 117
Table 14 *Delphi survey response rates* 119
Table 15 *Employees in the Delphi survey participants' organisations* 120
Table 16 *Industry sector of the Delphi survey participants' organisations* 120
Table 17 *Roles of the Delphi survey participants* 120
Table 18 *Delphi survey participants years of experience working in cyber security* 121
Table 19 *Delphi recommendation ranking descriptive statistical results* 125
Table 20 *Delphi recommendation ranking test statistics results* 125
Table 21 *Quantitative Delphi survey results for recommendation: Evaluate the effectiveness of the learning process* 126
Table 22 *Quantitative Delphi survey results for recommendation: Demonstrate an openness to hearing about incidents* 127
Table 23 *Quantitative Delphi survey results for recommendation: Foster trusted relationships and actively promote knowledge sharing with peers and supply chain* 129
Table 24 *Quantitative Delphi survey results for recommendation: Ensure effective participation in post-incident reviews* 131
Table 25 *Quantitative Delphi survey results for recommendation: Delve into underlying causes and trends* 133
Table 26 *Quantitative Delphi survey results for recommendation: Champion addressing structural causes* 135
Table 27 *Quantitative Delphi survey results for recommendation: Drive the implementation of lessons and testing* 137
Table 28 *Research findings mapped to research questions* 143
Table 29 *The finalised list of prioritised recommendations* 146
Table 30 *Summary of responsible parties mapped to final recommendations* 154
Table 31 *Summary of contributions* 159

List of figures

Figure 1 *Research mapped to thesis structure* 21
Figure 2 *The phases of the learning process adapted from Drupsteen, Groeneweg, et al. (2013) and Littlejohn et al. (2017)* 31
Figure 3 *PRISMA flow presenting the inclusion process* 33
Figure 4 *The publication year of the articles analysed* 34
Figure 5 *Single-loop and double-loop learning adapted from (Argyris, 1990)* 58
Figure 6 *Attributes of isomorphic pressures. Adapted from* Dimaggio & Powell (1983) 59
Figure 7 *Overview of research approach* 62
Figure 8 *Exploratory poll results to the question: What type of learning happens in your organisation following a cyber security incident?* 71
Figure 9 *Exploratory poll results to the question: When investigating the causes of incidents we consider (tick all that apply)?* 72
Figure 10 *Exploratory poll results to the question: Who in your organisation do you share lessons with (select one option)?* 73
Figure 11 *Exploratory poll results to the question: How are lessons acted upon (tick all that usually apply)?* 74
Figure 12 *Exploratory poll results to the question: Which would help your organisation to learn more from incidents (tick all that apply)?* 75
Figure 13 *The Delphi study depicting the two rounds* 113
Figure 14 *Screenshot of the ranking which participants were asked to perform (note: recommendations were presented in a random order for each participant)* 115
Figure 15 *Screenshot of Delphi survey round 2 showing some of the feedback from round 1 (note feedback continued over multiple screens)* 116
Figure 16 *Delphi study recommendation scoring results in round 1* 122
Figure 17 *Delphi study recommendation scoring results in round 2* 122
Figure 18 *Delphi study recommendations ordered according to the average ranking starting with the highest priority in round 1* 123
Figure 19 *Delphi study recommendations ordered according to the average ranking starting with the highest priority in round 2* 123

Glossary

Attack Trees: A hierarchical model used to visualise and analyse potential attack paths, showing the steps an attacker might take to compromise a system.

Causal Analysis: A systematic approach to identifying the causes of an incident to address underlying vulnerabilities or systemic issues.

Cognitive Biases: Psychological tendencies, such as hindsight bias, that can distort judgment during incident analysis and decision-making.

CREST (Council of Registered Ethical Security Testers): An international organisation that provides accreditation and certifications for cyber security professionals and services.

Delphi Study: A structured communication technique used to achieve consensus among a group of experts through multiple rounds of questionnaires and feedback.

Double-loop Learning: A concept in organisational learning where organisations not only address immediate problems but also challenge and improve underlying assumptions, processes, and systems.

Incident Response: The coordinated process of detecting, managing, and recovering from a cyber security event to minimise damage and restore normal operations.

ISACA (Information Systems Audit and Control Association): A professional association providing standards, guidance, and certification for IT governance, risk, and security.

ISO (International Organization for Standardization): An international body that develops and publishes standards, including those related to information security such as ISO/IEC 27001 and ISO/IEC 27035.

Isomorphic pressures: A concept from neo-institutional theory describing the forces that cause organisations within a field to become increasingly similar in structure or behaviour.

MITRE ATT&CK: A globally accessible knowledge base of adversary tactics and techniques based on real-world observations, used to enhance threat detection and response.

NCSC (National Cyber Security Centre): The United Kingdom's government organisation responsible for providing guidance and support to enhance cyber security resilience across the nation.

Neo-Institutional Theory: A theoretical framework used to study how external pressures, norms, and institutional influences shape organisational behaviour and practices.

NIST (National Institute of Standards and Technology): A US-based organisation that develops and provides standards, guidelines, and best practices to improve information security and risk management.

Organisational Learning Theory: A theory that examines how organisations learn and adapt by incorporating experiences, fostering knowledge sharing, and implementing changes at systemic levels.

Post-incident learning: The process of reflecting on and analysing security incidents to derive actionable lessons for improving defences and preventing similar events.

PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses): A methodological framework designed to ensure transparency, structure, and repeatability in systematic reviews and meta-analyses.

SANS (SysAdmin, Audit, Network, and Security Institute): A US-based cyber security training and research organisation known for developing widely adopted frameworks and technical guidance.

Stakeholders: Individuals or groups directly or indirectly involved in or affected by an organisation’s security practices, including employees, contractors, and regulators.

Supply Chain Attacks: Cyber attacks targeting an organisation's suppliers or third-party service providers to compromise their systems and gain access to the primary organisation.

Systemic Vulnerabilities: Weaknesses in organisational systems or processes that can be exploited to compromise security on a broad scale.

Unified Kill Chain (UKC): A cyber security framework that integrates elements of Lockheed Martin's Cyber Kill Chain and MITRE ATT&CK to provide a comprehensive model for defending against sophisticated attacks.

Introduction

This chapter provides the necessary context for the study by defining the scope of the research and introducing key concepts. It begins by discussing cyber security incidents, current trends, and the challenges inherent in researching them, laying the foundation for understanding their broader implications. The chapter then introduces the concept of learning from incidents, explaining its importance and relevance to the research. It also presents the research questions, justifies the study's scope, and concludes by outlining the structure of the thesis.

1.1 Context of cyber security incidents

In an increasingly digital world, society's dependence on Information Technology (IT) systems leaves us vulnerable to an ever-growing threat of cyber security attacks. In accordance with the National Institute of Standards and Technology (NIST) definition, a cyber security incident is "*an occurrence that jeopardises the confidentiality, integrity, or availability of an information system or the information it processes, stores, or transmits, including violations or imminent threats to security policies, procedures, or acceptable use policies* (NIST, n.d.)." A cyber security incident has the potential to disrupt critical infrastructure such as public utilities, financial systems, healthcare, research, and other critical supply chains. As these sectors rely heavily on complex IT ecosystems, the scale and complexity of cyber-attacks continue to rise globally, with new methods of attack emerging daily (CrowdStrike, 2023).

Despite global spending on security and risk management reaching an estimated USD 215 billion in 2024 (Gartner, 2023), cybercrime continues to escalate, with projected global costs expected to reach USD 12 trillion by 2025 (Knowles, 2024). In the UK, three-quarters of businesses experienced at least one incident in the past year (UK Government, 2024), and cyber risk now ranks among the top five threats to business leaders worldwide (PwC, 2023). However, alongside rising threats is a well-documented shortage of cyber security professionals (Department for Science Innovation and Technology, 2024), underscoring the urgent need for organisations to improve how they manage and learn from these events.

Cyber security incidents often represent critical junctures for organisations, revealing vulnerabilities in their systems and providing valuable opportunities for learning and enhancing resilience (Baskerville et al., 2014). By extracting and applying lessons from these incidents, organisations have the potential to strengthen their defences and better protect themselves from future threats (Van der Kleij et al., 2017). However, with the increasing volume of incidents, it remains unclear whether organisations are truly capitalising on these opportunities for learning. There is a gap in understanding whether organisations are consistently applying structured learning processes to extract value from these disruptions. This research seeks to address this gap by exploring how much organisations currently learn from cyber security incidents, the challenges they face in doing so, and by offering recommendations to enhance their learning practices.

Cyber security incidents vary widely in form, cause, and impact, but they often stem from underlying vulnerabilities within an organisation's systems. These vulnerabilities typically fall into three broad categories: design flaws in system architecture, implementation errors during deployment, and insecure configurations resulting from oversight or complexity (Howard & Longstaff, 1998). As organisations operate within increasingly interconnected digital ecosystems, often underpinned by complex and opaque supply chains, they may be unaware of critical vulnerabilities that emerge across systems they do not fully control or oversee.

The range of threat actors exploiting such vulnerabilities is equally diverse. Some attackers, including hobbyists and activists (Libicki, 2021), are motivated by recognition or ideology, while others—such as criminal groups and nation-state actors—pursue financial or strategic gain (Brantly & Smeets, 2020; Howard & Longstaff, 1998). Insider threats, whether through negligence or malice, continue to pose significant risks, particularly in environments where access controls are poorly enforced (Cappelli et al., 2012. Newer concerns have emerged around voyeuristic actors targeting Internet of Things (IoT) devices and personal data for surveillance or exploitation (DiNardi, 2023; Nurse, 2019).

Just as there are numerous ways to design an IT landscape for an organisation, there are equally many ways to attack it. Cohen (1997) lists 94 types of attacks in his classification scheme, aiming for comprehensiveness. Organisations use various models such as *attack trees* to visualise possible attack paths and understand likely compromises (Schneier, 1999). The *MITRE Adversarial Tactics, Techniques & Common Knowledge for Enterprise (ATT&CK)* model helps organisations understand attacker tactics in a non-sequential framework. Thwarting an attack requires an adaptive defence-in-depth approach (Pols, 2017). Learning from incidents can help organisations to identify the vulnerabilities which the attacker exploited and then explore what allowed these vulnerabilities to exist in the organisation. Taking lessons from analysing the cause of incidents enables organisations to adapt to evolving threats.

The rapid digitalisation of society has led to the creation of interwoven, interdependent systems that significantly amplify risks, particularly within complex supply chains (World Economic Forum, 2022). Organised crime has increasingly exploited these vulnerabilities for financial gain, while state-sponsored actors use cyber tools to gain political leverage and spread misinformation (Connolly & Wall, 2019).

Notably, ransomware and business email compromise (BEC) have emerged as some of the most prevalent and financially damaging types of attacks (Britton, 2024). Notable incidents—such as the Colonial Pipeline attack and the Kaseya supply chain breach—have demonstrated the systemic impact such attacks can have, not only on individual organisations but also across national infrastructure and global supply chains (BBC, 2021; Mandiant Services, 2021). The evolution of ransomware tactics, such as double extortion, further complicates the landscape, as attackers now threaten to publicly expose stolen data unless ransoms are paid (Mandiant Services, 2021). Business Email Compromise (BEC) schemes have also caused substantial financial losses. According to the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3), BEC attacks resulted in reported losses of nearly $3 billion in 2023, representing a 7% increase over 2022's total of $2.7 billion (FBI IC3, 2024).

As the threat landscape grows more complex, organisations must move beyond purely preventive approaches. Effective post-incident learning requires understanding not just how incidents occur, but also who is behind them, what tactics they use, and how existing vulnerabilities are exploited. This evolving context underscores the importance of continuous improvement in incident detection, response, and post-incident organisational learning to enhance long-term cyber resilience.

1.2 Challenges of researching cyber security incidents

Researching cyber security incidents poses numerous challenges due to the absence of an agreed-upon taxonomy, inconsistent reporting practices, and the subjective nature of how incidents are classified (Ibrishimova, 2018). For an incident to be included in research, it must be detected, reported, and categorised, but these steps are often influenced by organisational norms and social constructs (Salane & Jay, 2011). Incident data is typically self-reported by organisations, and there is limited if any, independent verification of the data reported. Additionally, many publicly cited statistics are provided by security vendors, who may have a vested interest in highlighting particular trends (Florêncio et al.,

2013). The data collected from these surveys is often methodologically inconsistent, leading to challenges in drawing reliable conclusions.

Detection of incidents can vary widely, and some attackers, particularly those involved in espionage, aim to avoid detection altogether. By contrast, ransomware attackers want their presence known to extract payment (Mandiant, 2022). Some incidents are never reported due to fear of disciplinary action, as found in a study by Arlington Research (2020), which reported that 62% of organisations rely on individuals to report breaches, but 46% of those who did were subsequently disciplined, creating a disincentive for transparency.

Even when incidents are detected, their categorisation can be inconsistent. For instance, Kuypers et al. (2016) found that, in the large organisation they studied, incidents taking less than 30 minutes to investigate were not even recorded by the incident response team. This inconsistency makes it challenging to measure the efficacy of interventions or detect trends across organisations. The variability in categorisation is illustrated by the 2021 Irish Health Service attack, which involved multiple stages, including phishing and ransomware, complicating its classification (PwC, 2021). Furthermore, different frameworks apply different perspectives when defining severity. For example, the UK National Cyber Security Centre (NCSC) classifies incidents based on their impact on national security rather than the specific consequences for the affected organisation[1]. This distinction means that an incident deemed critical at the organisational level may not meet the highest severity category under the NCSC's framework, highlighting the challenge of aligning incident categorisation across different contexts.

Regulatory frameworks—like the United States Securities and Exchange Commission's (SEC) cyber security disclosure rules and the General Data Protection Regulation (GDPR)—require certain incident reports, but organisations often disclose only the bare minimum required (Neto et al., 2021). The reluctance to fully report incidents stems from concerns about reputational damage and the belief that internal handling may better mitigate risks (Cobb, 2015). The commercial pressures to attract media attention further distort incident data and encourage selective reporting of sensational statistics, a practice referred to as "data dredging" (Spiegelhalter, 2019). This creates difficulties for researchers attempting to analyse trends or assess whether learning from incidents can reduce future threats.

Furthermore, the subjective nature of incident classification adds another layer of complexity. For example, incidents might involve multiple stages or be nested in a hierarchy. In cases where incident response is outsourced to third-party vendors, incident definitions may be influenced by contract terms, potentially leading to an inflation of incident counts to meet contractual obligations (Kuypers et al., 2016). Such variability across organisations makes comparisons difficult and highlights the need for standardised definitions.

Overall, the lack of reliable, standardised data makes it difficult to establish a clear baseline for measuring the effectiveness of cyber security interventions. Future research needs more robust methodologies and consistent reporting standards to address the challenges of researching incidents in a fast-evolving threat landscape (Neto et al., 2021).

[1] The NCSC cyber categorisation framework prioritises incidents based on their impact on UK national security, public safety, and critical services, rather than focusing on the specific organisational impact. For further details, see *(National Cyber Security Centre, n.d.)*.

Examples of recent cyber security publicised statistics on incidents:

- 86% of business and 91% of cyber leaders anticipate a major cyber event due to geopolitical instability (World Economic Forum, 2024)
- Over 8 billion records compromised globally in 2023 (IT Governance, 2024)
- Business email compromise (BEC) incidents surged by 67% in 2023, disproportionately impacting SMEs (Tytler & Copson, 2024)
- 30% of cyber security incidents in 2023 were attributed to hacking incidents, 16% misuse, 13% malware, 7% social, 7% error and 7% other, 20% not categorised (Statista, 2024)
- 2.2m malicious websites taken down by the UK government in the year ending August 2024 (National Cyber Security Centre, 2024)

1.3 Organisational learning from cyber security incidents

Understanding how organisations learn from incidents is increasingly critical in today's threat landscape. The academic literature on organisational learning is extensive, reflecting decades of interest in how organisations can improve their performance and adapt to changing environments. However, much of this research has focused on enhancing innovation or competitiveness, or on learning at the team or group level to support skill development and knowledge transfer. While these areas contribute to overall organisational performance, they offer limited insight into how organisations learn from disruptive events such as cyber incidents. Although organisational learning is often viewed as a foundation for resilience, recent research suggests that the relationship between the two remains under-explored, particularly in terms of the mechanisms through which learning contributes to improved resilience over time (Evenseth et al., 2022). This highlights the importance of examining how learning processes are actually enacted in the aftermath of incidents.

In contrast, this thesis explores organisational learning in the specific context of cyber incidents, examining how organisations intentionally identify, internalise, and implement lessons learned. This focus is essential because cyber incidents are not exceptional anomalies—they are now a persistent and expected feature of the digital environment. Organisations can no longer rely solely on prevention or assume they can avoid disruption altogether. Instead, they must continuously improve how they respond to and recover from incidents. Learning effectively from each incident is central to building stronger organisational resilience. Improving organisational learning from incidents is not simply about working harder or adding more processes—particularly as many organisations already face significant constraints, including acute shortages in cyber security expertise (de Zan, 2019). Better learning practices can help organisations to use their existing resources more intelligently, enhancing risk awareness, strengthening protective measures, and sharpening response capabilities (Connolly & Wall, 2019).

Organisational learning, as conceptualised in this study, refers to collective learning that leads to changes at the organisational level, rather than improvements confined to individual knowledge or performance (Crossan et al., 1999). Although industry guidance such as the NIST Special Publication 800-61 Revision 2 (National Institute of Standards and Technology [NIST], 2012) includes a post-incident review as a key component of incident response, there is limited evidence on whether such reviews result in meaningful learning across organisations. While researchers such as Murphy et al. (2021) have highlighted the potential benefits of strengthening post-incident learning practices, recent empirical work has not established whether these recommendations have been widely adopted or how they are operationalised in practice.

To address this gap, this study investigates the ways in which organisations currently approach learning from cyber security incidents, and the challenges they face in doing so. It draws on two theoretical lenses to analyse the forces that shape these practices: neo-institutional theory and organisational learning theory. Neo-institutional theory sheds light on the external expectations, norms, and institutional pressures that influence organisational behaviour (Hasan et al., 2021), while organisational learning theory offers a framework for assessing how lessons are captured, communicated, and embedded within the organisation (Rządca & Strumińska-Kutra, 2016). Together, these perspectives support a deeper understanding of the conditions under which learning from incidents can be improved and sustained across different organisational contexts.

1.4 Why study learning from cyber security incidents?

Cyber security is becoming increasingly critical to society as the frequency and severity of incidents continue to rise (World Economic Forum, 2022). With digital infrastructures supporting more aspects of everyday life, the potential impact of cyber security incidents is escalating, threatening not only individual organisations but entire sectors, economies, and even national security. Despite record levels of investment in security technologies and controls, the persistent rise in successful attacks (Gartner, 2023; Knowles, 2024) raising questions about how well they are able to learn from previous incidents and adapt to the evolving threat landscape.

Studying how organisations respond to and learn from cyber security incidents is essential because incidents provide valuable insights into potential weaknesses and vulnerabilities. Without taking the time to analyse what happened and why, the underlying conditions that enabled an incident to occur may remain unnoticed and unaddressed, leaving organisations vulnerable to similar incidents in the future. By investigating incidents, organisations can identify patterns in their defences, processes, or behaviours that contributed to the event and explore how different decisions or strategies might have altered the outcome. Learning from incidents is not simply about identifying immediate technical failures. It involves recognising deeper organisational issues, such as inconsistent policies, inadequate staffing, ineffective communication, or a lack of clarity in roles and responsibilities.

Learning from incidents is a well-established practice in industries such as aviation, healthcare, and energy, learning from incidents is a long-established practice. These sectors have developed structured approaches to post-incident reviews and have invested in building learning-oriented cultures. The aviation industry, for example, has significantly reduced accident rates through robust investigation processes, cross-organisational information sharing, and the use of lessons learned to drive improvements in regulation, design, and operations (Gattuso, 2003). These sectors have invested in systematic processes to reflect on failures and identify strategies to prevent similar issues in the future. However, in the field of cyber security, the emphasis tends to be on immediate response and recovery, rather than on deriving long-term improvements from incident analysis.

Although industry standards, such as NIST Special Publication 800-61 Revision 2 (2012) and ISO/IEC 270035-2 (2023) recommend conduct post-incident reviews, they typically do not provide detailed guidance on how to translate these into meaningful learning. As outlined in Chapter 2, much of the existing academic literature has focused on root cause analysis and the mechanics of incident response. Few studies examine the full learning cycle—from identifying which incidents are worth learning from, through investigation and reflection, to implementing changes and evaluating whether those changes have been effective (Ahmad et al., 2020; M. Evans et al., 2019). Even where lessons are identified, they may not be shared widely across the organisation or with external partners, nor acted upon in ways that lead to lasting improvements. Existing studies have predominantly focused on how organisations analyse causes, rather than examining the full learning cycle—from identifying incidents worth learning from to ensuring that lessons are implemented and lead to meaningful improvements.

Many of these studies have encouraged organisations to delve deeper into underlying issues rather than stopping at immediate causes, and they have also called for further research in this area.

This research addresses a significant gap in both practice and scholarship by examining how organisations approach learning from cyber security incidents and by identifying the factors that enable or hinder that learning. It applies organisational learning theory and neo-institutional theory to better understand the internal dynamics and external pressures that shape how organisations learn. It recognises that organisational learning is not solely a technical matter, but is influenced by structural, and institutional factors, including regulatory compliance requirements, professional norms, resourcing constraints, and leadership expectations. This study contributes to a clearer understanding of the learning practices currently in use and offers recommendations to help organisations turn incidents into a source of insight, rather than a repeated source of disruption.

This research on learning from cyber security incidents seeks to help organisations develop more effective practices for addressing not just the symptoms of an incident, but also the deeper systemic conditions that enabled the breach or failure. By understanding these root conditions, organisations can improve decision-making, enhance security governance, and adopt more resilient practices. Furthermore, placing a stronger emphasis on learning could foster greater collaboration between organisations, allowing them to share insights and best practices that benefit the broader industry and improve the collective resilience of supply chains and ecosystems. This study aims to contribute to a more proactive and reflective approach to cyber security, which could help organisations reduce the frequency of future incidents and build stronger, more adaptive defences in an increasingly complex digital landscape.

1.5 Research aim and questions

This research aims to assist organisations in mitigating the risks posed by cyber security incidents by investigating how to enhance learning from post-incident reviews. Specifically, the focus is on gaining insights into current organisational practices for learning from cyber security incidents, identifying barriers that hinder effective learning, and providing strategies to improve organisational resilience against future incidents. The research is structured around three specific research questions (RQs), as outlined below:

> **RQ1:** What organisational practices of learning from cyber security incidents have researchers found?
>
> **RQ2:** How do organisations currently learn from cyber security incidents and what challenges do they experience in the learning process?
>
> **RQ3:** What new approaches to improve learning from cyber security incidents can be recommended?

1.6 Scope and research framing

This research investigates how organisations, rather than individuals, learn from cyber security incidents. Learning from incidents occurs on three interconnected levels: the individual level, informal learning at the organisational level, and formal learning at the organisational level (Murphy et al., 2021). While individual and informal learning are important (Curado, 2006), this study focuses specifically on formal organisational learning. This focus was chosen because formal learning processes—such as structured post-incident reviews, root cause analysis, and policy revisions—are more visible, systematic, and therefore easier to examine empirically. These processes typically leave

auditable trails and are embedded in organisational routines, making them more accessible for research than informal or tacit learning. These processes are aligned with the learning levels described by ESReDA (2015): optimising existing practices (single-loop learning), adapting organisational behaviours and processes (double-loop learning), and developing the capacity to innovate (learning to learn). Future research could build on this foundation by exploring how informal and individual learning contribute to organisational resilience, and how these forms of learning interact with formal mechanisms over time.

The research focuses specifically on learning from cyber security incidents, which involve an adversary (outside or inside the organisation). Broader IT incidents, such as hardware failures or performance issues, are excluded to maintain focus. Similarly, Operational Technology (OT) systems, such as industrial control systems, and home devices are explicitly excluded due to their unique technical and engineering requirements. OT systems, for instance, often require expertise that combines engineering and technical security knowledge, making their security a distinct field of study. By narrowing the scope to IT systems within organisational environments, this research ensures a focused examination of post-incident learning, while acknowledging that OT and home device security may warrant separate investigations.

The study examines post-incident learning, which occurs after an incident has been resolved, rather than the real-time detection or response to incidents. It focuses on formal post-incident reviews—structured processes in which organisations reflect on what happened, analyse root causes, and determine how to prevent similar incidents in the future. Informal learning that may occur during an incident, as well as personal lessons learned by those directly involved, are excluded. The aim is to understand and improve the formal mechanisms that support organisational learning.

Additionally, this research does not focus on the technical aspects of digital forensics, which are vital for determining how specific attacks occur. Digital forensics, as outlined by Kävrestad et al. (2024), provides structured methodologies for identifying, preserving, and analysing digital evidence. Similarly, the National Institute of Standards and Technology (NIST) Guide to Integrating Forensic Techniques into Incident Response (SP 800-86) (NIST, 2006) highlights the role of forensic processes in incident response, offering a structured approach to handling digital evidence. While these methodologies are crucial in understanding attack vectors and attribution, and can provide data to enable learning, the post-incident reviews and investigations in this study go beyond technical forensic analysis to encompass a broader organisational perspective. This includes assessing the impact on people, business operations, and contributing factors such as resource allocation, budgets, and staffing levels, which influence system effectiveness. Similarly, national security and warfare are excluded from the scope of this research, as these areas require specialised military expertise and access. The emphasis remains on everyday cyber security incidents encountered by organisations, rather than state-level conflicts.

The study adopts a socio-technical perspective, exploring how cyber security practitioners describe their actions and practices. This approach aligns with Goldkuhl's (2012) concept of "referential pragmatism" within a social constructivist framework. By focusing on post-incident learning, the research not only aims to explore how organisations implement lessons from cyber security incidents to enhance their overall security but also seeks to provide practical recommendations to improve organisational resilience and reduce the impact of future incidents. This dual focus ensures the findings are both theoretically insightful and practically relevant.

1.7 Research contributions

This research offers contributions to both academia and practice. Academically, it provides a systematic review of existing studies on learning from cyber security incidents, while also incorporating insights

from other disciplines, such as safety science, that have more established learning frameworks. This interdisciplinary approach enriches the understanding of learning from incidents specifically within the cyber security domain and highlights areas for future research.

Empirically, the research contributes an evidence-based analysis of current learning practices, derived from a broader and more diverse sample than previous studies. With participants from multinational organisations spanning various sectors, this research presents an up-to-date and broader representation of incident learning practices, updating the narrower scope of sector-specific or case-study-based insights. This expanded scope advances the existing knowledge on organisational learning and lays the groundwork for future studies that explore the social, political, and organisational influences on learning practices.

Practically, the research develops and validates a set of recommendations designed to foster a culture of continuous improvement in cyber security. These recommendations are aimed at helping organisations respond more effectively to the rapidly evolving cyber threat landscape. By grounding the recommendations in empirical data and practitioner expertise, this research ensures that the proposed solutions are both actionable and relevant to real-world security challenges.

Methodologically, this research contributes by employing research methods such as the Delphi study that are under-utilised in cyber security studies (Fujs et al., 2019). Specifically, it demonstrates the value of using in-depth interviews and the Delphi method to capture and analyse the experiences of cyber security practitioners. By employing a pragmatic research approach using an exploratory sequential mixed methods design, this study provides transparency in its research design choices. This transparency can enable future researchers to adopt similar approaches, broadening the range of methodologies considered within the field.

Theoretically, the study extends the application of neo-institutional and organisational learning theories into the domain of cyber security. This demonstrates the relevance of these frameworks in understanding the external and internal pressures that shape how organisations learn from incidents. The findings highlight that incidents are the result of complex socio-technical interactions and organisational choices, and that causes and lessons are co-created through social processes rather than being objective facts. This underscores a key gap in existing industry guidance, reinforcing the need for a deeper exploration of how organisations can effectively learn from cyber security incidents in a more holistic and nuanced manner.

1.8 Structure of the thesis

The thesis is structured into eight chapters, each addressing specific aspects of the research on organisational learning from cyber security incidents. These are mapped to the research questions in **Figure 1**.

Chapter 1 introduces the subject of cyber security incidents and the concept of organisational learning, providing the context for the study. This chapter outlines the key research questions, and the overarching aims of the thesis and its contributions.

Chapter 2 addresses the first research (RQ1) question by analysing the guidance available from industry standards on organisational learning. It presents a systematic literature review of cyber security studies focused on learning from incidents, supplemented by research from adjacent disciplines with more established learning frameworks. The chapter also explores organisational

learning and neo-institutional theories, establishing the theoretical framework that underpins the research and informs the analysis in the later chapters.

Chapter 3 details the methodology used in this study, justifying the chosen research design and methods. It explains the rationale for the mixed methods approach adopted, which includes an exploratory poll, semi-structured interviews with practitioners, thematic analysis, and a Delphi study to validate and refine the recommendations. This chapter also reflects on the researcher's positionality as an experienced cyber security professional.

Chapter 4 answers the second research question (RQ2) by presenting the findings from the exploratory poll and the in-depth practitioner interviews. It explains the participant selection process and offers a detailed analysis of the findings, positioning them within the broader context of the literature.

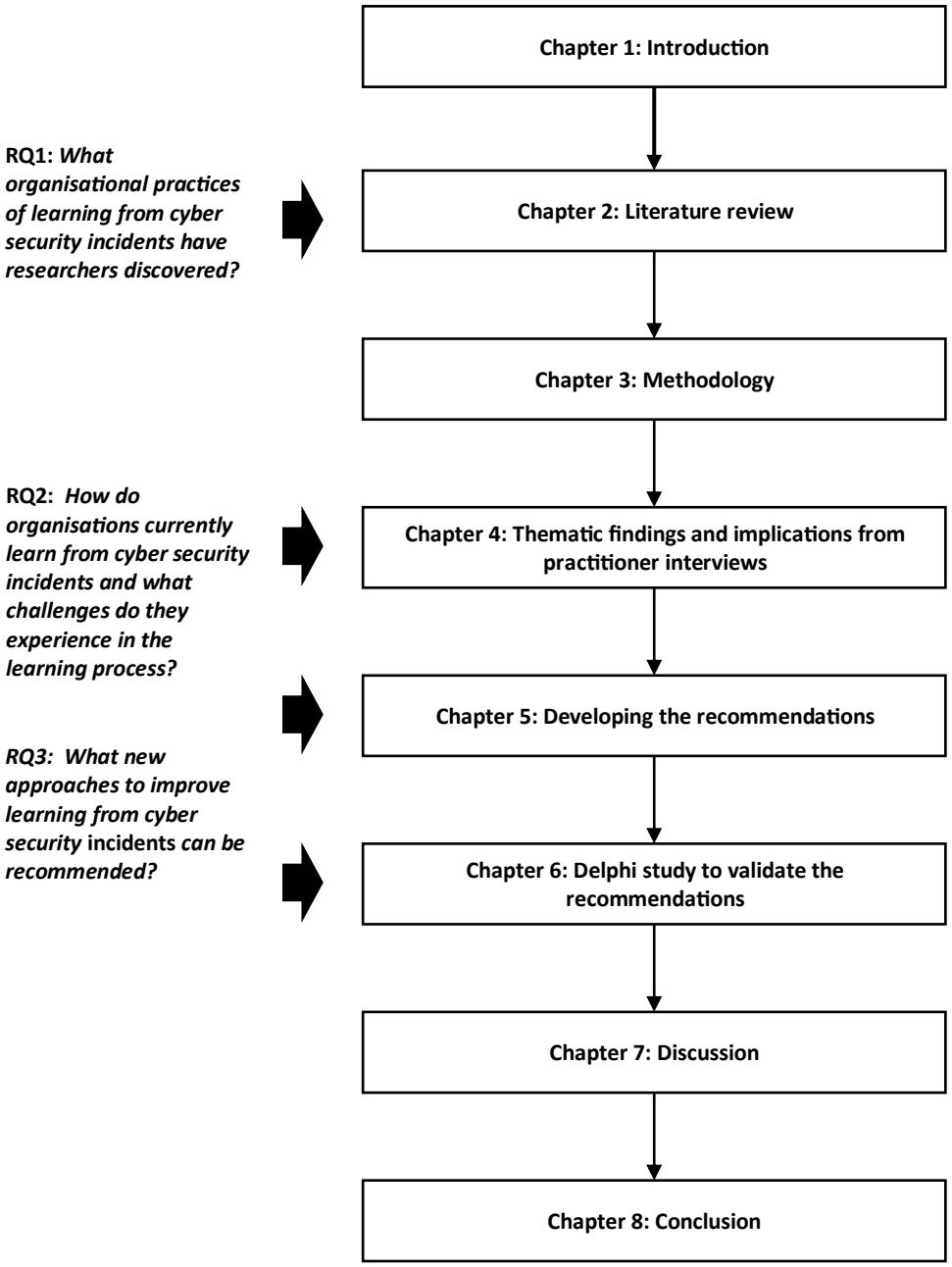
Chapter 5 begins addressing the third research question (RQ3) by analysing the themes from Chapter 4 and exploring their implications for organisations. Drawing on both cyber security and relevant interdisciplinary literature, it proposes a set of preliminary recommendations for improving organisational learning from incidents.

Chapter 6 continues to address the third research question (RQ3), describing how a two-round Delphi study was used to validate and refine the recommendations developed in Chapter 5. The chapter provides an overview of the Delphi method, including participant selection, survey design, and the approach to achieving consensus. The findings and participants' qualitative feedback are discussed, leading to the final set of validated recommendations.

Chapter 7 presents the main discussion of the research findings, critically examining them in the context of the existing literature. This chapter highlights the study's contributions to under-researched areas and reflects on the implications of the findings.

Chapter 8 concludes the thesis by summarising the main findings, addressing the research questions, and outlining the key contributions of the research. The chapter also considers the limitations of the study and suggests directions for future research. The appendices include additional materials such as details on industry standards, literature search queries, exploratory poll questions, interview participant attributes, the interview protocol, the coding framework, and the Delphi study participants and survey questions.

Figure 1 *Research mapped to thesis structure*



2 Literature review

Building upon the goals introduced in Chapter 1, this chapter establishes the theoretical basis for the thesis through a comprehensive review of relevant literature. It examines the standards and guidance on learning from incidents, assessing how these frameworks could be effectively applied by organisations to enhance their learning practices. The detailed methodology used to conduct the review is provided in Chapter 3 (Section 3.3.1).

To answer the first research question introduced in Chapter 1, this chapter reviews academic studies on organisational learning from cyber security incidents. Insights from other domains, particularly the safety discipline's approach to learning from incidents, are integrated to enrich the review. Additionally, the chapter explores organisational learning from incidents and neo-institutional theories, including previous studies in the cyber security domain. This provides the theoretical frameworks that guide the remainder of the research described in this thesis. The chapter concludes by summarising the key findings from the literature and outlining how this research addresses the identified gaps in knowledge.

2.1 Standards and guidance on learning from incidents

IT teams, facing an increasing number of cyber security incidents, often seek out formal standards and industry guidance to support effective incident response and promote learning. This section systematically reviews the most relevant documents offering guidance on organisational learning from cyber security incidents. It assesses their scope and adequacy of these documents in helping organisations improve their learning from incidents.

2.1.1 Search and selection strategy

To ensure a focused and relevant set of documents, a structured selection process was adopted. The starting point was a review of five comparative studies on cyber security standards (Andrade et al., 2019; Gikas, 2010; Giulio et al., 2017; Hamdani et al., 2021; Rahman & Choo, 2015). From this, a longlist of potentially relevant standards was identified. For this research, only standards specifically focused on security incident management were included. The decision whether or not to include was guided by the relevance to the research objectives of understanding incident learning practices across a broad range of sectors. Standards that dealt exclusively with sector-specific security requirements, such as those for healthcare, nuclear, or finance, were excluded to avoid overly niche perspectives. Similarly, national standards that were not widely adopted internationally were also excluded, with two exceptions: the UK National Cyber Security Centre (NCSC) guidance, which was included due to the UK context of this PhD research, and NIST Special Publication 800-61 Revision 2 (NIST, 2012). Despite being funded by the US government to help US companies remain innovative and competitive, the NIST cyber security framework has been widely adopted by many companies globally.

Based on the screening criteria set out in **Table 1** security incident management standards and guidance documents— called “documents” hereafter—from six organisations are reviewed in this section. Documents selected had to offer broader applicability beyond niche industries and contain detailed guidance on incident management and post-incident learning. The UK NCSC guidance, for example, refers organisations to Council of Registered Ethical Security Testers (CREST) (Creasey, 2013), NIST Special Publication 800-61 Revision 2 (NIST, 2012), and ISO/IEC 27035-2, published by the International Organization for Standardization (ISO, 2023) for further details. Similarly, Information Systems Audit and Control Association (ISACA) (2020) references the NIST and ISO guidance.

Table 1 *Screening criteria*

Inclusion criteria	1. The document must provide guidance on cyber security incident management, including post-incident activities. 2. The guidance must include reference to learning, whether framed as lessons learned, causal analysis, or organisational improvement. 3. It must have cross-sectoral relevance, avoiding niche applicability (e.g., sector-specific frameworks in healthcare or nuclear industries). 4. It must be widely recognised or adopted across multiple jurisdictions.
Exclusion criteria	1. Sector-specific standards (e.g., for finance, healthcare, or energy) with limited generalisability were excluded. 2. National standards with limited international uptake were excluded unless justified by context. Two exceptions were made: • The UK National Cyber Security Centre (NCSC) guidance, included due to the UK context of this research. • The NIST Special Publication 800-61 Revision 2, included because of its widespread international adoption despite its US origin.

2.1.2 Incident learning guidance assessment approach

To evaluate the scope of guidance provided in the documents, their coverage of the end-to-end learning process was analysed using themes based on organisational learning studies by Drupsteen et al. (2013) and Lukic et al. (2012). The theme of "participants" aligns with Lukic et al.'s (2012) concept of "participants of learning," while "improving learning" corresponds to Drupsteen et al.'s (2013) "evaluation" category. Both studies also address phases related to investigation, analysis, and the types of knowledge generated in the learning process. By integrating insights from both studies, this analysis offers a view of the learning processes presented in the documents. The documents were examined to assess the guidance on causal analysis, improving incident response, enhancing overall cyber security, and refining the learning process. Effective learning from incidents necessitates identifying underlying causes, as organisational expectations about what can be learned significantly shape the investigation process (Lundberg et al., 2010).

While all the reviewed documents suggest that incidents present opportunities for learning and improvement, they primarily concentrate on enhancing incident response capabilities. Although some documents highlight the importance of identifying underlying and systemic causes, they tend to assume that these causes are already well understood. Since these documents are primarily aimed at guiding organisations on incident response, it was crucial to evaluate not only how they addressed improvements to incident management but also whether they offered guidance on interventions to enhance the overall security posture of an organisation. This broader focus is essential because, without lessons being applied to prevent future incidents, organisations risk only improving their immediate response capabilities without addressing the underlying vulnerabilities that allowed the incidents to occur in the first place.

2.1.3 Guidance on learning in the reviewed documents

All reviewed documents acknowledged the importance of learning from incidents, typically incorporating a final "lessons learned" phase, albeit under varying terminology. However, the primary emphasis was often on improving operational response rather than deeper organisational learning. While some documents recognised the value of identifying systemic causes, this was usually implied rather than fully developed. Few offered detailed guidance on how lessons should be institutionalised or used to inform broader risk reduction strategies. Table 2 presents a summary of how each document covers the topic of learning from incidents. Guidance in these documents is intended to be generic

and high-level, so coverage is marked positively even if it is only a brief mention. All include a final step where lessons learned are identified, although this is termed differently across the documents.

Table 2 *Incident management standards and guidance analysis*

Organisations	Learning phase	Guidance
CREST Cyber Security Incident Response Guide (Creasey, 2013)	Follow up	Encourages organisations to use incidents to improve incident response and overall cyber security posture. Limited guidance on how to conduct causal analysis other than to involve relevant parties.
Information Systems Audit and Control Association (ISACA) — *Audit/Assurance Program for evaluating the management and handling of security incidents* (2020)	Lessons learned	Suggests including all stakeholders involved or affected by the incident, although focus is on improving incident response.
International Organization for Standardization ISO/IEC 27035-2:2023 — *Information security, cybersecurity and privacy protection – Information security incident management – Part 2: Guidelines to plan and prepare for incident response* (2023)	Lessons learned	Recommends including the security team and contractors and gives guidance on investigating causes to improve security control implementation, policies, risk assessments, threat intelligence, security databases and the incident management plan. It also suggests organisations look beyond single incidents for trends where preventative actions would reduce the likelihood of future incidents.
NIST Special Publication 800-61 Revision 2 Computer Security Incident Handling Guide (NIST, 2012)[2]	Post-incident activity	Guides organisations to include all involved people and others relevant for future cooperation. It suggests questions to ask to improve both incident response and wider security measures.
National Cyber Security Centre (NCSC) UK Cyber Assessment Framework (CAF) — *A guide to achieving and demonstrating the outcomes of the NCSC's cyber security principles* (2019)	Lessons learned	It does not guide organisations on who to involve but does encourage them to solve underlying causes giving the example of going beyond merely applying the missing patch but also addressing the overall patch management process.
SANS Institute Six-Step Incident Response Process — *Preparation, identification, containment, eradication, recovery, and lessons learned* (2021)	Lessons learned	Suggests conducting the review with the incident team and is focused on improving incident response, urging organisations to capture the who, what, where, why, and how of incidents.

[2] NIST released an initial public draft of *Special Publication (SP) 800-61 Revision 3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management* on April 3, 2024. Although the draft highlights the importance of continuous improvement in incident response capabilities it does not give any additional guidance on how organisations can enhance their learning from incidents capability. Public comments on the draft were accepted until May 20, 2024, and a final publication date has yet to be announced, as per the NIST Computer Security Resource Center (CSRC) website https://csrc.nist.gov/pubs/sp/800/61/r3/ipd

Forensics typically addresses the technical aspects of how incidents occur, but it often overlooks the organisational processes and behaviours that contributed to them. Only the CREST guidance (Creasey, 2013) offers substantial advice on cause analysis, while SANS (Kral, 2012) encourages organisations to avoid blame and to consider whether controls are functioning as intended. However, none of the documents address cognitive biases, such as hindsight bias[3] (Cook, 1998; Dekker, 2019), that may influence cause analysis. Additionally, there is limited guidance on adopting a continuous improvement approach to ensure lessons from incidents are effectively integrated into broader security strategies.

All six documents recognise that learning from incidents presents an opportunity to enhance broader cyber resilience. For instance, ISO/IEC 27035-2 (2023) includes recommendations for improvements to security control implementation, policies, risk assessments, threat intelligence, security databases, and the incident management plan. It also advises organisations to look beyond individual incidents for trends that could indicate the need for preventative measures. SANS (Kral, 2012) focuses primarily on improvements to the incident response process, but earlier guidance for small and medium businesses encourages exploring ways to improve the overall security of systems. The NCSC's Cyber Assessment Framework (NCSC 2019) explicitly suggests going beyond merely applying a missing patch and addressing the entire patch management process.

The quality of lessons learned from incidents depends on how well the underlying causes are identified (Boin et al., 2008). ISO/IEC 27035-2 (2023) and NIST Special Publication 800-61 Revision 2 (2012) acknowledge the need to identify systemic weaknesses but do not provide specific guidance on best practices. While Grispos (2016) acknowledges NIST Special Publication 800-61 Revision 2 (2012)'s guidance on post-implementation questions, he criticises the lack of detailed guidance on how to answer them and suggests using "light-weight retrospectives" based on the Manifesto for Agile Software Development. CREST (Creasey, 2013) provides more detailed recommendations, including techniques such as Failure Mode and Effects Analysis (FMEA), Current Reality Tree (CRT), Fault Tree Analysis, the Five-Whys Approach, Why-Because Analysis (WBA), and Cause and Effect Analysis fishbone diagrams. These methods help organisations move beyond the immediate details of individual incidents and recommend regular reviews of incident data to identify trends and assess the effectiveness of controls.

To ensure that all lessons from incidents are captured and fully understood, it is valuable to involve participants beyond the immediate incident response team (Ahmad et al., 2012). Organisations must balance practical trade-offs between comprehensive participation, logistics, and competing priorities. Guidelines that prompt careful consideration of participants can help achieve this balance. NIST Special Publication 800-61 Revision 2 (2012) highlights the need to involve teams that may need to implement the lessons in the future. It also recommends sharing post-incident lessons with users so they can understand how their actions impact the organisation's security.

ISO/IEC 27035-2 suggests considering groups outside the organisation, including contractors. ISACA (2020) recommends including all those involved in or impacted by the incident. SANS (Kral, 2012) focuses on the incident team itself, which Ahmad et al. (2012) also found in their study. Conversely, the UK National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF) (2019), and CREST (Creasey, 2013) do not provide specific guidance on who should be included in the post-incident review. Without explicit guidance, organisations may not recognise the benefits of broader participation and might only involve those directly within their team. Lukic et al. (2012) found that employees wanted greater involvement in learning from incidents. The trends highlighted in Section

[3] Hindsight bias – ""People who know the outcome of a complex prior history of tangled, indeterminate events, remember that history as being much more determinant, leading 'inevitably' to the outcome they already knew."(Weick, 1995)

1.1, such as supply chain attacks and sophisticated phishing, increase the need to expand learning beyond the incident team to identify socio-technical lessons in addition to purely technical vulnerabilities.

The guidance on who should participate in post-incident reviews could be much stronger. Often, the documents do not elaborate on which participants are essential, simply referring to 'stakeholders' or 'relevant parties'. While such documents cannot specify exact groups due to organisational differences, this is a crucial area where more detailed guidance would be valuable. The quality of underlying cause identification and the success in implementing lessons can be significantly influenced by who is included in the learning process (Ahmad et al., 2012). Limited participation may cause organisations to focus only on the immediate incident—and how to respond better to similar incidents—rather than addressing the underlying conditions that allow incidents to occur.

Overall, the reviewed guidance documents for organisational learning from cyber security incidents broadly emphasise the importance of learning from incidents, recognising the need to identify underlying and systemic causes to enhance overall cyber resilience. They also stress the value of involving a range of participants in post-incident reviews to capture diverse perspectives and improve incident management processes. However, while the standards acknowledge the necessity of systemic learning, they often fall short of offering specific, actionable guidance on how to identify and implement lessons effectively to prevent future incidents.

Most of the guidance focuses heavily on improving incident response capabilities but lacks depth in fostering continuous learning or addressing the socio-technical factors that contribute to security breaches. Although some documents recommend techniques like Failure Mode and Effects Analysis (FMEA) or the Five-Whys Approach, detailed methodologies for conducting these analyses are often absent (Creasey, 2013). Additionally, the guidance typically assumes that the causes of incidents are well-known and easily identifiable, neglecting the complex organisational behaviours and processes that enable such events (Ahmad et al., 2020). Furthermore, none of the documents offer advice on overcoming cognitive biases like hindsight bias, which can distort the process of identifying causes (Lundberg et al., 2009a, 2010a; Reed, 2020).

Although standards like CREST and SANS encourage broader reflection on the effectiveness of security controls and organisational practices, these insights are not consistently addressed across all documents. This gap reflects a larger issue: the documents tend to adopt a positivist stance, treating lessons as straightforward entities when, in fact, learning from incidents involves complex collaboration among various stakeholders (Lundberg et al., 2009a, 2010). Without clear guidance on enabling broader learning and evaluating the effectiveness of lessons learned, security teams risk being caught in a cycle of reactive responses to incidents, unable to reduce the prevalence of future events (Gonzalez, 2005). As Ahmad et al. (2020) and Reed (2020) argued, organisations need to move beyond compiling simple action lists from post-incident reviews and use these opportunities to reflect on and improve the processes and practices embedded in their complex IT systems.

2.2 Research into organisational learning from cyber security incidents

This section delves deeper into the academic studies on how organisations learn from cyber security incidents, building on the foundational concepts of organisational learning previously discussed. Although the literature on organisational learning has been comprehensively summarised in various studies (Chuah, 2020; Argote, 2013; Easterby-Smith & Lyles, 2012; Fiol & Lyles, 1985; Huber, 1991), there is still no universally accepted definition. Argote (2013) described organisational learning as a change in the organisation's knowledge as a function of experience. Fiol et al. (1985) included the translation of this new knowledge into actions taken by the organisation in their definition of organisational learning. Argote and (2017) referred to it as a process where changes are made as a

result of experiences. Murphy et al. (2021) defined three interconnected forms of learning from incidents: at the individual level and at both the formal and informal organisational learning levels. Schilling and Kluge (2009) also modelled learning at distinct levels, from the individual to the organisational level. Individual learning is part of the process but, for an organisation to learn, it must go beyond and include shared knowledge interpreted in an organisational context (Curado, 2006). The research into general organisational learning is vast, with much of it focused on using knowledge to improve productivity or competitiveness—for example, Peter Senge's popular 1990 business book *The Fifth Discipline: The Art and Practice of the Learning Organization* (1990, rev. 2010) or on enhancing skills and emergent team learning (Argote & Levine, 2017). This section aims to further explore these theories in the specific context of learning from cyber security incidents, providing a nuanced understanding of how organisations can effectively integrate and act upon the lessons learned.

This thesis examines how organisations intentionally identify and implement lessons learned from incidents. Rather than providing an extensive review of the theories of organisational learning, this literature review leverages existing models aligned with the focus of this research. Research into how organisations learn specifically from incidents has been concentrated in the safety discipline, with prominent studies into public disasters such as the Deepwater Horizon Macondo oil rig, the Challenger space shuttle, and the Fukushima nuclear power plant (Swuste et al., 2020). There is an opportunity to borrow concepts from research on learning from safety incidents to advance the field of cyber security (Line & Albrechtsen, 2016).

The objective of this research is to help organisations enhance their overall security posture by understanding and addressing the complex causes of cyber security incidents. This literature review concentrates on formal learning at the organisational level, specifically focusing on changes to systems, procedures, and technology that occur as a result of these incidents. As per the scope outlined in Chapter 1, it is limited to cyber security incidents and post-incident organisational learning.

Shedden et al. (2010) reviewed the literature available in 2010 to understand how organisational learning research could be applied to security incident response. At that time, there had been scant research into how organisations learn from cyber security incidents. More recent literature reviews have studied the complete security incident management process and, while they partially cover learning, they do not delve into the topic in depth (Grispos et al., 2014; Horne et al., 2020; Line & Albrechtsen, 2016; Tøndel et al., 2014). To address this gap, a systematic literature review was conducted, building upon previous research to provide an up-to-date overview of the literature focused specifically on learning from incidents.

2.2.1 PRISMA systematic literature review approach

PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) was selected for its well-established and rigorous approach, which ensures a structured, transparent, and repeatable method for conducting systematic reviews (Page et al., 2021). This is particularly important in cyber security research, where a comprehensive understanding of existing literature is essential due to the rapidly evolving nature of the field. By adhering to PRISMA, this study aims to provide a thorough and unbiased synthesis of the current research on organisational learning from cyber security incidents. Following this framework, the review outlines the rationale for decisions taken with regard to search strategy, sources, eligibility criteria, selection process, and analysis of the studies (Moher et al., 2009). The principles of repeatability, as described by Kitchenham et al. (2010), are followed to ensure transparency in the search approach, making it possible for other researchers to replicate or extend this review. PRISMA is a well-established technique in cyber security research (Ho et al., 2022; N. F. Khan et al., 2022; Uchendu et al., 2021), further justifying its selection for this study. The review also includes an additional literature search to supplement the PRISMA approach, ensuring a comprehensive exploration of relevant studies.

The search terms used were refined iteratively. Initially, terms naturally linked to the topic, such as “security incident” and “learning”, were employed. These search terms were then refined based on the results obtained. This refinement process was also guided by a set of gold standard papers on the topic—those precisely aligned with the research area—discovered early in the search, as well as by methodologies used in other recent systematic literature reviews in the cyber security area, such as Humayun et al. (2020).

The search terms were refined iteratively based on the returned search results and known key papers on the topic. Terms such as “learning” now return many results related to machine learning rather than organisational learning. For this reason, search terms such as “organisational learning” and “lessons learned” were used. In an attempt to balance being too narrow and missing publications, or being too broad and generating unwieldy results, the final search string combined several critical search terms: “security incident” / “CSIRT”, “organisational” / “organizational learning”, “lessons learned” / “lessons learnt”. Where appropriate and supported by the search database, wildcards were used (e.g., learn*). These terms were used to search each of the databases, and the exact search strings, adjusted according to the database search rules, are shown in Appendix A – Literature search queries. There are no perfect search terms, and research in IT is particularly challenging as the terms are constantly evolving and databases treat search terms differently (Beiderbeck et al., 2021).

The initial search was augmented through an iterative process of interpretation and understanding (Boell et al., 2014). This included searching journal databases, examining key journals’ tables of contents, and reviewing relevant conference proceedings, as well as reviewing the citations of articles on the topic and using Connected Papers and Web of Science to identify articles citing those already found. Key authors’ Google Scholar pages were also reviewed to identify any missed papers. The search results were compared against the bibliographies of Shedden et al. (2010) and Tøndel et al. (2014) to ensure all key studies had been identified. This approach balanced the risk of being too narrow and missing relevant publications against being too broad and generating unwieldy results. Full-text searches were conducted without date restrictions or other filters. An initial literature review was carried out in September 2022 in preparation for the main fieldwork. This search was repeated in full in December 2024, and the findings from the December 2024 search form the basis of this literature review chapter.

2.2.1.1 Eligibility criteria

The returned papers were reviewed using the screening criteria set out in in
Table 3.

Table 3 and were included if the research covered learning from incidents even if this was not their main focus.

2.2.1.2 Information sources

The following online sources were selected to conduct the search: ACM (Association for Computing Mchinery) Guide to Computing Literature; IEEE Xplore; ScienceDirect; Wiley Online Library; SpringerLink; ProQuest One Literature and Publicly Available Content Database (excluding Global Theses and Dissertations); Scopus; and the Web of Science Core Collection (links in Appendix A). Google Scholar was not included due to the limitations of its search functionality (Gusenbauer & Haddaway, 2020). These sources included both journals and conferences aimed specifically at cyber security, as well as other disciplines which may have covered organisational learning in a cyber security context. This increased the chances of finding relevant peer-reviewed studies which met the inclusion criteria 1 and 2, in

Table 3.

Table 3 *Screening criteria*

Inclusion criteria	1. Papers which report on cyber security research on post-incident organisational learning. 2. Studies published in peer-reviewed journals or conference proceedings.
Exclusion criteria	1. Duplicates and repeated studies. 2. Grey literature (e.g., books, theses/dissertations) and non-peer-reviewed sources. 3. Studies written in a language other than English or for which the full text was not available. 4. Studies not relevant to the research questions, including those which focus on: • user behaviour monitoring to predict incidents or fraud • learning to detect, diagnose, or respond to incidents during the incident rather than post-incident learning • the authors' view of the lessons learned from a public incident instead of how the organisation which experienced the incident learnt • training or other simulations, e.g., games, tabletop exercises, and user awareness training

2.2.1.3 Article selection

The results of the database searches were screened according to exclusion criteria 1-4, in **Table 3**. First, 479 duplicate studies were discarded. Another 10 papers not written in English or those where the full text was not accessible, and 861 non-academic and non-peer reviewed articles were removed. Titles, abstracts, and keywords were reviewed for the remaining 2,606 articles to assess their relevance in answering our research questions. This resulted in 2,495 studies being excluded and another 103 excluded after a full-text review, leaving 18 papers selected through the initial search.

Due to the evolving nature of IT terminology and the inconsistencies in how publication databases process search queries (Zhang et al., 2011), identifying all relevant literature through keyword searches alone can be challenging. To mitigate this, supplementary methods were employed to capture additional relevant studies. These additional articles were then reviewed against the eligibility criteria outlined in **Table 3** resulting in 13 more papers being included. Figure 3 presents a PRISMA flow diagram illustrating the selection process that led to the final set of 31 articles.

2.2.1.4 Data collection

As directed by PRISMA, the data items collected against each criterion are set out in Table 4. To present an overview of the types of research conducted and published in this area, the selected articles were analysed by original publication details and by the research methods used. To understand how researchers have assessed the learning practices for cyber security incidents, the foundation they used to frame their studies was reviewed.

Table 4 *Data items collected*

Data item	Description
Publication details	Where the article was published and the year of publication.
Research details	Countries and the industries in which the research was conducted, if stated. The type of research method (e.g., case study, interviews, theory-based research).

Data item	Description
Research foundation	The models and standards used to frame the research, such as ISO/IEC 27035-2 (2023) and NIST Special Publication 800-61 Revision 2 (2012), or models borrowed from management science (such as double-loop learning (Argyris, 1976) or from safety science such as Goal Structured Notation (The Assurance Case Working Group, 2021).
Learning practices	Which parts of the learning process are covered by the study, either completely or partially; what practices were found and what improvements were recommended.

To collect data on which cyber security incident learning practices the studies covered, we examined how other researchers described the practices of learning from incidents. We found that the most relevant studies for learning from cyber security incidents were those focused on learning from safety incidents (Drupsteen, Groeneweg, et al., 2013; ESReDA, 2015; Littlejohn et al., 2017; Vastveit et al., 2015). Drupsteen et al. (2013) described a four-step process:

1. Investigating and analysing incidents, which includes incident reporting and incident analysis.
2. Planning interventions.
3. Intervening.
4. Evaluating—a phase which informs the first three.

Littlejohn et al. (2017) describe a similar process but with seven parts:

1. Reporting.
2. Investigating, which includes safety concerns raised by employees.
3. Developing incident alerts, which includes input from incidents at other companies and sites and has a two-way feedback loop with Contextualising.
4. Disseminating.
5. Contextualising, which has a two-way feedback loop with Developing incident alerts.
6. Implementing actions.
7. Change in behaviour or processes, which includes sharing the outcomes with other companies and employees.

These practices are applicable to learning from cyber security incidents due to the recognised similarities between safety and security (Cockram & Lautieri, 2007; Kaur et al., 2021; Kriaa et al., 2015; Lisova et al., 2019).

Various models have been used within safety research, aligned to the different angles from which the topic has been studied (Le Coze, 2013). Murphy et al. (2021) analysed learning from safety incidents using the 3-P model of workplace learning, which comprises three phases: presage, process, and product. Their study was focused on the perspective of the frontline worker. In contrast, Le Coze (2013), in his overview of research into learning from safety incidents, used a broad framework covering industry, national contexts, actors, event intensity, disciplines, and steps. The steps element, which includes the learning activities of reporting, selection, investigation, dissemination, and prevention, is the most relevant to this study.

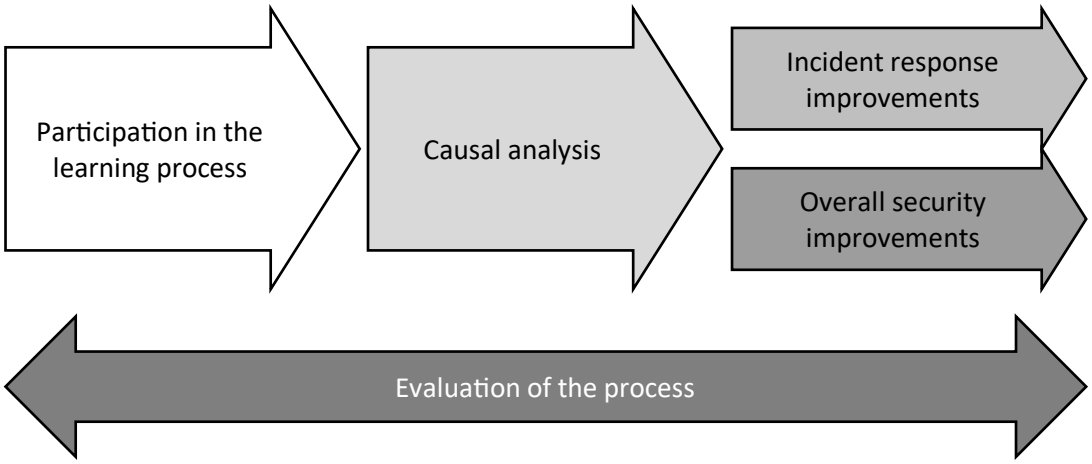
For this review, we sought to analyse the learning process in more depth to understand the activities organisations conduct to learn from incidents, identifying learning process models with greater detail. Drupsteen et al. (2013) developed a learning from incidents process model based on a review of safety literature and consulting with safety experts from industry. This model emphasised investigating the cause in order to acquire knowledge and translate that knowledge into actions, including an evaluation step to assess the effectiveness of implementing the lessons learnt.

Lukic et al. (2012) also developed a framework for learning from safety incidents based on the literature and validated the model at two organisations. Littlejohn et al. (2017), incorporating input from additional sites and companies and sharing lessons learned with others, examined the learning process in terms of context, participants, type of incident, and knowledge. Despite the relative maturity of safety research compared to cyber security research on learning from incidents, it has yet to develop a unifying theory (Swuste et al., 2020). To create a practical tool for collecting data on the learning practices, the process definitions from both the Littlejohn et al. (2017) and Drupsteen, et al., (2013) models were combined to include the end-to-end process. These two studies provided the most comprehensive analysis of the learning process activities organisations can perform.

To provide more insight into the coverage of the research for cyber security, the interventions or actions step was split into two parts: incident response improvements, and overall security improvements. This distinction was made to separate studies that only covered improvements to an organisation's incident response capability from those that also studied how lessons led to changes in the wider security posture. This created five categories: participation in the learning process, causal analysis, incident response improvements, overall security improvements, and evaluation of the learning process.

Participation in the learning process includes how learning is organised and the involvement of different areas of the organisation. Causal analysis includes reporting incidents, categorising incidents, and analysing the causes. Both improvement categories include determining and prioritising actions, allocating accountability, dedicating resources, and tracking actions to completion. The participation of different teams and the learning approach taken will impact the breadth of causes considered, and the causes found will impact the improvements made. How these improvements are implemented can affect the organisation's security. The final learning evaluation phase includes ensuring that actions are completed and confirming that the actions enabled the anticipated improvements. It also includes evaluation of how well the organisation is learning from incidents. Insights from this phase help an organisation improve its learning process. A poor learning process would be evident through the recurrence of incidents with similar causes or impacts, indicating the organisation has not adapted its protection, detection, and response capabilities. The phases of the learning process set out in Figure 2 were used to collect the data in Table 4 using a deductive approach to examine and describe the coverage of learning.

Figure 2 *The phases of the learning process adapted from Drupsteen, Groeneweg, et al. (2013) and Littlejohn et al. (2017)*



2.2.2 Research and publication details

This section provides an overview of the research interest in the topic, including the annual publication trends, preferred publishing venues, and geographical research clusters. This analysis offers insights into the existing research on organisational learning from cyber security incidents. Despite the increase in cyber security incidents, there are surprisingly few studies dedicated to exploring how organisations can learn from these incidents to mitigate their impact and frequency. Articles are only categorised by data collection when this is explicitly stated. Several of the included papers were part of larger, multi-year research programmes, and as such, multiple publications were derived from the same underlying project. For example, the papers by Jaatun et al. (2009) and Line et al. (2006) both stem from the "Incident Response MAnagement" (IRMA) project, funded by the IKT SoS programme of the Research Council of Norway and The Norwegian Oil Industry Association (OLF), 2005 to 2007. Similarly, the work by Bartnes et al. (2016) and Line (2013) was conducted as part of a research programme involving power distributors in Norway. Grispos et al. (2015, 2017, 2019) all report findings from the same research project at a UK financial organisation. He, Johnson, Lu, et al. (2014) and He & Johnson (2015, 2017) relate to the same research project at a Chinese healthcare provider while He et al. (2015) and He, Johnson, Renaud, et al. (2014) draw on related work concerning the usability of Goal Structuring Notation (GSN).

Figure 3 *PRISMA flow presenting the inclusion process*

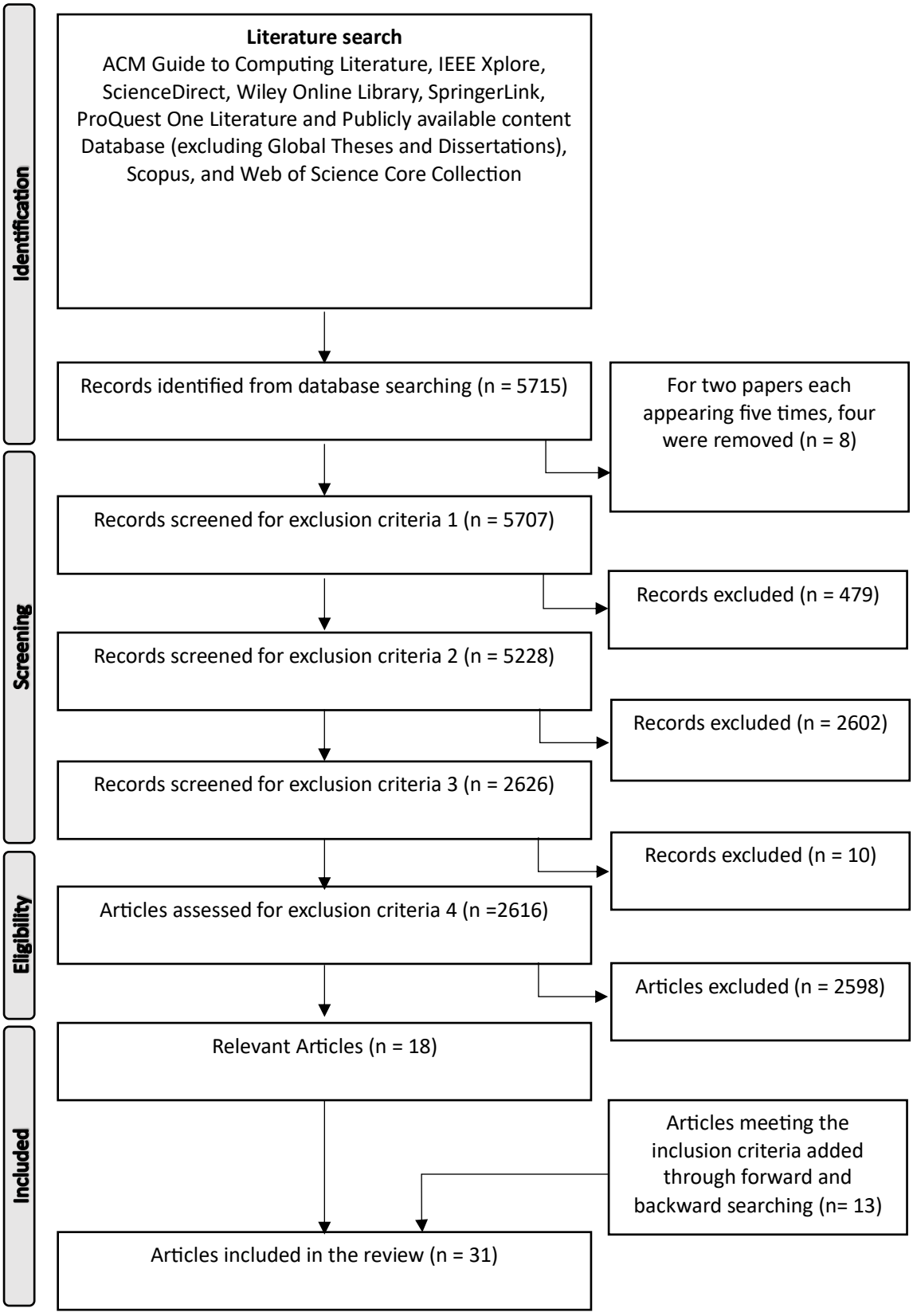
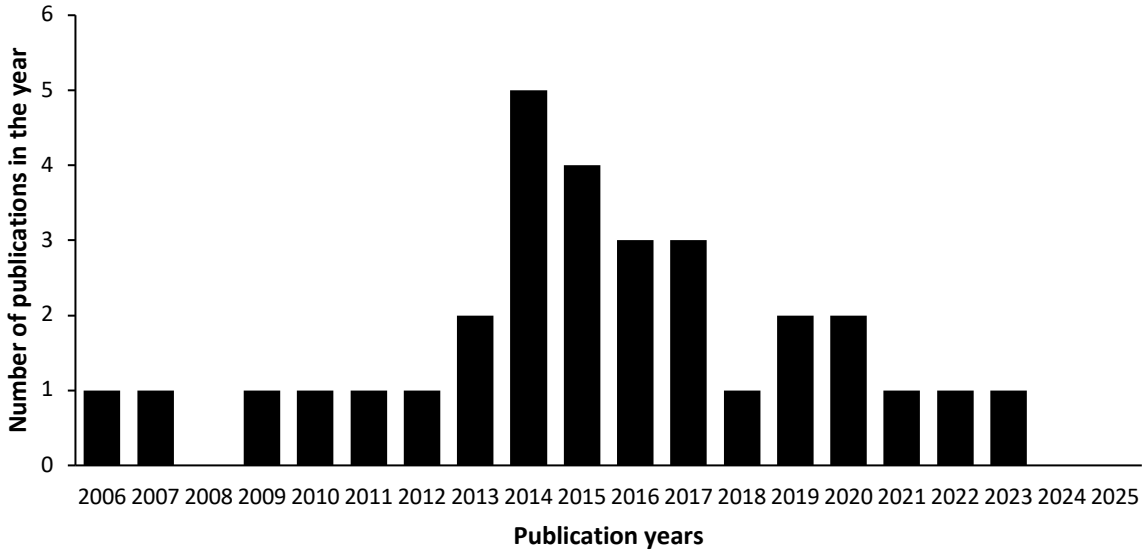


Figure 4 *The publication year of the articles analysed*



All selected articles were published within the last 19 years. The timing of the publications does not show a distinct trend, although there was a noticeable surge in activity between 2014 and 2016. However, given the small sample size, such fluctuations are anticipated. There has been a sustained interest in the topic, as depicted in

Figure 4. The most frequent publication venue was the *Computers & Security* journal, which featured five papers on the topic. Nonetheless, there was a diverse set of venues, including the *International Journal of Information Management* and the *Hawaii International Conference on System Sciences*.

Table 5 *Geographical location where the analysed studies were conducted*

Geographical location of where the study was conducted	No. of papers	References
Australia	5	(Ahmad et al., 2012a, 2015, 2020; Lakshmi et al., 2021; Shedden et al., 2011)
China	5	(He et al., 2015; He, Johnson, Lu, et al., 2014; He, Johnson, Renaud, et al., 2014; He & Johnson, 2015, 2017)
Europe (specific countries not listed)	1	(Baskerville et al., 2014)
Netherlands	1	(Van der Kleij et al., 2017)
Norway	5	(Bartnes et al., 2016; Jaatun et al., 2009; Line, 2013; Line et al., 2006, 2016)
UK	5	(Grispos et al., 2014, 2015, 2017, 2019; He et al., 2022)

Geographical location of where the study was conducted	No. of papers	References
Unspecified or not applicable	9	(Bernsmed & Tøndel, 2013; Ebert et al., 2023; M. Evans et al., 2019a; Horne et al., 2020; Line & Albrechtsen, 2016; Shedden et al., 2010; Sveen, Sarriegi, et al., 2007; Tatu et al., 2018; Tøndel et al., 2014)

The geographical location in which the studies were conducted is shown in Table 5. The majority of the selected papers were conducted in four countries and in only three sectors—i) the Norwegian energy industry (Bartnes et al., 2016; Jaatun et al., 2009; Line, 2013; Line et al., 2006, 2016); ii) Australian (Ahmad et al., 2012a, 2015; Shedden et al., 2011) and UK financial services (Grispos et al., 2017a, 2019); iii) Chinese (He et al., 2015; He, Johnson, Renaud, et al., 2014; He & Johnson, 2015, 2017) and UK healthcare (He et al., 2022). There were 9 papers where the location was not specified or not applicable (for example, articles presenting literature reviews).

Table 6 highlights the diverse research methods applied to studying organisational learning from cyber security incidents. The table includes studies that review existing literature, such as Shedden et al.'s (2010), which focused on organisational learning, Tøndel et al.'s (2014) reviewing current incident management practices, and Line and Albrechtsen (2016) and Ebert et al. (2023), who explored how theories and techniques from industrial safety could be applied to cyber security. The paper by Grispos et al. (2014) evaluated the standards for incident management and is focused on using Agile concepts in incident management yet also highlights the importance of learning and encourages organisations to learn throughout the incident lifecycle. Horne et al. (2020) reviewed both academic literature and industry standards with a focus on the governance of incident response, highlighting the lessons learned phases in both the standards and the literature. Additionally, there were theoretical studies such as those by Bernsmed and Tøndel (2013) and He et al. (2015; 2014) which not only discussed existing literature but also introduced new models or analytical approaches. Other studies developed models that were applied to either hypothetical case studies or publicly available data, exemplified by Ahmad et al. (2020) and He et al. (2022).

Table 6 *Research methods used by the articles analysed*

Research Methods Used	No. of papers	References
Case study	9	(Ahmad et al., 2012, 2015; Bartnes et al., 2016; Baskerville et al., 2014; Evans et al., 2019; Grispos et al., 2017, 2019; He & Johnson, 2017; Line, 2013)
Combination of methods (interviews, case studies, questionnaires and workshops, or incident analysis)	1	(Jaatun et al., 2009)
Focus groups	1	(Shedden et al., 2011)
Interviews	8	(Grispos et al., 2015; He, Johnson, Lu, et al., 2014; He & Johnson, 2015; Lakshmi et al., 2021; Line et al., 2006, 2016; Tatu et al., 2018; Van der Kleij et al., 2017)

Research Methods Used	No. of papers	References
Literature review	6	(Ebert et al., 2023; Grispos et al., 2014; Horne et al., 2020; Line & Albrechtsen, 2016; Shedden et al., 2010; Tøndel et al., 2014)
Systems thinking	1	(Sveen, Sarriegi, et al., 2007)
Theoretical study	5	(Ahmad et al., 2020; Bernsmed & Tøndel, 2013; He et al., 2015, 2022; He, Johnson, Renaud, et al., 2014)

Numerous studies have employed interviews or focus groups to gather data (Grispos et al., 2015; He, Johnson, Lu et al., 2014; He & Johnson, 2015; Lakshmi et al., 2021; Line et al., 2006, 2016; Shedden et al., 2011; Tatu et al., 2018; Van der Kleij et al., 2017). Interviews are a valuable method for understanding social processes and participant perspectives, although it is crucial that responses are interpreted within the context they are provided (Silverman, 2017). Due to their relatively quick execution compared to in-depth case studies, interviews allow for the inclusion of a broader range of organisations (Lakshmi et al., 2021; Line et al., 2006, 2016; Van der Kleij et al., 2017) and can offer a more comprehensive perspective by involving multiple participants from the same organisation (Grispos et al., 2015; He, Johnson, Lu, et al., 2014; He & Johnson, 2015; Tatu et al., 2018).

Case studies are another commonly used research method (Ahmad et al., 2012, 2015; Bartnes et al., 2016; Baskerville et al., 2014; Evans et al., 2019; Grispos et al., 2017, 2019; Große et al., 2020; He & Johnson, 2017; Line, 2013), often combined with other research techniques (Jaatun et al., 2009). They are particularly effective for exploring real-world practices and addressing 'how' or 'why' research questions (Yin, 2018). While generalising findings from a single case study can be challenging, the accumulation of multiple case studies presenting similar results about learning from incidents allows researchers to construct a broader understanding of organisational approaches to learning. However, gaining access to organisations for such studies can be challenging, especially given the sensitive nature of the information regarding incidents (Ahmad et al., 2012; Bartnes et al., 2016).

The extensive use of case studies has provided valuable insights into how organisations learn from incidents. Yet much of this research was conducted between five to ten years ago, a period when the frequency and severity of incidents were generally lower than they are now for many organisations. Additionally, few studies have specifically focused on learning, with the majority only mentioning lessons learned as a minor aspect of broader research study. Given the rapid pace of change in cyber security, there is a clear need for new studies that specifically focus on learning from incidents.

2.2.3 Research foundations

The models and standards that shape the research framework, such as the NIST Special Publication 800-61 Revision 2, are outlined in this section, which examines the advantages and constraints of these foundations both in relation to the broader field and to this specific study. An analysis of how researchers structured their studies reveals various underlying frameworks used. Table 7 indicates that safety research commonly serves as the principal foundation for existing studies. Management science ranks as the next most utilised foundation, with further studies leveraging IT standards to guide their research. Additionally, elements from software engineering and psychology have been integrated into a selection of studies, broadening the interdisciplinary approach within this domain.

Table 7 *Research foundations used to frame the studies*

Research foundations used	Origin	No. of studies	References
4I model	Management Science	2	(Ahmad et al., 2015, 2020)
Agile Manifesto	Software engineering	3	(Grispos et al., 2014, 2017a; He et al., 2022)
Goal Structuring Notations (GSN)	Safety	5	(He et al., 2015; He, Johnson, Lu, et al., 2014; He, Johnson, Renaud, et al., 2014; He & Johnson, 2015, 2017)
Human Error Assessment and Reduction Technique (HEART) & Human Reliability Analysis (HRA)	Safety	1	(Evans et al., 2019)
Incident Response Management (IRMA) & Sequential Timed Events Plotting (STEP)	Safety	1	(Jaatun et al., 2009)
Incident-centred security	Security	1	(Baskerville et al., 2014)
ISO/IEC 27035-2	IT Standard	5	(Bartnes et al., 2016; He & Johnson, 2017; Line, 2013; Line et al., 2006, 2016)
Needs Assessment	Psychology	1	(Van der Kleij et al., 2017)
NIST Special Publication 800-61 Revision 2	IT standard	4	(Ahmad et al., 2020; Grispos et al., 2015; He & Johnson, 2017; Line et al., 2006)
Organisational learning such as double-loop learning	Management Science	4	(Ahmad et al., 2012a, 2020; Shedden et al., 2010, 2011)
Resilience based Early Warning Indicators (REWI)	Safety	1	(Bernsmed & Tøndel, 2013)
Sensemaking	Psychology	1	(Lakshmi et al., 2021)
Systems Thinking	Management Science	1	(Sveen, Sarriegi, et al., 2007)
Theory of involvement	Psychology	1	(Tatu et al., 2018)
Unspecified or not applicable	-	4	(Ebert et al., 2023; Grispos et al., 2019; Horne et al., 2020; Tøndel et al., 2014)

Note: some researchers applied multiple models in the same paper (Ahmad et al., 2020; He & Johnson, 2017; Line et al., 2006).

ISO/IEC 270035-2 (2023) and NIST Special Publication 800-61 Revision 2 (2012) have been extensively used in the studies under review: ISO/IEC 27035-2 (Bartnes et al., 2016; Jaatun et al., 2016; Line, 2013; Line et al., 2006, 2016) and NIST Special Publication 800-61 Revision 2 (Ahmad et al., 2020; Grispos et al., 2015). The inclusion of learning as a component of their end-to-end processes has prompted these studies to focus specifically on this aspect of incident management. For instance, Grispos et al. (2015) implemented a case study in a global Fortune 500 financial organisation in the UK, employing an exploratory series of interviews framed by the NIST Special Publication 800-61 Revision 2 phases to present the Security Incident Response Criteria (SIRC), which assesses cyber security incident response solutions.

The lessons learned phase of ISO/IEC 270035-2 (2023) prompts organisations to identify lessons that could enhance their controls, risk assessments, and overall incident management. It also encourages the identification of trends that may provide early warnings of potential future incidents. While both NIST Special Publication 800-61 Revision 2 (2012) and ISO/IEC 270035-2 (2023) provide guidelines for questions to be asked during post-incident meetings, these questions primarily focus on improving incident response. Given that these standards do not extensively cover learning, studies utilising them have often integrated models from management science (Ahmad et al., 2012a, 2015, 2020; Ebert et al., 2023; Jaatun et al., 2009; Jaatun & Tøndel, 2015; Shedden et al., 2010, 2011; Sveen, Sarriegi, et al., 2007) to enrich their analytical framework.

Many studies in this research draw on the concept of “double-loop learning”, which was first introduced by Argyris in the 1970s (Argyris, 1976). For instance, Grispos et al. (2017) highlighted that without a genuine commitment to learning, organisations fail to address underlying causes. For organisations unfamiliar with causal analysis and organisational learning, implementing the double-loop learning model can be challenging without additional support.

In the Norwegian oil and gas industry, a method called Incident Response Management (IRMA[4]) has been developed, incorporating Argyris's concept of double-loop learning (Argyris, 1976). The IRMA model integrates phases from the ISO/IEC 270035-2 (2023) and NIST Special Publication 800-61 Revision 2 (2012) standards and emphasises the post-incident learning phase, drawing from the Sequential Timed Events Plotting (STEP) method, which was introduced by Hendrick and Benner in their 1986 book, *Investigating Accidents with STEP*. The model is designed to help teams identify root causes and vulnerabilities in the barriers they have established to prevent accidents.

Bernsmed and Tøndel (2013) adapted the Resilience based Early Warning Indicators (REWI) method, originally designed for safety incidents in the Norwegian energy sector, to address cyber security incidents. The REWI method categorises the attributes necessary for resilience against incidents into three key areas: risk awareness, response capacity, and support (encompassing technical, human, and organisational aspects). It emphasises the importance of learning from incidents, including those where responses were successful, as resilience involves strengthening an organisation's capacity to respond effectively. Ebert et al. (2023) used a narrative review technique to compare various models from safety science that could be applied to understanding the causes of security incidents. They argue that incidents do not have a singular cause but can be interpreted through multiple “realities”. To support this, they provide a framework enabling practitioners to select a model that aligns with the specific incident under investigation and the resources available for the analysis.

Five studies, (He et al., 2015; He, Johnson, Lu, et al., 2014; He, Johnson, Renaud, et al., 2014; He & Johnson, 2015, 2017) investigated the use of Goal Structuring Notations (GSN), a safety engineering approach originally developed for safety-critical systems, to analyse potential causes of cyber security

[4] IRMA is the abbreviation of **I**ncident **R**esponse **MA**nagement.

incidents. GSN, established over several years by the Safety-Critical Systems Club, enables organisations to construct safety cases for critical infrastructure (The Assurance Case Working Group, 2021). The primary aim of this notation is to articulate the causes of incidents as failures in controls or policies.

He, Johnson, Renaud, et al. (2014) conducted two studies involving students. The first involved training them in GSN techniques and evaluating their efficacy, while the second tasked students with using the GSN template to map the causes of a simplified incident and build a safety case. Subsequently, GSN was trialled at a Chinese healthcare provider (He, Johnson, Lu, et al., 2014; He & Johnson, 2017). The feedback received was mixed; although some groups, such as those within the incident response team, found it a valuable framework, its applicability was limited for broader audiences. GSN, with its mechanistic perspective, delineates incidents as failures within a system component, assuming a known and linear relationship between components. This characteristic means it is primarily suited for assessing system issues rather than eliciting socio-technical and underlying causes.

Others have adopted the Agile approach from software engineering (Grispos et al., 2014, 2017a; He et al., 2022). This approach originated from the Manifesto for Agile Software Development, which has significantly influenced software product development. Beck et al. (2001) and Grispos et al. (2017) experimented with employing this methodology to learn from security incidents. While agility in incident response is crucial, adapting certain Agile principles can be challenging due to the core design and planning principles of product development versus the inherently reactive nature of incident response. Nevertheless, Agile's emphasis on continuous learning and product refinement could be beneficial in involving software developers familiar with Agile methods in incident learning processes.

Several researchers have incorporated psychology models into their studies. Lakshmi et al. (2021) employed the concept of sensemaking, typically used to analyse socio-cognitive and socio-organisational activities, applying a socio-technical lens to the activities of Cyber Security Incident Response Teams (CSIRT). While their study did not delve deeply into learning from incidents, it did explore how individuals construct narratives about what transpired during an incident, finding that incident responders engaged in “Enactment”, “Selection”, and “Retention” to make sense of the incident response process. Van der Kleij et al. (2017) used four needs assessment categories—Organisation, Team, Individual, and Instruments—to understand the skills required by CSIRTs. They concluded that organisational learning from incidents needed enhancement and recommended the implementation of a lessons learned procedure to improve performance. Tatu et al. (2018) adapted involvement theory to security contexts, transforming the “knowledge” dimension into “experience sharing”, which included lessons learned from security incidents. Their study of an organisation that had suffered a ransomware attack revealed improvements in security awareness, potentially safeguarding the organisation against similar future incidents. Overall, the literature reviewed utilises a diverse collection of models; however, there has yet to be a comparative analysis of the models proposed by researchers or specific recommendations on which approaches organisations should adopt in particular scenarios. Further research is required to test and recommend the best models for organisations to use to understand the causes of cyber security incidents.

2.2.4 Learning practices

The concept of an organisational learning process is central to understanding how organisations adapt and improve from experiences. This section explains the relevance of organisational learning processes and how they were used to evaluate the extent to which existing literature covers these learning practices. The discussion then examines how the selected studies address each phase of the organisational learning process as outlined in Figure 2.

The assessment of the selected articles' coverage of the learning process utilises the five phases depicted in Figure 2. Each phase's coverage by the articles is categorised using the following graphic symbols:

a) ● "Substantial coverage" represents articles that comprehensively address this part of the process.

b) ◑ "Partial coverage" is noted where the topic is discussed but not all relevant aspects are covered. For example, an article might suggest an approach to causal analysis but fail to consider how it would be conducted amid organisational politics and agendas, or it might suggest improvements without including the prioritisation or tracking of actions.

c) ◔ "Light touch" is used when a paper only briefly comments on the topic. An example of this would be a reference to the distribution of a post-incident report to management without covering other participation aspects, such as who was involved in analysing the causes or deciding on the lessons learned.

d) ○ "None" indicates no explicit mention of the topic within the article.

Due to the lack of a consensus framework for researching learning practices, there are inconsistent approaches to describing the learning expected or observed by researchers. This inconsistency is evident in Table 8, which showcases the varied ways in which learning practices are addressed across the studies.

Table 8 *Coverage of the learning process by the articles analysed*

Articles	Participation in the learning process	Causal analysis	Incident response improvements	Overall security improvements	Evaluation of the process
(Grispos et al., 2015; He et al., 2015; He, Johnson, Renaud, et al., 2014)	○	◑	◔	◔	○
(Line et al., 2006)	◑	◑	◑	◑	◑
(Sveen, Sarriegi, et al., 2007)	○	◔	◑	◑	◔
(Jaatun et al., 2009)	◔	◑	◔	◔	○
(Shedden et al., 2010)	◔	◔	●	◑	○
(Shedden et al., 2011)	○	○	●	◔	○
(Ahmad et al., 2012)	●	●	●	●	○
(Bernsmed & Tøndel, 2013)	○	◔	◑	◔	◔
(Line, 2013)	○	○	◔	○	○
(Baskerville et al., 2014)	○	◑	◑	◑	○
(Tøndel et al., 2014)	●	◑	◑	◑	◔
(He, Johnson, Lu, et al., 2014)	◔	◑	◑	◑	○

Articles	Participation in the learning process	Causal analysis	Incident response improvements	Overall security improvements	Evaluation of the process
(Grispos et al., 2014)	○	◑	◔	◔	○
(Ahmad et al., 2015)	●	●	●	●	◔
(He & Johnson, 2015)	○	◑	◔	◑	○
(Line et al., 2016)	◔	◔	○	○	○
(Line & Albrechtsen, 2016)	◑	◑	◔	◔	○
(Bartnes et al., 2016)	●	◔	◔	◔	●
(He & Johnson, 2017)	◔	◑	◑	◑	◔
(Van der Kleij et al., 2017)	○	○	◑	◔	◔
(Grispos et al., 2017)	◑	◑	●	●	●
(Tatu et al., 2018)	○	○	○	◔	○
(Grispos et al., 2019)	○	◑	◔	◔	○
(Evans et al., 2019)	○	●	◔	◔	○
(Ahmad et al., 2020)	○	●	◑	◑	◔
(Horne et al., 2020)	○	◔	◔	◔	○
(Lakshmi et al., 2021)	◑	●	◑	◔	○
(He et al., 2022)	◔	◔	◑	◑	○
(Ebert et al., 2023)	●	●	◔	◔	◑

2.2.4.1 Participation in the learning process

Most researchers did not specify which members of the organisation participated in learning from incidents, with less than a third of the studies addressing this aspect in any depth. Those who did explore this facet generally found that formal learning processes were typically reserved for major incidents (Ahmad et al., 2012a, 2015; Line, 2013; Line et al., 2016). There is a prevailing recommendation among researchers that organisations should broaden their scope to include learning opportunities from a wider range of incidents. For instance, Ahmad et al. (2015) highlighted the potential to learn about critical assets, technology risks, and the causal structures of security incidents from an expanded selection of events.

These comprehensive reviews of major incidents often only included individuals directly involved with the incident (Ahmad et al., 2012, 2015; Grispos et al., 2017; Jaatun et al., 2009). For example, research by Ahmad et al. (2012, 2015) indicated that only technical teams participated in post-incident learning, potentially limiting the identification of causes to technical aspects alone. Grispos et al. (2017) recognised a limitation in that incident response teams did not develop actions on the lessons learned for issues beyond their direct responsibilities. Bartnes et al. (2016) proposed that organisations might benefit from employing trained facilitators to enhance the effectiveness of retrospective analyses to identify lessons from incidents, although the specific benefits of this approach remain underexplored. Ebert et al. (2023) underscored the importance of incorporating diverse perspectives on incident

causes and demonstrated how systematic models from safety science, designed for investigating incidents, rely on gathering insights from multiple stakeholders.

Furthermore, researchers observed that lessons identified from incidents were often not disseminated beyond the incident response teams (Ahmad et al., 2012, 2015; Grispos et al., 2017; Jaatun et al., 2009). Line et al. (2006) underscored the importance of sharing lessons from incidents across all parts of the organisation, including management, suppliers, and employees, to ensure comprehensive organisational learning. Despite this general trend, there were notable exceptions. He and Johnson (2017) reported that the healthcare provider they studied conducted informal meetings to share lessons learned with various stakeholders. In a case study by Baskerville et al. (2014), which examined three organisations (rail, postal, and military), it was found that the postal organisation began to share more incident data with its competitors following a serious incident, indicating a shift towards greater openness in the sharing of security insights.

The literature has not extensively covered the impact of sharing lessons from security incidents with different stakeholders and peers. Jaatun et al. (2009) highlighted the importance of learning from incidents and recommended the IRMA model, wherein learning is integrated back into the preparation phase. However, during their fieldwork, Jaatun et al. (2009) found that few respondents had directly experienced a security incident. For those who had, the interval between incidents ranged from one to two years, providing the researchers with limited practical examples to analyse. Additionally, the study uncovered a cultural reluctance to report incidents, suggesting that respondents might not have been fully aware of all incidents occurring within their organisations. Although many interviewees acknowledged the significance of the learning phase, opinions varied, with some expressing scepticism about its effectiveness, fearing that the lessons learned would be quickly forgotten. The reasons behind these differing perspectives were not clearly articulated in the study.

The organisations examined by Bartnes et al. (2016) had not experienced any major cyber security incidents; however, they routinely conducted post-incident reviews for safety incidents. Consequently, it was anticipated that they would apply similar practices to security incidents should they arise. The main challenges identified included a lack of prioritisation for learning activities, inadequate efforts to understand underlying causes, and missed opportunities to apply lessons learned to enhance the overall security posture of the organisation. Bartnes et al. (2016) noted that even minor incidents could provide valuable learning opportunities and recommended that organisations engage in more in-depth learning for all incidents, regardless of their scale. However, the benefits of analysing minor incidents were not specifically explored in their study.

In another study by Shedden et al. (2011), the role of informal learning within Cyber Security Incident Response Teams (CSIRTs) was investigated through a focus group involving five security professionals. This study identified potential for organisations to benefit from integrating both formal and informal learning processes, as these approaches can mutually reinforce each other. Despite recognising the value of informal learning, the paper did not detail specific strategies to facilitate or enhance this type of learning within organisations.

2.2.4.2 Causal analysis

This aspect of the incident learning process has garnered the most attention from researchers. Although many studies indicate that respondents recognise the need for learning, there is limited evidence of comprehensive investigations to uncover underlying causes (Ahmad et al., 2012; Jaatun et al., 2009). Grispos et al. (2015) reported that seven out of ten respondents conducted root cause analysis post-incident, and all recognised the potential to enhance security measures through post-incident analysis.

Shedden et al. (2010) observed that most research on incident response has been technically focused, highlighting an opportunity to apply organisational learning principles to identify and address underlying causes to strengthen both incident response and organisational security. Baskerville et al. (2014) noted that, in one of the three companies they studied, more in-depth learning was implemented following serious incidents, though the article offers scant details on this process. In a more recent study, Ahmad et al. (2020) explored how the integration of security management and incident response teams through a double-loop learning model could enhance organisational learning and security. Using a hypothetical incident, they developed a conceptual framework demonstrating that greater integration between these teams could improve learning opportunities and subsequently enhance organisational security. Ahmad et al. (2020) also discussed how double-loop learning helps organisations to reassess the assumptions underlying their information security management systems. Ebert et al. (2023) noted that single-factor models with a clear root cause might contribute to human error often being described as the primary cause in cyber security literature. They described how safety research has evolved to include linear, cultural and management, systemic control, and resilience models. Ebert et al. (2023) suggested that models should be selected based on the purpose and scope of the incident review, as well as the skills of the investigators conducting the review.

Lakshmi et al. (2021) discovered that post-incident reviews could update the mental models that incident responders maintain about the causes of incidents, aiding in understanding subsequent incidents. Evans et al. (2019) adapted the Human Error Assessment and Reduction Technique (HEART) to analyse human error and underlying causes based on a year's worth of security incidents reported at a service provider. Their analysis aimed to calculate human error probabilities and found that the actual likelihood of incidents being caused by human error was lower than predicted, suggesting a need for further recalibrations for more accurate predictions. Over half of the incidents in their study were attributed to human error, leading to a recommendation for organisations to delve deeper into the root causes to identify conditions that allow errors to occur, thereby helping to prevent future incidents. Although the studies reviewed how organisations investigate the causes of incidents, there was no in-depth analysis of which tools and techniques are most effective, which remains a gap in the literature.

2.2.4.3 Incident response improvements

While most studies have highlighted the security benefits that can be derived from lessons learned, there has been a greater focus on enhancing the capabilities of incident response teams rather than on broader security measures (Bernsmed & Tøndel, 2013; Lakshmi et al., 2021; Shedden et al., 2010; Van der Kleij et al., 2017). The Agile retrospectives discussed in Grispos et al. (2017) facilitated incident response teams in pinpointing specific areas for improvement in their response strategies. However, the literature generally lacks detailed information on how organisations determine which improvements to implement, prioritise resources, or track the progress of these enhancements. There seems to be an underlying assumption that once a team has identified the causes of an incident, they will naturally proceed to implement the necessary improvements. This assumption contrasts with the definition of organisational learning provided by Fiol and Lyles (1985), which clearly differentiates between the acquisition of knowledge and the subsequent action.

2.2.4.4 Overall security improvements

In the study conducted by Ahmad et al. (2015), it was observed that there was no direct connection between post-incident analysis and the information security team within the company studied. Some respondents viewed this as a missed opportunity to enhance policies based on the lessons learned from incidents. The researchers suggested that this disconnect might be attributed to cost pressures that limit broader organisational changes. Line and Albrechtsen (2016), examining the literature through an earlier version of the framework of ISO/IEC 270035-2 (2023), advocated for organisations to adopt more adaptive approaches to incident management rather than merely updating existing

standards or introducing additional procedures. They called for further empirical research into how industrial safety methods could be adapted for managing cyber security incidents, suggesting that more flexible strategies could lead to more effective overall security enhancements.

2.2.4.5 Evaluating the learning

Although the research assessed learning practices, there was scant discussion on the learning process itself and how organisations evaluated the effectiveness of their learning. Grispos et al. (2017) experimented with lightweight Agile retrospectives in a financial organisation. They introduced two types of retrospectives; the first focused on evaluating what worked and what did not during the incident response, while the second type, termed 'meta-retrospectives', assessed the effectiveness of the lessons learned from past incidents. They discovered that these retrospectives were beneficial in enhancing the identification of post-incident actions aimed at improving security measures. However, less than half of the retrospectives contained more detailed information, and it remained unclear whether the discussions included analysis of underlying causes and risks. Furthermore, senior business leaders appeared not to be engaged in the post-incident learning process, as the actions identified in the post-incident review were ultimately not implemented by the organisation.

Bartnes et al. (2016) found that the organisations they studied did not make significant investments in learning to enhance their incident response capabilities. The study highlighted that management commitment is crucial for facilitating learning. It noted that, since these organisations had not experienced significant incidents, they might not yet recognise the risks and the value of investing in learning. While they do not explicitly discuss how to improve the end-to-end learning process, Ebert et al. (2023) urged organisations to consciously select the most appropriate model from their taxonomy when analysing the causes of an incident. However, that paper focused on analysing incident cause models that could be used; it did not assess the learning practices organisations have adopted in practice. The authors called for further research to determine which models and practices actually improve cyber security in organisations.

None of the studies indicated that organisations were actively exploring ways to enhance their learning processes or had implemented measures to evaluate their learning capabilities and the effectiveness of improvements following incidents (Ahmad et al., 2015; Line, 2013). It remains unclear whether the researchers directly sought data on evaluation practices. In Ahmad et al.'s (2012) study, the company credited a significant reduction in incidents to their learning practices, although the specifics of how this outcome was measured were not detailed. Line et al. (2006), in their paper on incident response metrics, proposed using a "five orders of feedback" model, based on an earlier version of ISO/IEC 270035-2 and the work by Van Court Hare (1967) on learning from experience. They also suggested the incorporation of incident response metrics across organisations, one of which was "learning" which could be used to assess the effectiveness of learning from incidents. However, they acknowleged these may be difficult to quantify, and their proposals were not empirically tested with organisations.

2.2.5 Summary of the cyber security literature and research gaps

This section reviews the existing research on how organisations learn from cyber security incidents, identifying under-researched areas and establishing a foundation for exploring relevant insights from other domains. While some studies address organisational learning in this context, the academic literature remains sparse. This limited body of work provides insufficient guidance on how organisations can effectively apply lessons from incidents to mitigate future risks.

Many existing articles explicitly call for further research into this area, underlining a persistent need for deeper understanding (He, Johnson, Renaud, et al., 2014; Line & Albrechtsen, 2016; Shedden et al., 2010; Tøndel et al., 2014). The scarcity of focused research on how organisations effectively learn from cyber security incidents suggests that there is substantial scope for studies that could provide

valuable insights into enhancing organisational resilience and security postures. This gap presents an opportunity to expand current knowledge by integrating established learning frameworks from other disciplines, adapting them to enhance security incident learning within organisations.

2.2.5.1 Learning practices

While there is a general agreement that organisations would benefit from enhancing how they learn from incidents, consensus on the best methods to achieve this or on what constitutes good practice is lacking. The absence of a consistent model and common terminology for describing learning hinders the sharing of ideas and best practices. This challenge is not unique to the relatively new field of cyber security; even in well-established fields such as management science, the adoption and evolution of models occur gradually over time (Piazza & Abrahamson, 2020). However, the lack of agreement on how to assess learning from incidents hinders the progress of both academic research and practical implementation.

2.2.5.2 Evaluating the learning capability

To date, there has been minimal focus on how organisations assess the effectiveness of their learning capabilities. It remains unclear how organisations should evaluate and continuously improve their ability to learn. While there has been extensive research on learning in organisations within the field of management science, such as the work by Garvin et al. (2008), who recommended enhancing learning capability by fostering a supportive environment, establishing robust learning processes, and ensuring leadership commitment, no studies have yet examined whether these approaches are effective for improving learning from cyber security incidents. To fully understand and enhance learning capabilities in the context of cyber security, future research must assess whether the measures implemented, based on lessons learned from incidents, effectively reduce the frequency of future incidents. This approach would not only validate the effectiveness of learning strategies but also contribute to a more resilient organisational stance against cyber threats.

In the selected studies, none reported attempts to measure how learning from incidents improved security, nor did they mention if the organisations evaluated their own learning capabilities. As previously noted, it is challenging to robustly measure incidents, and much of the research operates under the implicit assumption that learning from incidents is beneficial, without seeking explicit evidence to support this view. Researchers found that post-incident reviews are typically conducted only for major incidents, not necessarily those with the greatest learning opportunities, nor do they often invest time in learning from systemic causes (Ahmad et al., 2015; Bartnes et al., 2016). Few studies acknowledge the dilemmas faced by organisations in dedicating time and resources to learning.

Ahmad et al. (2015) suggested that further research is needed to explore the competing priorities of security management and incident response teams to understand how these can be balanced to maximise the security of an organisation's technology. While researchers have urged organisations not to focus only on high-impact incidents but also to ensure broader participation, more research is needed to determine the optimal balance where the investment in learning activities is justified by the benefits.

However, using data to measure the effectiveness of learning in reducing the number of future incidents is extremely challenging due to the lack of independent and reliable sources of incident data available to academic researchers (Salane & Jay, 2011). As Ryan and Jefferson (2003) concluded, "In the information security arena, there is no reliable data upon which to base decisions. Unfortunately, there is unreliable data that is masquerading as reliable data." Although this study was twenty years ago, similar challenges persist, as highlighted in a more recent study by Neto et al. (2021).

Organisations need to balance the effort between learning from incidents and responding to them. Addressing underlying causes, if accurately identified, should theoretically reduce the number of incidents. Sveen, Sarriegi, et al. (2007) and Gonzalez (2005), using systems thinking, mapped this feedback loop in their systems diagrams of incident response teams. However, none of the research has studied this trade-off within organisations to determine the optimal balance. Understanding this balance is crucial for developing strategies that not only respond effectively to incidents but also learn from them to prevent recurrence.

2.2.5.3 Participation in learning

The studies indicate that the broader organisation is rarely involved in post-incident reviews, and reports are often not disseminated beyond the incident response team and their immediate management (Ahmad et al., 2012, 2015). Lukic et al. (2012) found a contradiction in the realm of safety incidents, where individuals wanted to be included in learning activities but were concerned about the additional effort required. This underscores the importance of researchers considering the commercial realities of investing time and resources in learning processes.

With the exception of the work by He, Johnson, Lu, et al. (2014), most studies have focused on incident response teams, neglecting the wider organisation outside of IT, which can also benefit from learning from incidents (Russell Vastveit et al., 2015). In the organisation studied by Tatu et al. (2018), it was found that user awareness improved following a ransomware incident. However, more research is needed to understand how lessons from cyber security incidents can be disseminated and learned by the entire organisation.

Jaatun et al. (2009) highlighted the lack of involving suppliers in post-incident learning. As organisations increasingly rely on an ecosystem of suppliers, more research is needed to clarify how these relationships can be leveraged to enhance learning from incidents. Understanding and improving the dynamics between organisations and their suppliers in the context of learning from incidents could significantly bolster overall cyber security resilience. Ensuring the broader involvement of the organisation and its supply chain in post-incident reviews can enhance the quality of the learning from incidents by bringing different perspectives on the causes and on the subsequent actions to take as a result of the lessons.

2.2.5.4 Investigating the causes

Studies exploring the incident management process have frequently applied the ISO/IEC 270035-2 (2023) and NIST Special Publication 800-61 Revision 2 (2012) standards. These standards include lessons learned as a critical step, thus broadening the scope of studies that incorporate learning into their research. However, while these standards advocate for learning, they fall short of explaining how to effectively extract lessons and, crucially, how to utilise them to reduce the likelihood and impact of future incidents (Ahmad et al., 2020). The standards seem to assume that organisations can identify valuable lessons without providing guidance on the optimal approach to elicit them, as if the lessons are simply waiting to be collected and reported. In reality, lessons are co-created by those conducting the investigation (Lundberg et al., 2009, 2010).

To study how lessons are identified, researchers have borrowed models from psychology, management science, and safety science, all of which incorporate organisational learning principles such as double-loop learning (Ahmad et al., 2012, 2015, 2020; Jaatun et al., 2009; Line et al., 2006; Shedden et al., 2010; Ebert et al. 2023). Some researchers reformat the findings from existing incident reports to present them in a new way to illustrate the cause (He et al., 2015; He, Johnson, Lu, et al., 2014; He, Johnson, Renaud, et al., 2014; He & Johnson, 2015). In the field of cyber security research, there is little discussion on the organisational politics and other barriers to effective learning, which have been more extensively studied by safety researchers (Drupsteen & Hasle, 2014; Murphy et al., 2018; Schilling

& Kluge, 2009; Zwetsloot et al., 2017). Grispos et al. (2017) found that retrospectives helped identify underlying causes but, despite this additional information, the organisation in the case study had not employed it to improve security. Further research is needed to understand what hinders better learning.

There is broad consensus among researchers that addressing underlying causes is essential to reducing the likelihood of future incidents. Although double-loop learning is frequently mentioned in studies for its importance in tackling underlying causes, there is little evidence of its practical application. The literature indicates a recurring theme that organisations are not sufficiently investigating underlying causes. Despite researchers' recommendations for double-loop learning models adapted for cyber security incidents, most of these models have not been empirically validated in organisations to test their effectiveness in identifying underlying causes. He et al. (2015) and He & Johnson (2015) evaluated the use of the Goal Structuring Notation (GSN) approach to represent causes in a healthcare provider, but these diagrams were based on causes already identified by the organisation, highlighting the need for further empirical research.

Many studies acknowledge the potential value in learning from incidents to address underlying issues, which could enhance the overall security of the organisation. However, given that the most extensive coverage of the learning process was in the causal analysis phase, Ahmad et al. (2020) stated “there has been little recognition of the potential role of incident response as a tool for learning and feedback for wider organisational objectives in particular security management.” This highlights a gap in recognising and leveraging incident response processes as a mechanism for broader organisational learning and improvement.

2.2.5.5 Organisation structure and culture

Ahmad et al. (2020) suggested that integrating incident response and security management teams could enhance learning opportunities. However, this may not be a universal solution, as the optimal team structure can vary significantly across different organisations, depending on numerous factors. The interpretation of organisational structures by employees and the relationships between their leaders, teams, and other stakeholders can have a more profound impact than the official structure alone (Schein, 2017). More research is needed to better understand the optimal organisational governance structures that facilitate decision-making and accountability for improvements based on lessons learned.

Much of the existing research has focused on the technical aspects of incident management rather than on learning processes (Ahmad et al., 2012; Shedden et al., 2010). The research to date has not sufficiently identified the organisational conditions that promote effective learning, such as a culture that values reflection and experimentation (Schein, 2017). Although there have been numerous studies on cyber security culture (Uchendu et al., 2021), these have not specifically addressed how organisational culture impacts the ability to learn from incidents. Structured observation and analysis of learning process artefacts could provide valuable insights into how an organisation’s behavioural norms shape their approach to learning from incidents. Understanding these norms and behaviours is crucial for developing effective strategies that foster a learning-oriented culture within organisations.

2.3 Research from other domains on organisational learning from incidents

To supplement the structured approach of reviewing existing research on learning from cyber security incidents, the search was broadened to include adjacent fields, particularly focusing on learning from other types of incidents, such as safety incidents. Initially, the scope was expanded to encompass learning from any IT incident, not just those related to cyber security. This process followed established

approaches for synthesising relevant literature (Torraco, 2016; Webster & Watson, 2002), ensuring a comprehensive review of how organisations learn from incidents beyond cyber security.

2.3.1 IT incident organisational learning research

The Information Technology Infrastructure Library (ITIL) is the most widely used framework for IT service management (Saarelainen & Jäntti, 2015). Originally established by the UK government, ITIL sets out the IT organisation structure and required skills within standard operational management procedures and practices. ITIL 4, the latest version, includes the ITIL 4 Incident Management Process, which outlines the management of all IT incidents, not specifically those related to cyber security. It covers the monitoring, discovery, reporting, handling, and resolution of incidents but does not explicitly address how organisations can learn from security incidents. The overall ethos of ITIL includes the "Continual Improvement Model" (*ITIL 4 Continual Improvement Model & VUCA | Axelos*, n.d.) which focuses on defining metrics and driving actions to improve them. While it can be applied to specific cyber security processes and measures, it does not cover how to enable an organisation to learn from cyber security incidents.

Although some studies have examined how organisations learn from IT incidents, research on this topic remains sparse (Mehrizi et al., 2022; Sillito & Pope, 2024). However, studies to date have not focused on the learning processes within organisations. Those that have considered learning processes often draw on safety research, such as the work by (Saarelainen & Jäntti, 2015), who utilised the Human Factor Analysis and Classification System (HFACS) developed by Shappell and Wiegmann (2000). Consequently, this literature review concentrated on extracting insights from research into learning from safety incidents, as these findings have the potential to provide valuable perspectives for improving learning from cyber security incidents.

2.3.2 Safety incident organisational learning research

An overview of the evolution of safety research into organisational learning from incidents highlights the maturity of the field and offers the latest recommendations for organisations on improving their learning from safety incidents. There are many parallels between the safety and cyber security domains, as both aim to reduce the risk of harmful incidents. These similarities have been recognised by several authors (Cockram & Lautieri, 2007; Ebert et al., 2023; Kaur et al., 2021; Kriaa et al., 2015; Lisova et al., 2019). Achieving absolute safety or security is impossible; both require continuous efforts. In some languages—namely German, Portuguese, and Spanish—the same word is used to denote both incidents and accidents (Kriaa et al., 2015).

Jore (2019) suggested that the distinction between security and safety lies in the intentionality of the attacker yet acknowledges the many commonalities between the two. Jore (2019) also noted the scarcity of studies testing the effectiveness of safety theories in a security context. Similarly, Herrmann & Pridöhl (2020) viewed security as aligned with deliberate acts and safety as primarily concerned with accidental events. Although the consequences of failure in each domain differ, the increasing dependency on IT for critical infrastructure, including healthcare, means that a security breach could potentially impact safety (Drupsteen & Guldenmund, 2014; Pietre-Cambacedes & Bouissou, 2013). The aviation industry, for instance, has considered security and safety in combination (Cockram & Lautieri, 2007). In the field of safety, there is a more prevalent use of statistics to quantify risks compared to the security field (Amundrud et al., 2017). This may reflect the relative maturity of the two disciplines and, as mentioned, the challenges of quantifying cyber security incidents.

As the cyber security field continues to develop, it can benefit from the established practices and insights from safety research to enhance organisational learning processes. The process of learning has been defined by safety researchers Drupsteen, Groeneweg, et al. (2013) and Littlejohn et al. (2017). Drupsteen et al. (2013) provided detailed insights into the investigating and implementing

steps, as well as covering an evaluation step to assess the effectiveness of implementing the lessons learned, which is crucial for enhancing learning (Argyris & Schön, 1978). Littlejohn et al. (2017) incorporated input from other sites and companies and begin the process with a reporting step, highlighting that organisations cannot learn if they are unaware of incidents. This helps to create a learning culture that encourages reporting and therefore drives improvements (Senge, 2010).

These process steps could be equally applicable to learning from cyber security incidents. They offer more detail than the generic phases found in the cyber security standards analysed earlier in Section 2.1. By adopting these detailed steps, organisations can better structure their learning processes to address security incidents, fostering a more comprehensive approach to incident management and organisational learning, going beyond the generic phases in cyber security standards analysed above.
The field of safety research, with its focus on socio-technical and human factors, has a long history of exploring ways to reduce the number and impact of incidents (Le Coze, 2013a; Line & Albrechtsen, 2016). This field recognises that explaining the cause of incidents is “an act of social constructivism” (Ebert et al., 2023). Notably, the journals *Safety Science* and the *Journal of Contingencies and Crisis Management* published special issues explicitly on the topic of learning from incidents in 2011 and 2009 respectively (Drupsteen & Guldenmund, 2014). Learning from incidents in the aviation industry has inspired similar approaches in the rail and medical sectors (Sanne, 2008). There is an opportunity to accelerate the understanding of human factor causes in information security incidents and improve organisational resilience by leveraging safety research and applying these concepts to information security (Kaur et al., 2021).

Evans et al. (2019) recognised the value of applying techniques developed in the safety field to understand human reliability causes of safety incidents and adapting them to security incidents. Similarly, Kaur et al. (2021), Murphy et al. (2021), and Brostoff & Sasse (2001) have commented that cyber security can benefit from safety science research, particularly in addressing human causes of incidents.

A guiding principle in safety research is to understand the causes of incidents to address them and reduce future occurrences (Lundberg et al., 2010). However, public examples of organisations failing to learn from incidents highlight the challenges of applying this principle in practice. Notable cases include the BP Texas City refinery explosion (2005), the Deepwater Horizon oil spill (2010), and NASA's Challenger (1986) and Columbia (2003) shuttle disasters. Such examples have prompted researchers to investigate barriers to learning and how organisations can improve their learning processes.

While prominent organisations are constantly targeted by attackers, there have not yet been repeated large-scale, publicly visible incidents in cyber security of the same nature as those in the safety field. This could indicate that organisations are learning, or it may be that large-scale cyber security incidents have only recently become more frequent. Over time, it may become apparent that some organisations have not learned from previous incidents. An industry report based on a self-reporting survey of security professionals by Cybereason (2022) found that 80% of those who paid a ransom experienced another attack, highlighting the need for more effective learning from incidents.

2.3.2.1 Historical evolution of safety research and its relevance to cyber security

Safety research began in response to the need for companies to compensate workers for injuries at work, with the first scheme established in Germany in 1884. A pivotal development came with Heinrich's "Industrial Accident Prevention: A Scientific Approach" in 1931. Heinrich, working at an insurance company, sought to help managers mitigate the risk of worker injuries and associated compensation costs. He was the first to connect human errors in one part of a process to accidents elsewhere, using the analogy of a row of dominoes to illustrate linear cause and effect. Root causes were identified as deviations from expected procedures, reflecting the industrial and engineering

mindset of the time. This approach continued post-World War II, leading to the creation of professional bodies such as the Human Factors and Ergonomics Society.[5]

Building on Heinrich's domino analogy, Reason introduced the "Swiss Cheese" model of causation in his seminal 1990 work *Human Error*. This model depicted how latent failures across different organisational layers could align to enable an incident due to an unsafe act. This shifted the perspective from blaming human error to understanding errors as symptoms of broader organisational issues. This led to the development of the Human Factors Analysis and Classification System (HFACS) by Shappell and Wiegmann (2000), which has been instrumental in understanding human causes of accidents. Leveson et al. (2012) extended the HFACS with the Systems-Theoretic Accident Model and Processes (STAMP) approach, explaining how failures propagate across both higher and lower organisational levels. STAMP adopts a systems-engineering perspective, focusing on control failures as causes of accidents. Some studies have adopted STAMP in cyber security to identify vulnerabilities (S. Khan et al., 2022).

Critics of Reason's "Swiss Cheese" model and its derivatives argue that it provides a snapshot of the time of the accident without explaining how organisations develop vulnerabilities and allow the gaps in the barriers to align (Dekker, 2019). This criticism mirrors early cyber security research, which often viewed security as a chain with humans as the weakest link and attempting to address this through detailed policies and user training to make humans a more reliable component in the system.

Understanding the historical evolution of safety research and its methodologies can provide valuable insights for the cyber security domain. By leveraging the established practices and frameworks from safety research, cyber security can enhance its own approaches to organisational learning, incident analysis, and the identification and mitigation of vulnerabilities.

The Three Mile Island nuclear accident in 1979 boosted funding and introduced new disciplines into the research area of safety. This shift allowed for new perspectives, moving away from the reductionist faulty barrier model towards a more dynamic and constructionist approach. Vicente and Rasmussen (1990) suggested that errors are defined by their outcomes, with individuals in the system making decisions based on economic, time, and resource constraints. Their choices, made at the time, were influenced by their understanding of the current situation, prior experiences, and mental models of similar circumstances. This process explains how organisations drift into failure, as described by Dekker (2016), with people often unaware of this drift until the boundary is crossed, a phenomenon Vaughan (2016) terms the "normalization of risk" caused by "macrostructural forces".

In the realm of cyber security, simple incidents may stem from a single root cause, but more complex incidents typically involve multiple underlying causes. This complexity was highlighted in PwC's review of the Irish Health Executive incident (PwC, 2021). Each organisation exhibits a range of adaptive behaviours that respond to a changing environment and maintain safety through what Woods (2018) calls "graceful extensibility". However, in competitive industries, the drive for efficiency can reduce this adaptive capability, creating brittle boundaries that, when crossed, result in incidents.

Perrow's (1984) book introduced the Normal Accident Theory (NAT), which assumes that accidents are normal and predictable within complex and tightly coupled systems that can fail in catastrophic ways beyond the imagination of the people within them. Incidents often have a long incubation period,

[5] Created in 1957 in the US, the Human Factors and Ergonomics Society provides education and fosters collaboration across the profession. https://www.hfes.org/about-hfes The UK Chartered Institute of Ergonomics and Human Factors (CIEHF) created in 1949, as the Ergonomics Research Society (later to become the Ergonomics Society and then achieved Chartered status in 2015). https://ergonomics.org.uk/about-us/our-story.html

shaped by commitments and narratives assigned to risks, leading to distributed risk acceptance and culpability (Vaughan, 2016). In contrast, La Porte (1996) studied High Reliability Organisations (HROs) to identify what practices contribute to building safety, rather than focusing on accidents as Perrow did, based on the nature of the organisation (Hollnagel et al., 2006). There has been limited research in the cyber security domain on what the equivalent of HROs are doing well to avoid incidents. Understanding these historical and theoretical perspectives from safety research can provide valuable insights for cyber security. By examining the adaptive behaviours and resilience strategies of HROs, cyber security professionals can develop more robust frameworks to prevent and manage incidents, enhancing organisational resilience and safety.

2.3.2.2 Investigating the causes of safety incidents

Safety researchers have extensively studied how the causes of incidents are investigated post-incident to understand their underlying causes (Jacobsson et al., 2012; Littlejohn et al., 2010). They found a lack of empirical evidence on the effects of different incident investigation methods and their success in preventing future incidents. Catino (2008) analysed the logic behind adopting either an individual accountability or organisational accountability approach when investigating incidents. The study concluded that organisational accountability leads to improvements, whereas blaming individuals does not eliminate risk-creating conditions. Lindberg et al. (2010) and Sanne (2008) explored why incidents are not reported, discovering that an organisation's response significantly influences whether employees are motivated to report. Employees often refrain from reporting incidents if they feel ashamed to admit mistakes or believe no changes will result from their reports. Hewitt and Chreim (2015) found that people did not report incidents they viewed as one-offs with a fix already in place or as chronic issues seen as part of their normal work life. There have not yet been the equivalent studies into employees' motivations to report cyber security incidents.

Schilling and Kluge (2009) explored barriers to learning through the organisational learning lens of the 4I framework (intuition, interpretation, influence, and institutionalisation). Ahmad et al. (2015) also used the 4I framework, although they did not incorporate Schilling and Kluge's (2009) findings on barriers in their application to cyber security. Murphy et al. (2021) used the 3-P model of workplace learning, which includes learner factors and context, learning process, and learning product, finding that different types of learning at formal and informal, organisational, and individual levels are interconnected.

Researchers such as Drupsteen & Guldenmund (2014) have studied how lessons learned are shared and implemented. They identified several conditions for effective learning, including organisational trust, willingness to learn and implement changes, the impact of the incident (with higher impact incidents being more likely to result in learning), and having a process for learning and storing lessons. Margaryan et al. (2017) recognised that learning does not occur simply because people are sent information on lessons; it requires two-way communication, deliberate practice, guided reflection, feedback, and observing and emulating others. Such studies have yet to be replicated in the cyber security domain.

Drupsteen & Guldenmund (2014) used organisational learning as a framework to analyse safety research on learning from incidents, whereas Le Coze (2013) adopted a multidisciplinary angle in his literature review. Wienen et al. (2017) conducted a systematic literature review of the methods and models used to understand the causes of accidents, identifying 63 types, most of which had only been mentioned in one or two papers. This suggests that many authors were not well-informed about previous research and had reinvented their approaches. They concluded that no single method or model had been widely adopted. Despite safety research being relatively mature compared to cyber security research on learning from incidents, safety science itself is relatively new and has yet to develop a unifying theory (Swuste et al., 2020). Drupsteen and Guldenmund (2014) noted that,

although there are many theoretical papers on the topic, there is limited empirical research on how organisations practise learning from incidents.

Different incident and accident models have been proposed for incidents in different domains, such as Driver Reliability and Error Analysis Method (DREAM) for road traffic and the Australian Transport Safety Bureau (ATSB) for railroad infrastructure. Many methods have little published evidence of being used more than once or twice. A few methods, like STAMP (Leveson, 2011) and AcciMap (Rasmussen, 1997), are cited frequently, and some techniques, such as fault tree analysis, are widely used in practice (Wienen et al., 2017). More research is needed to address the challenges of fully learning from safety incidents. Margaryan et al. (2017) highlighted key research gaps, including the need for a multi-level definition of learning from incidents, understanding cross-sectoral factors impacting learning across individuals, teams, organisations, and industries, fostering more collaborative research with a broader range of disciplines, and improving engagement with industry to develop practical guidance for practitioners.

2.3.3 Applicability of safety research to cyber security

Exploring the commonalities and distinctions between safety research and cyber security incidents reveals significant potential for transferring insights from safety science to the field of cyber security. Safety science, with its 30-40 years of experience investigating the challenges of learning from incidents, is more advanced than cyber security (Swuste et al., 2020). Kaur et al. (2021) highlighted an opportunity for cyber security to learn from safety research, particularly regarding human factors.

As industrial processes increasingly rely on IT, cyber security researchers can build on safety literature and evaluate models and approaches suited to the specific nuances of security incidents. Process models of learning from incidents defined in safety research, such as those by Drupsteen, Groeneweg, et al. (2013), Littlejohn et al. (2017) and Sveen et al. (2007), could be adapted for cyber security. The in-depth examination of incident causes in safety research can also be applied to cyber security, where few organisations engage in double-loop learning (Ahmad et al., 2012; Jaatun et al., 2009; Line & Albrechtsen, 2016).

Additionally, safety researchers have addressed the reluctance of organisations to adopt lessons learned from incidents (Drupsteen, 2014; Lundberg et al., 2010; Vaughan, 2016). However, no study has specifically examined the organisational barriers to learning from security incidents. High Reliability Organisation (HRO) researchers, such as La Porte (1996), have analysed attributes of high-risk organisations that successfully avoid incidents. Understanding why some organisations can minimise security incidents despite significant risks remains relatively unexplored. This presents an opportunity to build on the work of safety researchers in the context of cyber security.

By leveraging safety research insights, cyber security can develop more effective frameworks for understanding and mitigating incident causes. This includes adopting process models for learning from incidents, addressing human factors, and overcoming organisational barriers to implementing lessons learned. The cross-disciplinary application of safety research principles to cyber security could significantly enhance the ability for organisations to learn from incidents.

2.3.4 Summarising the research into organisational learning from incidents from other domains

Safety research has its origins in the need to address worker injuries and compensation, significantly evolving since Heinrich's foundational work in 1931. Heinrich's "domino theory" and Reason's subsequent "Swiss Cheese" model have been instrumental in shaping the understanding of how errors and latent failures align to cause incidents. These models reflect a shift from a linear cause-and-effect perspective to a more comprehensive view that considers systemic factors. The Human Factors Analysis and Classification System (HFACS) and Systems-Theoretic Accident Model and Processes

(STAMP) have provided robust frameworks for understanding human and systemic factors in safety incidents. Notably, these models have been adopted in some cyber security studies (S. Khan et al., 2022; Pollock, 2017; Saarelainen & Jäntti, 2015), indicating their potential applicability to the cyber security domain.

Safety research has progressively shifted from attributing incidents to individual errors towards understanding the organisational and systemic contexts that enabled the incident to occur. This shift assumes errors are often symptoms of deeper organisational issues. This perspective can significantly enrich the analysis of cyber security incidents by encouraging a more holistic approach to understanding and addressing root causes. Process models for learning from incidents, developed in safety research, such as those by Drupsteen et al. (2013) and Littlejohn et al. (2017), emphasised the importance of comprehensive reporting, investigation, implementation, and evaluation. These models could be adapted to enhance the learning processes following cyber security incidents.

Rasmussen's (1997) mapping of the layers of causation that lead to an incident further refines this understanding by illustrating how decisions and actions at various levels within an organisation contribute to incidents. His framework highlighted the interactions between different organisational layers, from policy and planning down to operations and technical activities. This multi-layered approach provides a nuanced view of how systemic failures propagate, offering valuable insights for cyber security researchers and practitioners aiming to prevent similar failures.

Double-loop learning (Argyris & Schön, 1978), which involves revisiting and revising underlying policies and objectives, is widely advocated in safety research but is less commonly practised in cyber security. Encouraging this deeper level of learning can help organisations address root causes and prevent future incidents. Studies in the safety domain also highlighted significant barriers to reporting and learning from incidents. Factors such as organisational response, employee shame, and the belief that reporting will not lead to change are crucial in determining whether incidents are reported. Understanding these barriers within the context of cyber security can improve incident reporting and learning practices.

Research supports the view that organisational accountability, as opposed to individual blame, leads to more substantial improvements in safety. Applying this approach to cyber security can foster a culture where systemic issues are addressed rather than focusing on individual errors. Additionally, High Reliability Organisation (HRO) research identifies attributes of organisations that successfully avoid incidents despite high risks. These insights can be applied to identify practices that improve cyber security resilience. However, more research is needed to understand why some organisations are better at minimising security incidents despite significant risks.

In integrating safety research principles, such as adaptive behaviours and resilience strategies, cyber security can enhance its frameworks for incident analysis, reporting, learning, and prevention. Collaboration across disciplines and better engagement with industry can foster the development of practical guidance and robust frameworks for learning from cyber security incidents. This cross-disciplinary approach could significantly enhance the resilience and security posture of organisations in the face of evolving cyber threats.

2.4 Chapter conclusion

In conclusion, this literature review has summarised key findings and identified significant gaps in the existing cyber security literature on organisational learning from incidents. Security incidents pose a substantial threat to society due to the vast amount of data and the complex web of interconnected systems and suppliers which heighten our vulnerability. The variety of incident types and the challenges in quantifying them are compounded by the absence of a universal taxonomy (Ibrishimova,

2018). Additionally, statistics on the number of incidents are often published by companies with an interest in marketing their security tools, further complicating the accuracy of these figures.

While current standards recommend learning from incidents, they often lack detailed guidance on how to effectively do so. Despite the critical importance of this topic, there has been relatively little research in the field of cyber security on organisational learning from incidents. By structuring the existing body of research, this review aims to propel the field forward by offering a foundational resource for other researchers to build upon. This work also emphasises the necessity of adopting insights from other domains, such as safety research, to enrich the understanding and practices of organisational learning in cyber security.

The literature currently places more emphasis on acquiring knowledge through post-incident investigations, with less attention given to the implementation of lessons learned. There has been no consistent model applied to assess how organisations learn from incidents. Existing studies recommend that organisations should improve their learning from incidents through wider participation and sharing of post-incident reports, often suggesting the use of double-loop learning in investigations to address systemic causes. The existing research indicates that organisations are not yet fully benefiting from learning from incidents and are not adequately evaluating the effectiveness of their learning processes.

The analysis of the literature has highlighted the need for further studies to explore the barriers that prevent organisations from understanding underlying causes, identifying necessary improvements, and implementing these improvements to reduce the risk of future incidents. Additionally, researching High Reliability Organisations (HROs) that excel in learning from incidents would provide valuable insights.

Identifying valuable lessons within an organisation's social and political environment requires significant effort. Ensuring that these lessons lead to meaningful changes that prevent future incidents requires evaluating how well organisations are learning. The existing literature does not determine how organisations can invest in learning to achieve the greatest benefits. By improving how organisations learn from incidents, it is hoped that they can reduce the likelihood and impact of future cyber security incidents, thereby mitigating the risks society faces due to its dependence on IT. This will help to enhance organisational resilience and contribute to a more secure digital environment. This literature review makes a contribution to the knowledge and established ideas on the topic of how organisations learn from cyber security incidents.

3 Methodology

This chapter sets out the research philosophy that underpins the approach taken in this study and the theoretical frameworks used. It describes the selection of research methods specifically chosen to address the research questions posed in Chapter 1, Section 1.5. It justifies the choices made and explains why these methods are appropriate for answering the research questions. Details on the practical application of these methods, including data collection and analysis, will be provided in subsequent chapters. Finally, the chapter addresses the limitations and ethical considerations associated with the research approach.

3.1 Research philosophy and approach

This section explains the philosophical underpinnings of the research, articulating the ontological stance—convictions regarding the nature of reality—and the epistemological approach concerning the acquisition and comprehension of knowledge. Sarker et al. (2018) emphasised the necessity for Information System studies to harmonise their methods of data collection, interpretation, and conclusion formulation with their theoretical underpinnings. Alvesson (2003) championed epistemological awareness, advocating for a mindful approach to selecting research methods, predicated on an understanding of the chosen epistemological position. With these ontological and epistemological foundations clarified, the research design can subsequently be detailed.

Although most of the existing research on learning from incidents has not stated its ontological perspective, there is typically an implicit positivist stance, which assumes that incidents are a specific observable phenomenon. Such perspectives overlook the social processes used to classify events as an incident and assume the existence of an objective *true cause* with definitive *lessons to be learned.* In contrast, this research adopts a social constructivist ontological stance recognising the subjective nature of attributing causes and selecting lessons. Assuming the existence of *multiple socially constructed realities,* Stahl et al. (2012) posited that organisational practices do not exist independently of people. What is defined as an incident, or a lesson to be learned from it, depends on the social structure of an organisation and the people who work there, who are both influenced by and are at the same time creating this reality. Epistemologically this research seeks not just to understand but to improve how organisations learn from incidents. Therefore, the study adopts a pragmatist approach, specifically chosen for its focus on improving how organisations practically implement learning from incidents.

3.1.1 Pragmatic research

This section outlines the adoption of a pragmatic research approach, rooted in the tradition of pragmatism that emerged in the late 19th and early 20th centuries (Kelly & Cordeiro, 2020). Pioneered by Charles Sanders Peirce and further developed by William James and John Dewey, pragmatism emphasises the practical application of ideas through real-world testing and experience (Kelly & Cordeiro, 2020). Dewey's contributions were especially significant, advocating for knowledge that goes beyond understanding the world to actively improving it. This aligns with the intent of the current research, which aims to enhance organisational cyber security through effective learning from incidents.

In the latter part of the 20th century, the pragmatic approach evolved as a distinct methodological stance, particularly in response to the constraints of both positivist and constructivist paradigms (Onwuegbuzie & Leech, 2003). These traditional approaches often proved inadequate for complex, real-world issues that did not conform strictly to quantitative or qualitative methodologies. Consequently, the pragmatic approach champions methodological pluralism, encouraging the use of diverse research methods best suited to specific research questions. Recent cyber security studies

(Mukhopadhyay & Jain, 2024; Tejay & Mohammed, 2023) have adopted a mixed methods approach to enable the answering of both exploratory and confirmatory questions.

This research adopts a pragmatic stance, balancing between the positivist and constructivist frameworks. It aims to comprehend how organisations learn from incidents, while acknowledging that individual experiences are shaped by the broader context of their organisation and industry. As Nicolini (2012) explained, using a mixed methods approach helps researchers practice good social science to provide richer and more nuanced understanding of the world. This perspective enables a more flexible and practical approach to research, especially valuable in fields where the objective is to generate knowledge with direct practical applications. Venkatesh et al. (2016) suggested such methods enable researchers to gain stronger insights due to combining both qualitative and quantitative inferences.

This thesis investigates how organisations learn and why they are successful or unsuccessful in improving security based on lessons from incidents. Pragmatism as a research approach is driven by the research questions; it is problem-centred, pluralistic, and oriented toward what works in practice. This research goes beyond interpreting the practices purely to enhance the understanding of them and makes recommendations to improve them.

Pragmatist researchers use a mix of methods which are best suited to answer their research questions. Consequently, this study adopts an exploratory sequential approach. Cresswell and Cresswell (2023) suggest that qualitative research is particularly effective for areas which have not been studied extensively or at least when it is unclear which variables to test. Additionally, Paulus and Lester (2021) stated that qualitative methods are valuable in understanding complex phenomena. This is because they offer in-depth insights into participants' perspectives and contextually rich understanding of interacting factors in real-life settings (Cresswell, 2008). This makes qualitative methods apt for investigating processes like learning from incidents (Lund, 2014).

As highlighted in Section 1.2, incidents are challenging to quantify accurately. Quantitative methods, while useful in evaluating recommendations, may not be feasible for counting incidents due to their sensitive nature and the challenge of obtaining adequate sample sizes. Furthermore, quantitative research might not fully capture the nuances of current practices and their underlying rationales. As pragmatist researchers blend methods to address their research questions this study uses qualitative methods for detailed understanding, complemented by quantitative measures for validating recommendations.

Elliott et al. (1999) offered guidelines for evaluating qualitative research, encompassing reflexivity, systematic inquiry, validation of interpretations, and coherence. These guidelines informed this research design, though Elliott et al. (1999) cautioned against treating them as a mere checklist, given the absence of a consensus standard for assessing qualitative research quality. Transparency in ontological and epistemological choices and research design decisions is crucial (Willig, 2022). This thesis thoroughly documents these decisions and choices to maintain the recommended transparency.

3.2 Theoretical frameworks

In contrast to quantitative research, which uses theory to explain the area of interest, qualitative researchers use general theories to both shape and interpret findings (Glesne, 2016). This research, adopting a pragmatist approach, applies theories to effectively answer its research questions. This section will detail how two theories have been employed: both to inform data collection and to assist in analysing the data. The first, organisational learning theory, provides insights on internal pressures, while the second, neo-institutional theory, is used to examine external pressures. The integration of these theories provides a more comprehensive understanding of learning practices, and the challenges

organisations face in this area. These discipline-based theories are key in shaping the expected outcomes for organisations.

3.2.1 Organisational learning theory and its application in cyber security research

Organisational learning from cyber security incidents is influenced by a range of factors including IT processes, standards, regulatory requirements, military and safety procedures, organisational culture, and established norms. Despite the extensive research on organisational learning, there remains no universally accepted theory or definition of it (Argote, 2013; Crossan et al., 1999; Easterby-Smith & Lyles, 2012; Fiol & Lyles, 1985; Huber, 1991). Argote and Ophir (2017) described organisational learning as a process shaped by experiences. Fiol and Lyles (1985) viewed organisational learning as acquiring knowledge from experiences and translating that knowledge into actions taken by an organisation. The research approach was designed to understand the practices organisations use to derive lessons from incidents and the subsequent changes they implement.

The concept of organisational learning was first introduced by Cyert and March, (1963). Argyris and Schön (1978) further developed this concept, introducing the key idea of single and double-loop learning. Learning is initiated by either aligned outcomes with planned expectations (a 'match') or unplanned outcomes (a 'mismatch'), as occurs in incidents (see **Figure 5**). Single-loop learning involves straightforward adjustments, such as adding an unmonitored server to the Security Operations Centre's monitoring scope. In contrast, double-loop learning examines deeper aspects like processes, organisational structures, and decision-making that led to the server's initial exclusion. Argyris (1976) noted that as "problems become increasingly complex and ill-structured, the need for learning increases, but so does the difficulty in carrying out effective learning" (p. 365), a statement relevant to today's cyber security challenges. Argyris found that organisations often promote learning that does not challenge their fundamental design or goals—a characteristic of single-loop learning. Double-loop learning, in contrast, involves understanding the immediate variables leading to an incident and delving deeper to identify contributing or enabling factors.

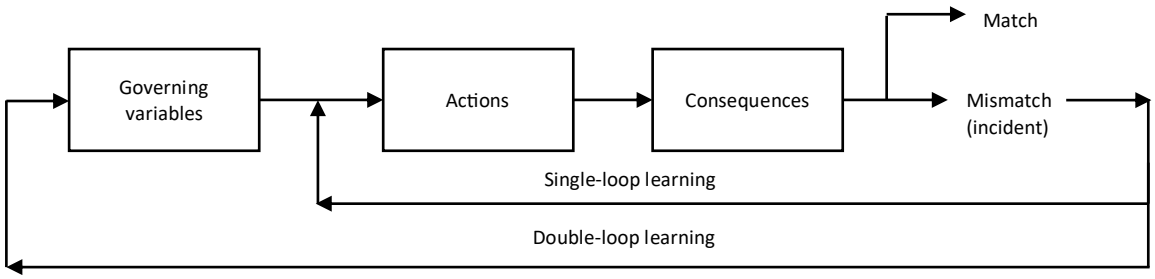
Cyber security researchers, including Ahmad et al. (2012, 2020) and Shedden et al. (2010, 2011), have applied double-loop learning models to study organisational learning from incidents. The application of the double-loop model in incident learning is demonstrated in Ahmad et al.'s (2012) cyber security incidents study, which builds on a model from safety incidents (Cooke, 2003) and Cooke's model had been inspired by Argyris's double-loop model (Argyris, 1976). Ahmad et al. (2015) further explored this theme using the 4I Organizational Learning framework, which draws on the management science work by Zietsma et al. (2002) and incorporated double-loop learning principles. This model has layers encompassing stakeholders, learning processes, and activities, aiming to embed learning within an organisation. Ahmad et al. (2020) emphasised double-loop learning's importance, comparing single-loop learning to fixing holes in a shield and double-loop learning to altering the shield's shape and thickness. While cyber security researchers Ahmad et al. (2012, 2020) and Shedden et al. (2010, 2011) recommended double-loop learning models, these models provide limited practical guidance for practitioners on fostering this type of learning within organisations.

Early research by Niekerk and von Solms (2004) introduced the concept of double-loop learning in the context of cyber security, highlighting the need for further investigation. Subsequently, Shedden et al. (2010) provided a review of organisational learning literature that emphasises the application of double-loop learning principles to strengthen incident response and overall organisational cyber security. Double-loop learning involves a deeper exploration into the factors contributing to an incident, going beyond mere identification of immediate causes. For instance, in the energy sector, Incident Response Management methods incorporate safety processes based on double-loop learning concepts as initially proposed by Argyris (1976). Studies by Jaatun et al. (2008; 2007) and Line et al. (2006) delved into the complete incident management process, pointing out the cultural hesitance in

reporting incidents and the importance of the learning phase in incident management (Jaatun et al., 2009). Bartnes et al. (2016) further underscored the importance of applying double-loop learning in the analysis of incidents, including minor ones.

However, while prior studies have used organisational learning theories to analyse incident causes, there has been limited focus on how data is collected during the reviews of incidents, the implementation of the lessons identified, and their impact on reducing future incidents. This gap in the literature highlights an opportunity for organisations to refine their incident learning processes. In addressing this gap, this study applies organisational learning theory to critically examine whether the practices organisations use to learn from incidents effectively contribute to improving their cyber security posture.

Figure 5 *Single-loop and double-loop learning adapted from (Argyris, 1990)*

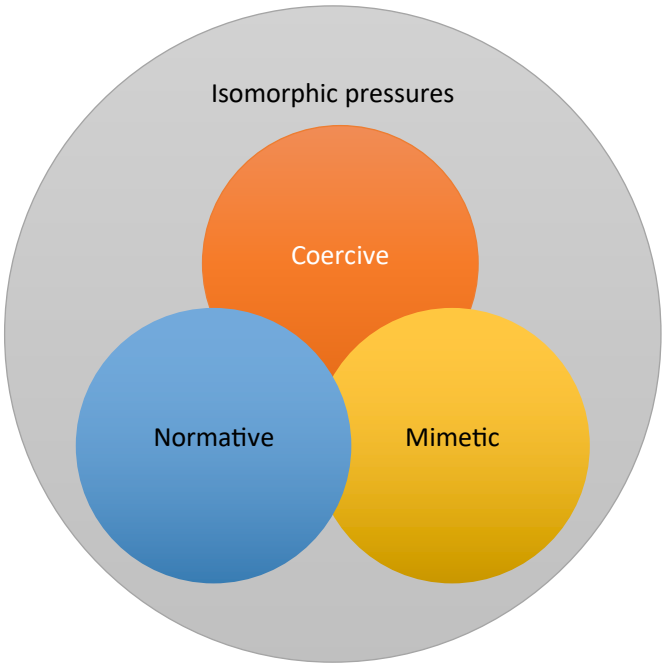


3.2.2 Neo-institutional theory and its application in cyber security research

This section introduces neo-institutional theory and positions it within broader institutional research, providing a summary of cyber security studies that have employed this theory and explaining its relevance to this study. Neo-institutional theory, often applied in information systems research, interprets organisational practices in the context of external pressures (Cavusoglu et al., 2015). Chosen for its explanatory power regarding the evolution of organisational practices (Hasan et al., 2021; Hu et al., 2007), neo-institutional theory is a prevalent framework in organisational studies (Alvesson & Spicer, 2019).

The model proposed by Dimaggio and Powell (1983) provides a valuable lens for examining the external forces that shape how organisations behave. It focuses particularly on isomorphic pressures, which refer to the social, professional, and institutional forces that cause organisations to become more alike over time. These pressures can be *coercive* (resulting from laws, regulations, or formal requirements), *normative* (arising from shared professional norms, education, and industry standards), or *mimetic* (emerging when organisations copy others in response to uncertainty or perceived best practice). Together, these mechanisms can lead organisations to adopt similar practices, often to maintain legitimacy or reduce perceived risk, without critically assessing their effectiveness in specific contexts (illustrated in Figure 6). In this research, neo-institutional theory serves as the analytical framework, enabling a deeper exploration of coercive, normative, and mimetic pressures that shape organisational learning practices in cyber security.

Figure 6 *Attributes of isomorphic pressures. Adapted from* Dimaggio & Powell (1983)



3.2.2.1 Coercive pressures

Coercive pressures include regulations, laws, legal contracts, and market structures that organisations must adhere to—such as GDPR, PCI DSS, HIPAA, DORA, etc.[6] With the introduction of new regulations, organisations rapidly implement practices in order to comply. The growing significance of cyber security has led to new laws and significant investment in compliance practices (Kosseff, 2023). Ashraf et al. (2022) found recent cyber incident disclosure regulations had shaped organisations practices, while Bulgurcu and Mashatan (2024) highlighted that market structures have created an attitude of minimal sharing across players despite the dependence on suppliers. Standards and guidance stress the importance of learning from incidents to enhance cyber resilience, as discussed in Chapter 0, Section 2.1.

3.2.2.2 Normative pressures

Normative pressures stem from the professionalism in the cyber security field and the dissemination of practices by service providers, such as consultants, and the use of standard tools and templates. Organisations might, for example, adopt incident management practices from military after-action reviews (Novak et al., 2021). Cyber insurers may establish requirements regarding an organisation's expected security practices (Mott et al., 2023), and the cyber security expertise of board members can shape leadership's expectations for security practices (Gale et al., 2022).

---

[6] Referenced regulations:
GDPR: The General Data Protection Regulation (EU 2016/679) governs data protection and privacy in the EU and EEA, with provisions for data subject rights and organisational accountability.
PCI DSS: The Payment Card Industry Data Security Standard defines requirements for securing credit card transactions, ensuring customer payment data is handled securely.
HIPAA: The Health Insurance Portability and Accountability Act (1996, USA) sets national standards for protecting sensitive patient health information and mandates secure practices for healthcare providers and associated entities.
DORA: The Digital Operational Resilience Act (EU 2022) establishes requirements for financial institutions to ensure they can withstand and recover from ICT-related disruptions and incidents.

3.2.2.3 Mimetic pressures

The uncertainty of rapid technological advancements and unpredictable cyber-attacks generate mimetic pressures. Organisations often emulate practices perceived as successful in other entities to gain legitimacy for their approaches. Cross-industry groups and conferences facilitate the spread of similar practices. There is a tendency for organisations to adopt measures simply because they are employed by more mature entities, without evaluating their suitability for the specific context of the adopting organisation (Jeyaraj & Zadeh, 2020).

3.2.2.4 Application of neo-institutional theory in cyber security research

In recent years, neo-institutional theory has become increasingly relevant in studies investigating the impact of isomorphic pressures on cyber security practices. The theory offers a lens through which various aspects of cyber security are examined, revealing differing influences of coercive, normative, and mimetic pressures.

Cavusoglu et al. (2015) explored the effect of institutional pressures on organisations' adoption of cyber security measures. Their findings highlighted the significant role of coercive and normative pressures in driving organisations to improve their security capabilities, while mimetic pressures were less influential.

Vuko et al. (2021) assessed the effectiveness of internal audit assurance in managing cyber security risks, noting the impact of mimetic pressures, particularly in the context of outsourcing. Their study also found that normative and coercive pressures were more influential, with normative pressures, such as the security qualifications of internal auditors, correlating with higher cyber security audit effectiveness.

Gale et al. (2022) used neo-institutional theory to analyse directors' engagement with cyber security at the board level. The study concluded that while coercive and normative pressures were predominant, such as regulations and prior experience in cyber security, mimetic pressures, such as directors being on multiple boards, also played a role in shaping board members' engagement with cyber security.

In contrast, in an earlier survey conducted by Barton et al. (2016) they identified only mimetic influences as significant in shaping senior management's belief in the importance of information system security. However, the survey had a high number of "do-not-know" responses and it was suggested a survey may not be a suitable method for this type of research. Normative and coercive pressures were found to be less impactful. Similarly, Al-ma'aitah (2022) observed in Jordanian governmental organisations that mimetic and coercive pressures were most influential in enhancing cyber security, a finding that contrasts with Jeyaraj and Zadeh (2020). This discrepancy might stem from a potential misunderstanding of normative pressures among survey respondents in the study by Al-ma'aitah (2022).

Jeyaraj and Zadeh (2020) explored the isomorphic nature of cyber security practices, discovering that mimetic pressures significantly influenced organisations to adopt security strategies similar to those employed by market leaders. Their study highlighted the evolution of these pressures over time, noting that, while coercive pressures were more immediate, normative pressures gained prominence over time as security practices became more established.

Lastly, Hu et al. (2007) focused on the impact of institutional pressures, such as those stemming from the Sarbanes-Oxley Act of 2002 (U.S. Congress, 2002), on organisations' cyber security capabilities. Their findings suggested that coercive forces were a significant influence on organisational security

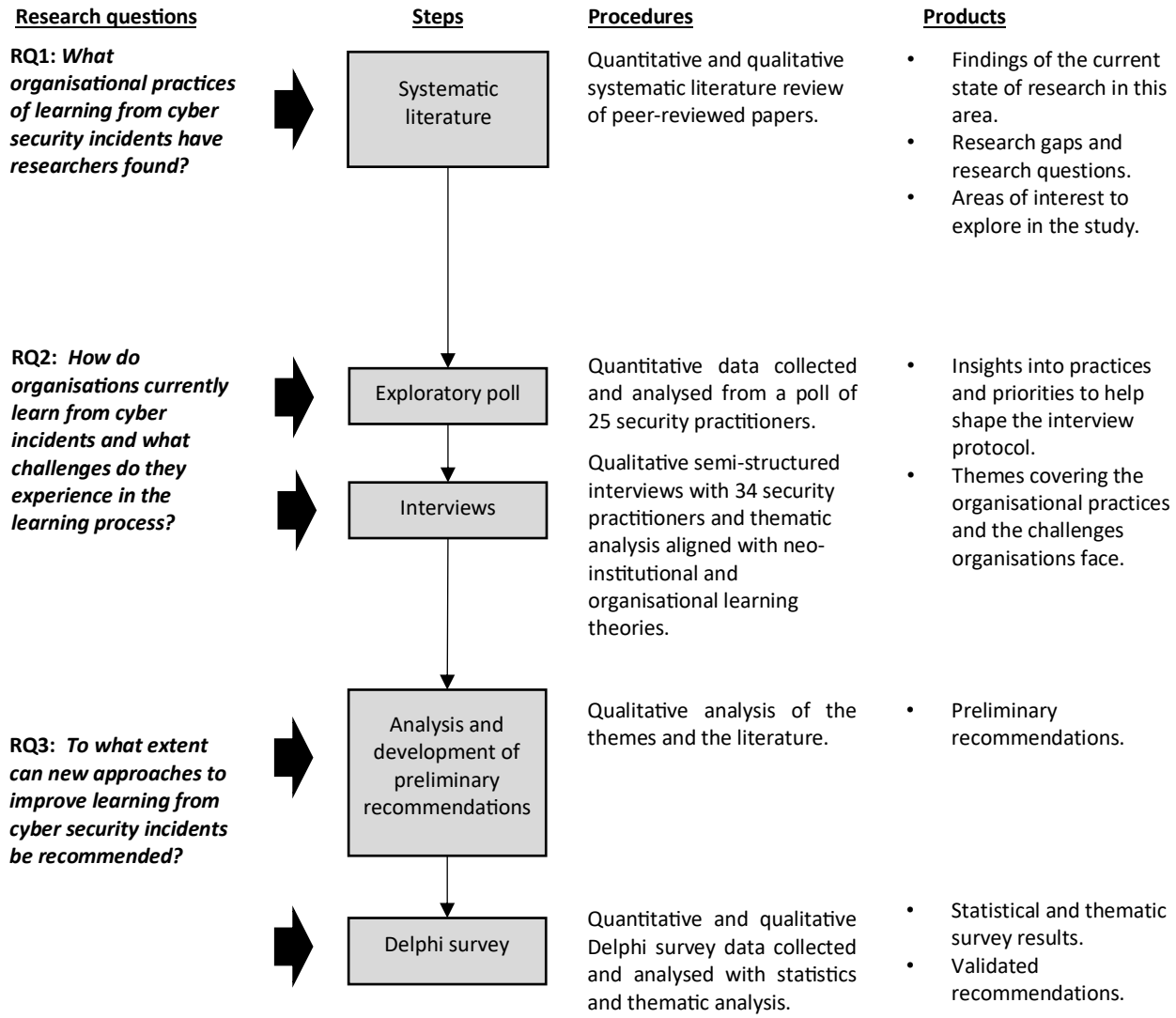
practices, though differentiating the effects of normative pressures from mimetic influences proved challenging in their specific organisational context.

The variation in these influences across these studies might be attributed to the diverse areas researched, the different organisations studied, or the varying interpretations by researchers or participants. Further research is essential to fully comprehend how each factor influences a range of cyber security aspects.

3.3 Research design

This section sets out the rationale for the selected research methods and explains how each phase of the research contributes to addressing the research questions. The methodological choices are anchored in the pragmatist research philosophy, which advocates for a blend of qualitative and quantitative methods. This mixed methods approach leverages the strengths of both methods while mitigating their respective weaknesses, thus providing a more comprehensive understanding of the research subject. Street and Ward (2019) suggested that internal validity depends on the alignment between a study's design, data collection, and analysis procedures. This strategy aims to ensure that the research process is methodical and aligns closely with the set research objectives. To provide a clear roadmap, Figure 7 presents a visual overview of the methods, data collection, and analysis techniques employed for each research question. These methodologies are detailed in the following subsections, explaining how they collectively contribute to answering the study’s research questions, set out in Chapter 1, Section 1.5.

Figure 7 *Overview of research approach*



3.3.1 Research Question 1: research methods

RQ1: What organisational practices of learning from cyber security incidents have researchers found?

To address the initial research question, a systematic literature review was undertaken, the findings of which were presented in Chapter 2. This review entailed a critical examination of industry standards, guidance documents, and academic research to assess the current scope of research concerning organisational learning from cyber security incidents. The effectiveness of the documented learning practices was appraised, incorporating insights from related fields such as safety and crisis management. Through this evaluation, gaps in the literature on organisational learning in the context of cyber security were identified. Insights drawn from the literature review were instrumental in shaping the interview protocol for the subsequent research question. It provided a foundation of the practices found from which interview questions could be formed to investigate if practices had evolved since existing research studies were conducted.

3.3.2 Research Question 2: research methods

RQ2: How do organisations currently learn from cyber security incidents and what challenges do they experience in the learning process?

To address RQ2, two investigative approaches were employed: an exploratory poll followed by in-depth interviews with cyber security practitioners. Thematic analysis was used to analyse the interviews.

3.3.2.1 Exploratory poll

Building upon the insights gained from the literature review on cyber security and related fields, an exploratory poll was conducted targeting security professionals from various sectors. This opportunity arose during the GDS Security Summit[7] in April 2022, which was held virtually due to ongoing COVID-19 precautions. The summit brought together leading security experts to engage in discussions about learning from incidents. The poll, constrained to five questions by the summit's format, aimed to unveil current practices and perceived barriers in learning from cyber security incidents. The design of the questions was informed by findings from the literature review, seeking to gather a snapshot of participants' perspectives on existing practices, challenges, and potential improvements in organisational learning from cyber security incidents.

The quantitative data gathered from this poll played a crucial role in shaping the subsequent qualitative interviews. It provided initial insights into key areas warranting deeper exploration. The responses were analysed using Microsoft Excel, employing basic descriptive statistics to interpret the scores. It is important to note that the sample size of the poll was relatively small and not designed to be representative of the broader population. Instead, the poll served as a preliminary step in the fieldwork, which was instrumental in designing the interview protocol for the more comprehensive interview phase of the study. The data from the poll helped identify specific areas of interest and concern, thereby informing the direction and focus of the subsequent qualitative research phase. Participants, occupying significant security roles in various large organisations, were briefed on their involvement and consented to participate in the research. The findings are analysed and presented in Chapter 4.

3.3.2.2 Practitioner interviews

The interview phase of this study was designed to enhance the understanding developed from the literature review and the exploratory poll, focusing on the processes and challenges associated with learning from cyber security incidents. This subsection outlines the interview methodology, which constitutes a key element of the fieldwork, and its alignment with the research questions. It discusses the participant recruitment strategy, the development of the interview protocol, the data collection process, and the methods employed for analysis.

Interviews were chosen for their effectiveness in eliciting detailed insights into participants' experiences with organisational learning from cyber security incidents. As a method, interviews are particularly suited for studying the complexities inherent in learning practices related to cyber security incidents. They create an environment that fosters trust and rapport with participants, which is essential given the sensitive nature of the subject. This trustful atmosphere ensures the confidentiality of the information shared, encouraging participants to provide frank and honest insights, where they may not have been comfortable providing such candid information in an online survey, or in a focus group or workshop setting with other participants.

[7] https://gdssummits.com/event/security-digital-summit-eu-apr-22/ and the recording of the panel session: https://gdsglobalmedia.s3.amazonaws.com/videos/summits2022/security/security eu day1 06 04 22 session2.mp4

A semi-structured interview format, a common approach in qualitative research (Willig, 2022), was used. This approach was selected to ensure all topics were covered with every participant while encouraging interviewees to share their personal experience and interpretations, which allowed the researcher to gain new insights. However, it is recognised that not all people are “equally articulate and perceptive” (Cresswell, 2008), and descriptions of experiences are shaped by the context of their organisation and the broader industry or societal environment. This study focused on the "lived experience" of cyber security practitioners, recognising that there are multiple constructed perceptions by other stakeholders on organisational learning (Willig, 2022). Additionally, interviews offered the flexibility for in-depth probing, allowing for clarification of responses and exploration of underlying motivations. This provided a more nuanced understanding of organisational learning practices than could typically be obtained through survey methods.

3.3.2.3 Thematic analysis

A thematic analysis, drawing on literature (Braun & Clarke, 2006, 2022; Terry et al., 2017), was employed to identify significant patterns within the interview data. This method of analysis is advantageous for gaining a deeper understanding of participants' experiences and can occasionally unearth unexpected insights (Braun & Clarke, 2006). An iterative coding procedure was used to capture the views expressed by participants. Following the initial coding, the analysis evolved from being inductive to a form of abductive research, clustering together relevant codes which related to the two theoretical frameworks (i.e. neo-institutional and organisational learning theories). From theses codes, themes were carefully interpreted to ensure they were substantiated by the data and offered meaningful perspectives on the research question. Details on the coding process, informed by Braun and Clarke (2006), and the development of themes are detailed in Chapter 4.

3.3.3 Research Question 3: research methods

RQ3: What new approaches to improve learning from cyber security incidents can be recommended?

3.3.3.1 Development of preliminary recommendations

This study embarked on developing recommendations to improve organisational learning from cyber security incidents by initially analysing empirical data from the practitioner interviews. These interviews shed light on the challenges organisations face and the impact of these challenges on the effectiveness of their learning practices. Due to a lack of comprehensive, standard guidance on effective learning from incidents, the research then leveraged insights from both the cyber security field and related research areas. The result was a set of tailored preliminary recommendations for cyber security practitioners in large organisations frequently dealing with security incidents. These preliminary recommendations aim to address the gaps identified in the practitioner interviews, integrating best practices and insights from the wider research literature.

The methodological approach began by examining the challenges and exploring possible solutions, identifying parallels in existing literature where similar challenges were addressed. The research aimed to evaluate the adoption and effectiveness of these solutions, considering their relevance and potential applicability in the cyber security context. Insights from the practitioner interviews laid the groundwork for identifying practices successfully implemented by some organisations to address these challenges. These interviews also provided practitioners' perspectives on factors that could enhance learning from incidents. These inputs were analysed and integrated into the preliminary recommendations. The detailed process of developing these recommendations, including how they were articulated and refined, is outlined in Chapter 5.

3.3.3.2 Delphi study

Following the development of preliminary recommendations, the Delphi method was employed to validate and prioritise them. The inclusion of “member checking” at this stage sought to enhance the

qualitative research's accuracy (Creswell & Miller, 2000). This section details the execution of the Delphi study, starting with an overview of its historical development and its application in consensus-building within research. The relevance of the Delphi method to the objectives of this study is also discussed, with a comprehensive description of how the method was applied in Chapter 6.

Originating in the 1950s, the Delphi method was named after the ancient Greek oracle of Delphi, renowned for its foresight. This method was conceived to guide structured group consensus, specifically to counteract the skewing effect of group dynamics on decision-making. Clayton (1997) notes that Delphi studies mitigate the risk of decisions being distorted by the reinforcement of like-minded opinions or the suppression of dissenting voices. This technique has been valuable in contexts where empirical data is scarce and analytical tools alone are insufficient for tackling complex issues (Farrell & Scherer, 1983). Linstone et al. (1975) identified the Delphi method as particularly well-suited to situations that benefit from a synthesis of expert judgements rather than from purely analytical solutions. While it is more complex and time-consuming than a single-stage survey, it provides an opportunity to align on a more shared view of knowledge (Spranger et al., 2022). Its asynchronous nature is beneficial, especially for accommodating the busy schedules of senior executive participants, who can contribute informed perspectives on the feasibility of recommendations within their organisations, shaped by their extensive experience.

The use of the Delphi method within the information systems sector has become increasingly prevalent (Thiebes et al., 2018). Its application in cyber security research is well-documented, with studies such as Goode et al. (2018), who engaged a panel of experts to curate topics for organisational cyber security awareness programmes, and Boakes (2022), who conducted a Delphi study to assess the importance of factors influencing the merger of physical and information security. Further applications include Cornejo (2021), who identified common human error causes of data breaches through expert panels, Akinrolabu (2019), who ranked the security factors of new cloud supplier security assessment tools via Delphi study, and Al Sabbagh et al. (2019), who validated a socio-technical security incident event monitoring artefact using a similar expert panel approach.

The Delphi method, by design, provides a platform without the social pressures and personality biases that could potentially influence outcomes during in-person discussions (Beiderbeck et al., 2021). While workshops, focus groups, or additional interviews could offer more detailed feedback, the Delphi technique was selected for its ability to systematically gather expert opinions in a time-efficient manner, making it suitable for participants with demanding schedules. In addition, the anonymity was helpful given the sensitive nature of the topic.

With the lack of a standardised protocol for implementing the Delphi technique, it is imperative to maintain transparency in the adopted methodology (Spranger et al., 2022). This study follows the guidelines established by Staykova (2019), ensuring that the recommendations are not only validated by a knowledgeable panel but are also robust and actionable. The specific details of the Delphi survey process and an analysis of the results are provided in Chapter 6.

3.4 Researcher perspective

A qualitative researcher is interpreting the world they are part of through their own personal lens, which has been shaped by their cultural memberships (Braun & Clarke, 2022). To provide transparency, details of the social reality which may have shaped the researcher’s perspective are discussed in this section. The researcher has an academic foundation in IT and cyber security, coupled with over 25 years of hands-on experience in the industry. This rich professional background not only granted exceptional access to senior professionals but also bolstered the credibility of the research during participant recruitment. There is a risk of being too embedded within the field which inhibits the questions a complete industry outsider might ask. Additionally, the researcher’s experience and

professional bias may have influenced the research approach and interpretations of the data. This was minimised by discussing the research approach and the analysis of the data with the supervisory team who could challenge assumptions and interpretations.

The researcher's British citizenship and exposure to international work environments, inevitably influenced the lens through which security agencies like the UK National Cyber Security Centre (NCSC) and regulatory bodies were perceived. Drawing from years of managing IT systems and cyber security, the researcher's conviction emerged that understanding the causes of incidents provides a foundation for deriving valuable lessons. This underlying perspective significantly influenced the development of recommendations in this research, reflecting a belief in the potential to enhance future security through informed incident analysis.

3.5 Limitations of the research

A summary of the limitations of the methods used by this work to answer the research questions is discussed in this section. This includes internal, external, and construct validity, as well as the overall reliability. Further discussions on the limitations of the methods, as applied in this research, is covered in the respective chapters.

Qualitative research is highly valuable for delving into the intricate details of people's experiences and their explanations of events. Nonetheless, the findings are often perceived as less readily generalisable. This limitation is counterbalanced by the particular contextual insights it provides within a specific study, time, and location (Creswell & Creswell, 2023). As researchers transition from specific empirical observations towards developing overarching propositions, they inherently engage in generalisation of the phenomenon (Conboy et al., 2012).

This study solely captures the perspective of cyber security practitioners, thus excluding the viewpoints of other stakeholders within the organisation regarding the security function's capacity to learn from incidents. While an ideal approach would encompass a representative sample of individuals outside the security domain within each organisation, this investment of resources and time would need to be part of a future study. Consequently, this research focuses on breadth over depth, gaining insights from cyber security practitioners across various organisations, as this enables the development of recommendations applicable to a wider range of organisations.

Interviews are complex social interactions involving both the interviewer and interviewee. The interpretation of interview data often faces criticism for lacking intersubjectivity. This limitation can be addressed by considering contradictory interpretations and challenging presuppositions (Kvale, 1996). The interpretation of findings may be influenced by the researcher's background and unconscious bias. To counteract this, Alvesson (2003) suggested maintaining awareness throughout the research process that empirical material can be interpreted in multiple ways. Providing reasons for specific interpretations can strengthen the research (Kvale, 1996). Silverman (2017) recommended understanding not just the literal content but also comprehending how participants have constructed their outcomes and the reasons behind their views.

Glesne (2016) cautioned against "backyard" research, where a researcher explores an area they are familiar with due to their existing role. In this instance, although the researcher formerly held a senior security position, they had disengaged from it before commencing the research. Moreover, most participants, in the interviews and Delphi study, were unknown to the researcher at the study's outset. The use of an existing network, while expanding from it, ensured participants met the inclusion criteria and held a certain level of credibility.

Another potential danger lies in researchers imposing theory-driven meanings on interview data, potentially misrepresenting participants' experiences and revealing more about the researcher's assumptions and theoretical inclinations than the studied practices (Willig, 2022). Transparency about decisions made during the research process is vital. It is particularly important to be transparent about assumptions and coding (Silverman, 2017). Researcher reflexivity was used in this study to evaluate alternative explanations and contribute to the research's rigour. Measures such as inter-coder reliability were not used as these assume there is an objective reality, which would not be consistent with the ontological stance of this work. Although such measures can be useful to communicate the transparency of the coding process and satisfy a broader acceptance of the work, there is also a danger that such numbers could convey a false precision (O'Connor & Joffe, 2020). Some researchers have strongly objected to the inclusion of inter-coder reliability rates (O'Connor & Joffe, 2020). The use of multiple coders was considered but, instead, thicker descriptions with raw quotations and the codebook were reported to provide transparency into the coding process. As Braun and Clarke (2022) explained, their view is "interpretation happens at the intersection of the data, the subjectivity of the researcher, and the scholarly and societal context of the research." Additional reliability was achieved through member checking to validate the recommendations in the next phase of the research.

Thematic analysis's theoretical independence can also be seen as a drawback, as it lacks strict rules, potentially leading to perceptions of reduced rigour (Braun & Clarke, 2006). Thematic analysis has also faced criticism for being more of a method than a theoretical approach like grounded theory, but it provides a defensible approach to engaging with data and generating robust analysis not bound to specific theories (Terry et al., 2017). Summarising data into themes does not inherently explain the effectiveness of specific elements in impacting learning compared to others. This would necessitate a distinct study. Some researchers argue that aggregating content into themes removes it from the original context in which it was shared (Silverman, 2017). While this holds true, findings need to be reported in a practical way to be digestible by the academic community.

The Delphi technique has evolved since its original forecasting purpose. While this approach offers flexibility for adaptation across various studies, it has faced criticism due to inconsistencies and subjectivity, particularly concerning key factors like panel size (de Loë et al., 2016). To address these concerns, this study adheres to the guidelines of de Loë et al. (2016), ensuring transparency in design choices and reporting, including participant continuity across the two rounds. Clayton (1997) emphasised that the Delphi study's quality is contingent upon the expert panel's credibility and their recognition as holders of valuable opinions on the surveyed topic. Linstone et al.'s influential 1975 paper on the Delphi technique, cautioned against the concept of "illusory expertise" within panels. They illuminated the inherent researcher bias in survey design and the selection of participants. Furthermore, they highlighted the risk of overemphasising consensus, which might exclude valuable yet unconventional viewpoints from lone experts. These risks were considered when analysing the results and in moderating the claims made of the findings.

This research design is centred within the local UK context and is not intended to compare findings from different countries or sectors. Recognising the dynamic nature of organisations, it is crucial to acknowledge that this study presents only a snapshot in time. In the rapidly changing landscape of cyber security, research findings can swiftly become outdated as organisations and attackers adapt. While this study delivers valuable insights, it is acknowledged it has some limitations in terms of generalisability, its concentration on cyber security practitioners, the specific UK context, and the single point in time nature of the research. Addressing these limitations and conducting further research will advance the understanding of effective incident learning strategies, ultimately enhancing organisational cyber resilience.

3.6 Ethical considerations

This section explains how ethical considerations were part of each phase of the research, including the ethics approval process, the informed consent of the participants, and how their data was protected. All research in this thesis was conducted in compliance with the University of Kent's code of practice and ethical guidelines, as well as adhering to the AIS Code of Research Conduct (Association of Information Systems, 2015). This involved pre-submitting all documents and detailed descriptions of the procedures to the University of Kent Central Research Ethics Advisory Group and obtaining their approval before commencing each of the three research activities that involved engaging with people—see Table 9. All data was analysed in a balanced way including the reporting of any contrary findings. Copies of the relevant publications were made available to participants.

Table 9 *University of Kent Central Research Ethics Advisory Group (CREAG) approvals*

Study	Date	Approval
Exploratory poll	22 February 2022	CREAG039-02-2022
Interview study	11 October 2022	CREAG099-08-22
Delphi study	7 July 2023	CREAG090-06-23

Participants in the exploratory poll, the interviews, and the Delphi survey were made aware of their rights before taking part in the research. This included collecting their informed consent, maintaining their anonymity and the confidentiality of their data, as well as ensuring they were aware of their right to not participate or withdraw their participation at any stage. For each study, a participant information sheet was shared explaining the purpose of the research, the process, how their data would be stored, and the expected outputs, including anticipated publishing. No incentives were offered to take part in the research and the research was not funded or managed by any third party.

The interviews were recorded using university supplied computer equipment. The recordings were transcribed using NVivo software or the Microsoft Teams software provided by the university, , both of which utilised encrypted storage. All data handling complied with General Data Protection Regulation (GDPR), including requirements to store data about European subjects within the European Economic Area (EEA), as recommended by the UK Government Service Manual under "Managing user research data and participant privacy."[8] regarding storage of data about European subjects in Europe. The Delphi study used the Qualtrics software to conduct the survey and Microsoft Excel software to analyse the data—both again provided by the university. All shared information within the three studies was handled confidentially, with data retention limited to the research's completion requirements. Given the sensitivity of cyber security incidents, individuals' and organisations' names were subjected to anonymisation. In cases where specific people or organisations were referred to in subsequent publications or presentations, pseudonyms were used.

Given the confidential nature of this research, establishing rapport emerged as a critical element to foster participants' trust in the security of their data. The potential risk of being perceived as an insider was balanced by enabling access to individuals who might otherwise have been challenging to engage due to the sensitive nature of the incidents. While building rapport was pivotal for successful semi-structured interviews, the researcher exercised caution to prevent any inadvertent encouragement of

[8] *Managing user research data and participant privacy*, UK government Service Manual. This guidance specifies that data must be securely stored, encrypted, and, where practicable, housed within the EEA to comply with GDPR standards. See also GOV.UK guidance on storing and handling research data: https://www.gov.uk/service-manual/user-research/managing-user-research-data-participant-privacy

interviewees to disclose more information than they were comfortable sharing (Willig, 2022). In instances where participants inadvertently revealed specific names of individuals or organisations, these identifiers were removed to protect confidentiality. Aggregate data related to participants' experiences in cyber security incidents and information about organisations' size and industry were collected and reported in a manner that prevented individual participants or organisations from being identified.

3.7 Chapter conclusion

This chapter positions the research within its ontological and epistemological framework, detailing the study's design, the rationale behind the selection of specific methods, and how these methods address the research questions. It also explores the limitations inherent in the research design and outlines the measures taken to manage ethical considerations throughout the study.

The combination of systematic literature review, the in-depth interviews, the development of recommendations, and the validation of these by a Delphi survey represents a comprehensive approach that allowed for a multifaceted understanding of how organisations manage incidents and how they can improve current learning practices. Leveraging the exploratory poll for preliminary insights paved the way for focused interviews. The insights from the practitioner interviews unearthed the barriers organisations face in gaining the most from learning from incidents. The thorough analysis of the themes from the interviews lent weight to the development of the initial recommendations. Validating and enhancing these recommendations by engaging with practitioners during the Delphi survey further reinforced the applicability and value of the research to practitioners.

Moreover, transparency and adherence to ethical principles served as foundational pillars throughout the research process. Obtaining prior approval from the University of Kent Central Research Ethics Advisory Group underscored the commitment to rigorous ethical standards. The assurance of informed consent, data anonymity, confidentiality, and the right to withdraw were fundamental to engendering trust among participants to study this sensitive topic.

Acknowledging the limitations inherent in any research endeavour, the design of the research navigated challenges surrounding this type of qualitative research. Conscientious efforts were made to be transparent about unavoidable biases inherent in such research, the choices made, and the techniques employed to enable other academics to assess the robustness of the research. The following chapters will present the application of the research methods described in this chapter and the findings of the research.

4 Organisational learning from cyber security incidents through an exploratory poll and interviews

Chapter 2 highlighted a gap in recent research concerning current learning practices from cyber security incidents and the obstacles organisations face in fully leveraging incident learning. Building on this, Chapter 3 detailed the pragmatic mixed methods approach underpinning this study. This chapter aims to address RQ2: "How do organisations currently learn from cyber security incidents, and what challenges do they encounter in the learning process?" This research involves direct engagement with organisations to gain insights specifically aimed at addressing the research question.

This chapter presents results from an exploratory poll which helped shape the interview protocol used in the study's main fieldwork with practitioners. It outlines the recruitment process for participants and details the formulation of the interview protocol. It then discusses the results of the thematic analysis of the interview data, examining their significance in relation to the existing literature.

4.1 Exploratory poll

4.1.1 Research methods

This section outlines the methodology behind the exploratory poll conducted as part of this research. In April 2022, a unique opportunity presented itself to engage directly with cyber security practitioners at the GDS Security Summit,[9] an event organised virtually in response to COVID-19 restrictions. The summit attracted security professionals from large organisations. This provided an ideal setting to explore their perspectives on learning from cyber security incidents.

As part of the summit, an opportunity emerged to host a panel discussion on learning from incidents, integrated with an exploratory poll designed to capture initial insights into organisational practices and perceived obstacles in learning from cyber security incidents. The development of the poll questions was directly informed by the literature review findings in Chapter 2, especially regarding the extent to which organisations engage in structured learning from incidents and the types of practices in place.

To ensure the poll was accessible and encouraged maximum participation during a fast-paced virtual conference, the format was deliberately kept concise. The poll consisted of five questions, each with no more than six response options. This structure was chosen to make it quick and easy for attendees to respond without interrupting the flow of the session. Both the questions and the answer choices were kept short and clearly worded to enable participants to scan and respond within seconds. Questions were designed to balance breadth and relevance, drawing from the literature, while being general enough to resonate across a wide range of organisations. Where appropriate, tick-all-that-apply formats were used to reflect the multifaceted nature of incident learning practices and to avoid forcing exclusive choices that might not reflect reality.

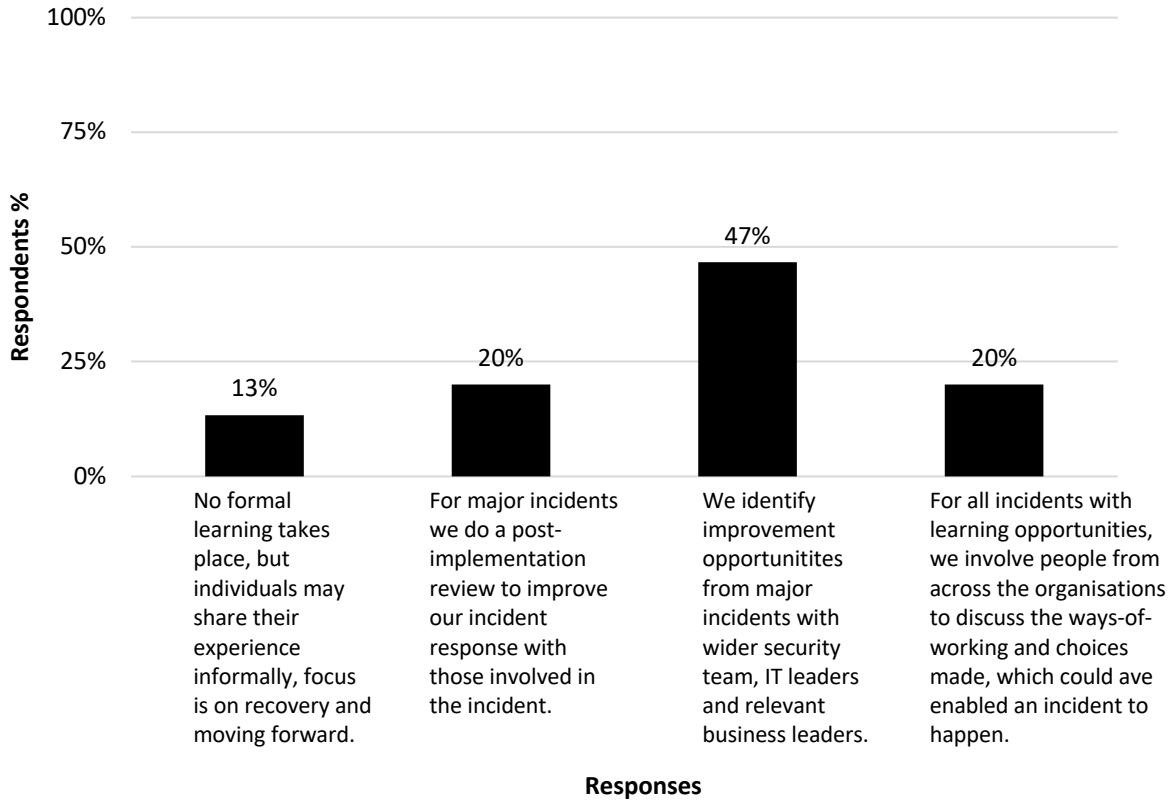
Conducted in real-time, the poll used the GDS Summit's virtual conference platform to display questions on attendees' screens, with responses submitted electronically. All attendees received relevant information about the poll, ensuring informed consent, and responses were collected anonymously to safeguard confidentiality. This exploratory poll was intended to provide initial insights that would inform and refine the questions for the subsequent in-depth interviews, helping to align them with real-world organisational practices in cyber security incident learning.

[9] https://gdssummits.com/event/security-digital-summit-eu-apr-22/ and the recording of the panel session: https://gdsglobalmedia.s3.amazonaws.com/videos/summits2022/security/security eu day1 06 04 22 session2.mp4

4.1.2 Results and discussion

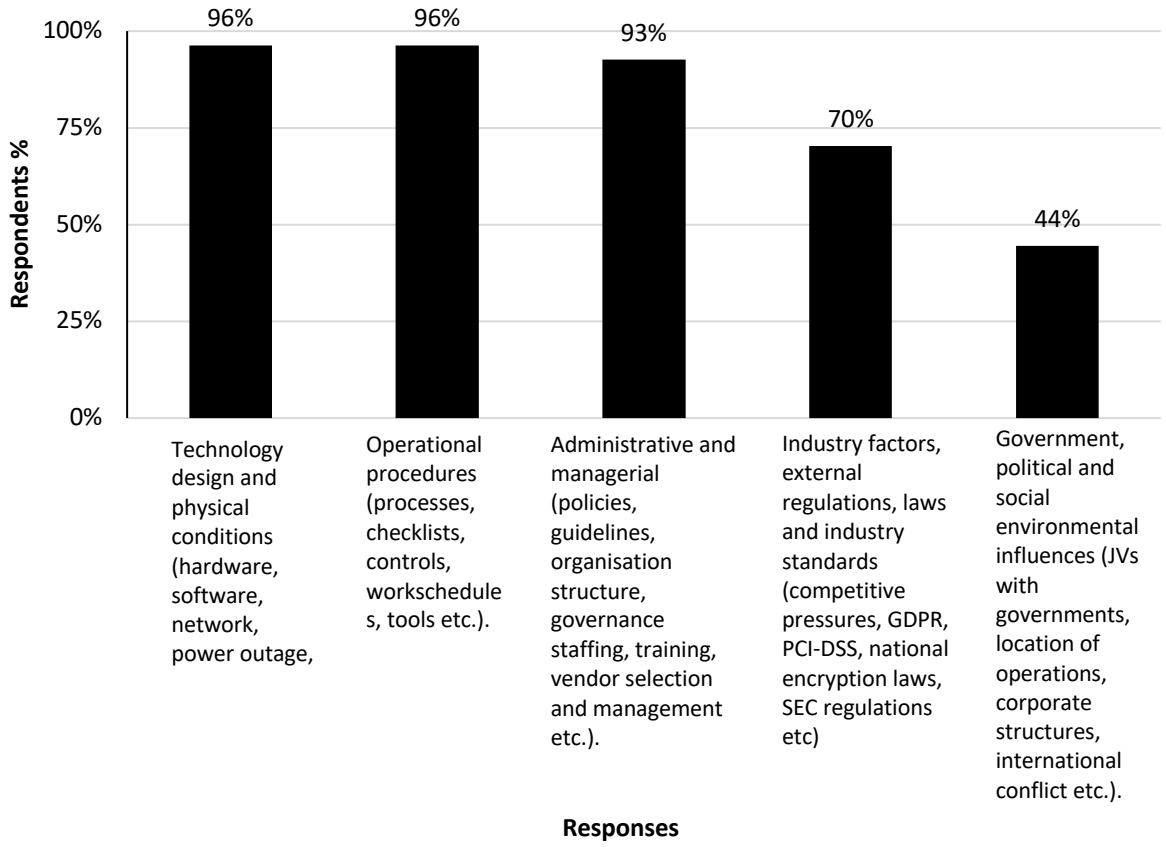
The exploratory poll's results, analysed question by question, offer initial insights into the current practices of learning from incidents within organisations. With 66 registered attendees for the session and an average response rate of 38% or 25 respondents across the five questions (detailed in Appendix C), the data provides a valuable snapshot of practices among senior security professionals in large organisations spanning various industries.

Figure 8 *Exploratory poll results to the question: What type of learning happens in your organisation following a cyber security incident?*



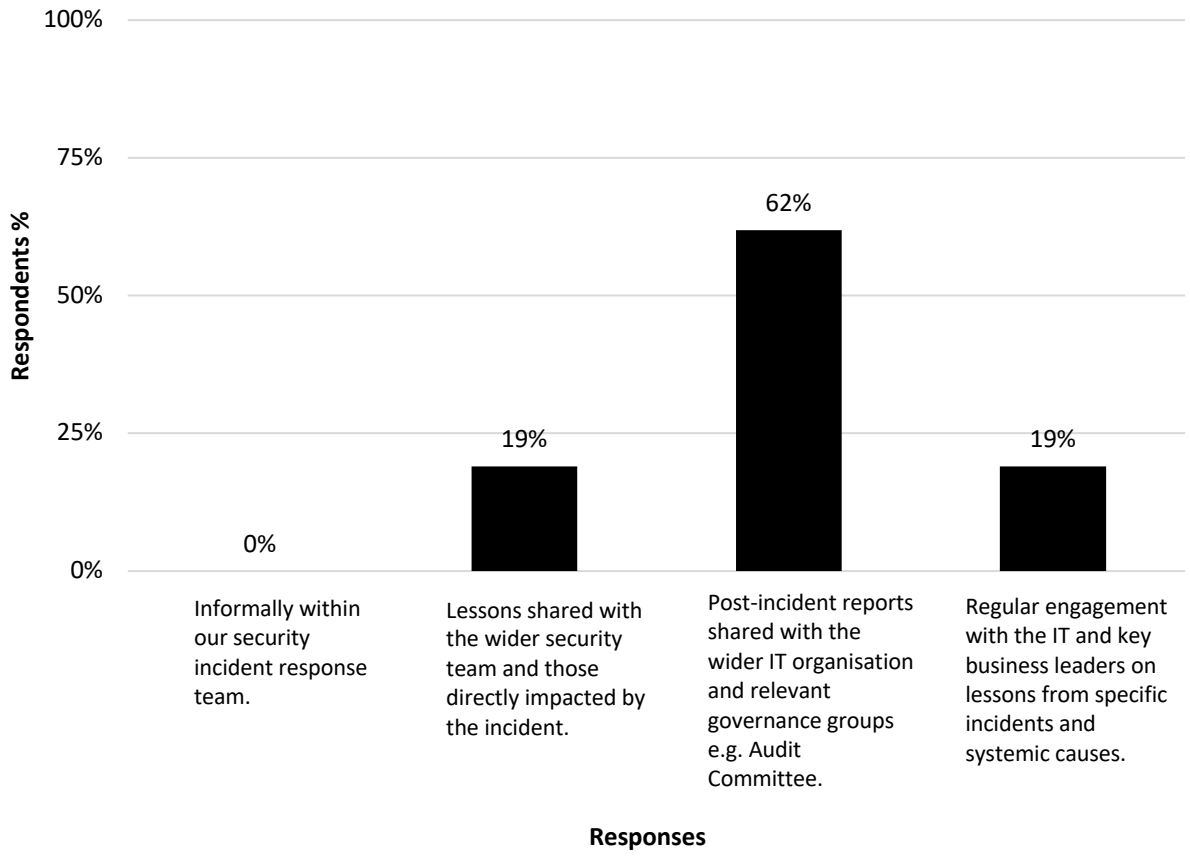
In the first question, Figure 8, a notable finding was that over half of the respondents' organisations included individuals beyond the IT department in incident learning activities, a figure higher than suggested by previous research (Ahmad et al., 2012, 2015; Grispos, 2016). This could be attributed to the larger size of the organisations represented, which typically have more formalised processes, or it may indicate a shift in organisational response strategies over time due to an increase in incident rates. Despite this, a third of responses indicated that only those directly involved in the incident were included in the learning process, potentially limiting the scope of lessons learned. Surprisingly, in just over 10% of cases, there was no formal learning process.

Figure 9 *Exploratory poll results to the question: When investigating the causes of incidents we consider (tick all that apply)?*



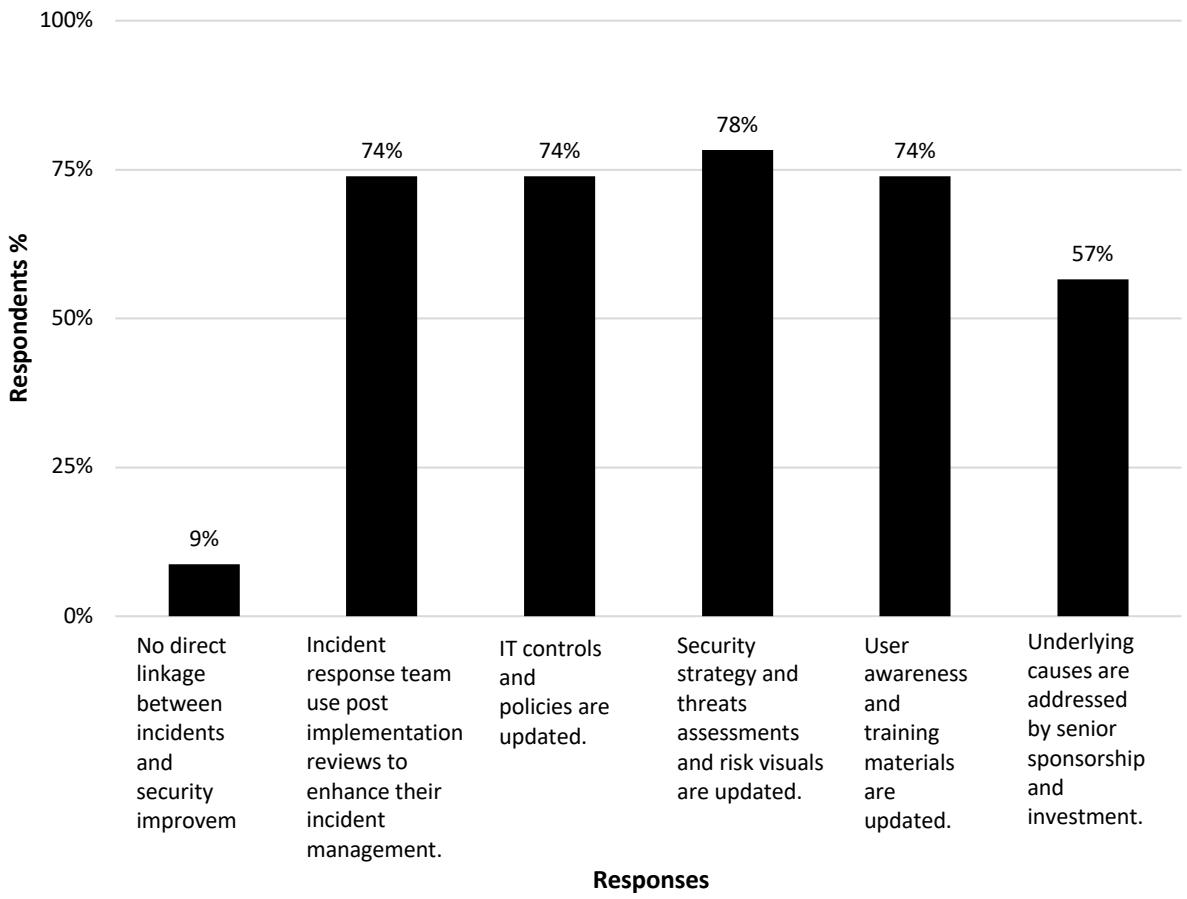
Responses to the next question, Figure 9, guided by the categorisation framework of Svedung and Rasmussen (2002), indicated that 70% of respondents considered industry factors, and 44% accounted for societal influences when analysing incident causes. This expanded consideration of contributing factors contrasts with Grispos (2016), whose findings suggested a narrower focus, potentially due to differences in organisational perspectives or the specific context of his case study nearly a decade ago. The observed discrepancy may reflect either a genuine understanding of complex causality among respondents or the influence of desirability bias, where participants provide answers they believe to be socially acceptable or aligned with organisational expectations. These differences were further explored through the practitioner interviews conducted in this study.

Figure 10 *Exploratory poll results to the question: Who in your organisation do you share lessons with (select one option)?*



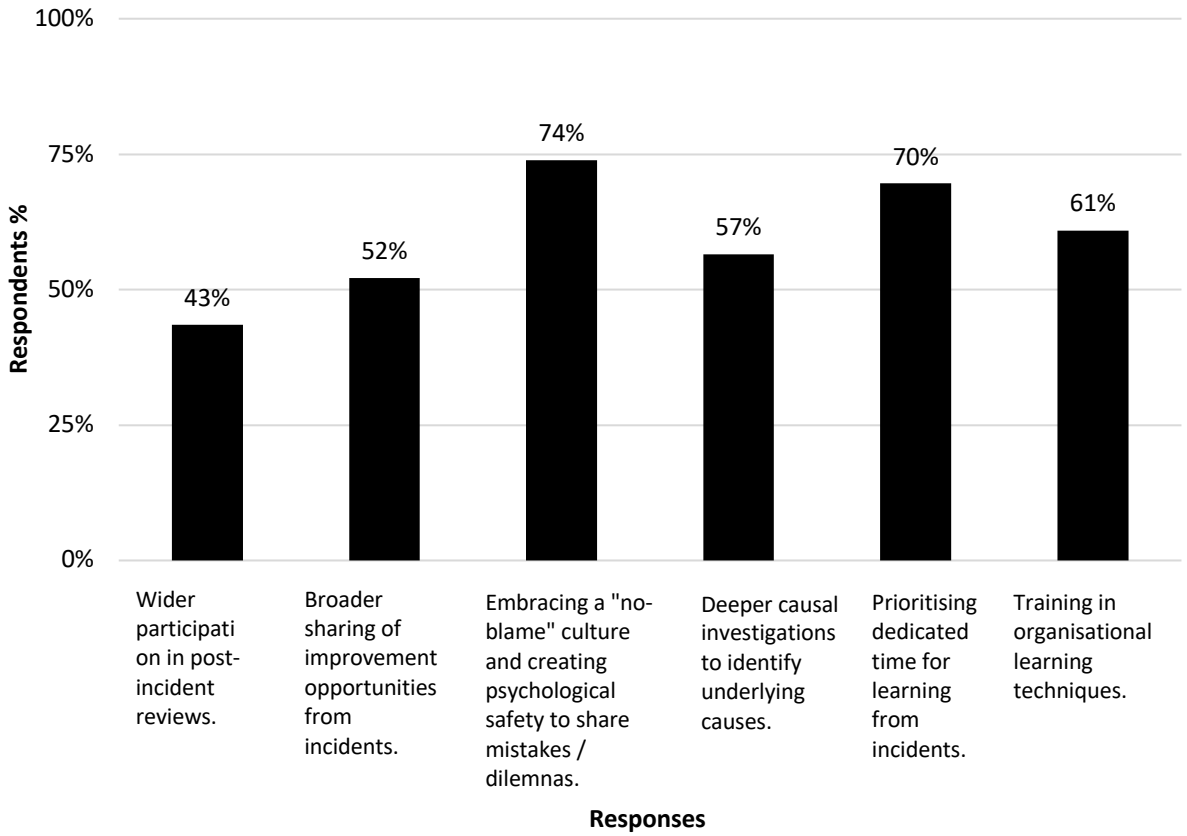
The third question, Figure 10, showed a broader sharing of incident reports and engagement across IT and governance groups than previously identified by Ahmad et al. (2015) and Line et al. (2006). However, still only 19% of respondents claimed to regularly engage with leaders on lessons learned. This suggests a possible gap in action implementation follow-up, echoing findings by Grispos (2016). Again, this was explored in the practitioner interviews.

Figure 11 *Exploratory poll results to the question: How are lessons acted upon (tick all that usually apply)?*



The poll also indicated a commitment to addressing underlying causes, with over half of the organisations involving senior leadership sponsorship, see Figure 11, although this result seems at odds with the 19% reporting regular leadership engagement on specific incident lessons in the previous poll question, as it is often necessary for teams to involve senior leaders to unearth and tackle contributory causes. This discrepancy might suggest respondents differentiate between lessons from specific incidents and more general underlying issues. The options 2-5 selected by over 70% of respondents aligns with the broad range of causes analysed (Figure 9). The responses align with the standards and guidance advocating for learning beyond mere incident response improvements, such as ISO/IEC 27035-2 (2023) and the NCSC's Cyber Assessment Framework. This could imply that organisations are implementing a broad range of changes following incidents, but it is difficult in a short poll to distinguish the difference between participants sharing their "espoused theory of action" (how they intellectually perceive their actions) and the practices their organisations actually follow (Argyris, 1994). This is an area which was explored in the next phase of the research, the practitioner interviews.

Figure 12 *Exploratory poll results to the question: Which would help your organisation to learn more from incidents (tick all that apply)?*



The final question, Figure 12, highlighted that while 43% of respondents see wider participation as beneficial for learning from incidents, aligning with the involvement reported in the first question (Figure 9), over half still advocate for more extensive sharing as a method to enhance learning. The recognition of the need to create psychological safety by nearly three-quarters of organisations aligns with established research (Catino, 2008; Edmondson, 2018; Schilling & Kluge, 2009), as does the emphasis on dedicating time to incident learning, supported by 70% of organisations, mirroring Drupsteen and Hasle (2014). The desire for deeper causal analysis, despite extensive investigations indicated in the second question (Figure 10), points to a need for further research to reconcile this apparent contradiction. The acknowledgement of the value of additional training in organisational learning suggests a gap in available guidance for enhancing organisational learning practices.

4.1.3 Limitations

The results from this exploratory poll, drawn from a limited sample of organisations and restricted to five questions, offer insights that, while not broadly generalisable, highlight several areas for deeper investigation in the next research phase. The anonymous format of the poll may also have encouraged respondents to indicate aspirational practices rather than actual ones, as it did not permit follow-up requests for examples or detailed clarification that interviews can provide. Further research is needed to examine observed discrepancies, especially around leadership engagement in root cause analysis and the reported thoroughness of investigations versus the desire for more comprehensive causal analysis. Key areas for exploration—such as fostering psychological safety for sharing errors, allocating time for learning, and training in effective learning techniques—emerged from these findings and were incorporated into the development of the interview protocol for the practitioner interviews.

4.1.4 Conclusions

This section reported the insights gained from the exploratory poll and outlined how these findings informed the subsequent in-depth interview research (Section 4.2). The poll, which gathered responses from 25 participants, each representing a different organisation, revealed an unexpectedly high level of engagement in learning activities and a more thorough investigation of underlying causes than prior research suggested. However, given the survey's limited scope, further research is needed to clarify the discrepancies between leadership's engagement in these activities and their commitment to addressing foundational issues, alongside the call for deeper causal analysis despite claims of comprehensive investigations. The poll underscored the importance of exploring factors that could strengthen organisational learning, such as fostering an environment where sharing errors is encouraged, securing dedicated time for learning, and providing training in effective learning methodologies. Together with the literature review findings presented in Chapter 2, these preliminary insights helped refine the design and focus of the practitioner interviews, contributing to a more nuanced understanding of how organisations currently learn effectively from incidents (Appendix E).

4.2 Practitioner interviews

This section outlines the research methods used for the practitioner interviews, including participant recruitment, data collection, and analysis. It presents the results, interpreted through the lenses of neo-institutional theory and organisational learning theory, to examine the challenges organisations face in learning from cyber security incidents.

4.2.1 Research methods

Building on insights from the literature review and exploratory poll, this phase of the research involved conducting practitioner interviews. Following the research design for semi-structured interviews outlined in Chapter 3, this section describes the application of these methods, including the timing, participant selection process, the balance between virtual and face-to-face interviews, and the duration of the sessions.

The semi-structured format provided a structured framework for discussion while allowing participants to share their first-hand experiences and perspectives openly. Questions were formulated based on insights from the literature review and exploratory poll, incorporating elements from established incident-based learning processes, such as those discussed by Drupsteen et al. (2013) and Littlejohn et al. (2017). Finally, the process of data analysis is detailed, from the initial stages of coding through to the development of overarching themes.

4.2.1.1 Participant recruitment

Semi-structured interviews were carried out from October 2022 to April 2023. These interviews were adapted to either virtual or in-person formats according to the preferences of the participants. Interviewees were selected based on their roles within their organisations to ensure a deep understanding of how their organisations learn from incidents. A purposive sampling strategy was employed to align the sample with the research objectives, as advocated by Campbell et al. (2020). This approach was complemented by snowball sampling to encompass a wide range of industries, recognising that practice variations across sectors could yield a richer understanding of the research questions. The selection process adhered to specific inclusion and exclusion criteria, mirroring the strategy utilised by Tetrick et al. (2016) in their exploration of Cyber Security Incident Response Teams across 17 organisations.

Recruitment leveraged personal networks, thus the calculation of response rates is not reported. Only participants with experience in cyber security were selected to participate (see Appendix D). Cyber

security practitioners from a spectrum of sectors, including private, public, and not-for-profit organisations operating within the UK and employing considered large (over 250 staff), were engaged. This criterion was based on the likelihood of these organisations having experienced incidents (NCSC, 2022) and undertaken subsequent modifications as a result of learning from these incidents. Although the number of practitioners interviewed represents a fraction of the potential population, this sample size was deemed adequate for addressing the research question. O'Reilly and Parker (2013) highlighted that the value of research findings hinges not on participant quantity but on the appropriateness of the data provided. This study aligns with such work.

4.2.1.2 Practitioner interviews data collection

A comprehensive interview protocol was devised to encompass crucial topics such as participants' experiences with learning from incidents, including successful practices as well as encountered limitations or barriers, and their perspectives on potential improvements. This methodological approach was informed by techniques from the field of safety to adapt learning from incidents for cyber security contexts, thereby ensuring a comprehensive examination of socio-technical dynamics. The interviews aimed to be an informative conversation and were approached with an inquisitive and non-judgemental manner to encourage open dialogue (Glesne, 2016). Details of the questions posed can be found in Appendix D.

Three pilot interviews were conducted, which were successful and included in the results. All interviews were either recorded using university-provided equipment or, for online sessions, recorded on MS Teams. At the beginning of each interview, participants were informed about the recording, which was subsequently transcribed. Online interview transcriptions were handled directly by MS Teams, whereas face-to-face session transcriptions were managed using NVivo software. The recordings were anonymised, with each participant assigned a unique code (e.g., P1 to P34) used to reference them in the results. All data was stored in compliance with GDPR and data encryption standards. The confidentiality of participant responses was protected, with access to the transcripts restricted to the researcher and their supervisory team.

4.2.1.3 Practitioner interviews data analysis

Following the approach used by Clare and Kourousis (2021) in their study of learning from incidents within aviation maintenance, this research employed a detailed coding process to analyse interview data. The coding facilitated the identification of significant patterns articulated by participants, which were refined through multiple iterations with feedback from the supervisory team. Using NVivo software, key themes were rigorously developed to ensure they were well-supported by the data and directly addressed the research question (RQ2). This process followed the thematic analysis framework outlined by Braun and Clarke (2006), with the codebook and identified themes provided in Appendix E.

To enhance the analysis, neo-institutional theoretical concepts introduced in Chapter 3 were applied as a structured lens, consistent with the qualitative research strategy of employing theoretical frameworks to interpret data (Glesne, 2016). A reflective thematic method was adopted, where initial themes were refined into a thematic map. This map underwent thorough review to ensure the significance and coherence of the themes, linking them to the overarching research aims. Findings were further validated through discussions with the supervisory team, ensuring both methodological rigour and practical relevance.

It is important to highlight, following Braun and Clarke (2022), that the aim of data analysis in qualitative research is not to detail every single nuance but to generate substantial insights that are relevant to the research question. The depth of the data, coupled with the transparency of sharing original quotations and the codebook in Appendix F, allows for the validation of interpretations by

other researchers (Glesne, 2016). Through iterative refinement, the themes were honed to offer a cohesive and comprehensive understanding of the interview data.

4.2.2 Results

4.2.2.1 Practitioner interviews participants

The interview cohort consisted of 34 cyber security practitioners from organisations with employee numbers ranging from 450 to over 200,000, representing a diverse cross-section of industries. These industries were categorised into four main groups for analytical purposes, detailed in Table 10 and elaborated upon in Appendix D. The majority of the interviews were conducted virtually (28), with a minority in person (6), and they averaged 39 minutes in duration.

The primary purpose of the interviews was to explore the cyber security practitioners' perspectives on their organisations' learning practices and the challenges encountered in enhancing these processes. Given the qualitative nature of this study, counting the frequency of specific topics mentioned by the participants was not considered an appropriate measure, as the depth and emphasis of discussions varied. To indicate the prominence of findings, terms such as 'many' were used when a topic was referenced by at least 20 practitioners. To illustrate and enrich the analysis, direct quotations from the data are presented.

The anonymous identifiers [P1], [P2], etc. do not correspond to specific individuals across different studies but were randomly assigned within each dataset. This approach maintains confidentiality while allowing for references to specific contributions in the analysis.

Table 10 *The organisations of interview participants by industry*

Industry	Count
Finance and insurance	11
Government, public bodies and non-for-profits	3
Services, retail, tourism and entertainment	7
Industrial, energy, transport and logistics	13
Total organisations	**34**

In terms of roles, half of the interviewees were serving as Chief Information Security Officers (CISOs), while others held similar positions—such as Chief Information Officers (CIOs), Heads of Incident Response, and Information Security Managers—or were responsible for reporting to CISOs, as set out in Table 11 (further details in Appendix C). The span of cyber security experience among participants varied widely, from 3 to 30 years, with both the mean and median figures standing at 15 years. This breadth of experience provided a rich and varied foundation of expertise for the study.

Table 11 *Roles of the practitioner interview participants*

Role	Count
CISO	17
CIO	3
Other	14
Total organisations	**34**

4.2.2.2 Practitioner interviews thematic analysis

The thematic analysis yielded four key themes that captured the factors shaping the organisational learning practices from cyber security incidents and the challenges encountered. These themes

collectively provided insights towards addressing the second research question (RQ2), including current learning practices and the challenges organisations face.

This section identifies four key themes related to organisational learning from cyber security incidents. The first theme, inspired by neo-institutional theory, is titled "Isomorphic Pressures on Organisational Learning Practices"—see Section 4.2.2.3. It illustrates the development of current learning practices under various isomorphic pressures and suggests that organisations often engage in these practices without formally evaluating their efficacy. Despite not having explicit assessments, many interviewees considered the non-recurrence of incidents as an informal indicator of effective learning. However, a few participants acknowledged repeat incidents as a sign that their organisations could have learned more effectively from past events.

In addressing the challenges of the learning process for the second part of RQ2, three additional themes were identified, focusing on barriers encountered at distinct phases of learning from incidents. These include:

1. Challenges of uncovering incidents (Section 4.2.2.4).
2. Challenges of identifying the causes (Section 4.2.2.5).
3. Challenges of implementing the lessons (Section 4.2.2.6).

Together, these themes offer a comprehensive perspective on the multifaceted challenges that hinder organisations from effectively learning from cyber security incidents.

4.2.2.3 Isomorphic pressures on organisational learning practices

Neo-institutional theory, as introduced in Chapter 3, describes isomorphic pressures—coercive, normative, and mimetic—that influence organisational practices. This section examines how these pressures shape organisational learning from cyber security incidents. Coercive pressures arise from external mandates such as regulatory requirements or contractual obligations. Normative pressures reflect industry norms and shared professional standards that guide incident management and classification. Mimetic pressures, meanwhile, emerge as organisations emulate the practices of others, particularly in uncertain or rapidly evolving contexts. Together, these pressures reveal the external and internal dynamics that drive the development of learning practices and highlight the challenges organisations face in fostering meaningful incident-based learning.

4.2.2.3.1 Coercive pressures

Regulatory reporting requirements, as a form of coercive pressure, have significantly shaped incident communication protocols. For instance, under the GDPR, organisations must report personal data breaches to the relevant supervisory authority within 72 hours of becoming aware of the breach if it is likely to result in a risk to individuals' rights and freedoms.[10] This has made it increasingly common for legal representatives to be part of incident response teams. Participants highlighted the complexities associated with operating within global organisations, where jurisdictional nuances emerge based on variables such as the affected subjects, breach locations, or attackers' identities [P6]. The necessity to engage with multiple regulatory bodies and government organisations introduces further layers of complexity to incident communications, as articulated by participant [P16]. A few participants described a cautious approach to information sharing, revealing only what is strictly required by local regulations, as guided by their legal departments [P12, P10].

Market structure's coercive pressures have compelled all surveyed organisations to impose mandatory incident reporting clauses on their suppliers, reflecting the deep entanglement of IT services with a network of suppliers. Participants expressed their frustration with suppliers' opacity, with one stating, "sometimes we see it in the press quite honestly and so even though we have contractual

[10] GDPR regulation: Regulation (EU) 2016/679 https://eur-lex.europa.eu/eli/reg/2016/679/oj

requirements, you know it's quite complicated" [P33]. Information dissemination on incidents is often perceived to be restricted to crafted public relations narratives or online announcements [P20]. This lack of transparency causes speculation and results in a lag in the organisation's capacity to evaluate incident ramifications, as explained by another participant: "In an ideal scenario, we'd like to know a lot sooner, but I think the reality is we come to know a lot later and then we investigate what's the impact on us" [P7]. While participants recognise these communicative obstacles, there's also an acknowledgement of their own influential role in fostering a culture of transparent communication with suppliers, which is deemed crucial for proactive and collaborative actions. For example, participant [P4] spoke of their efforts to encourage collaboration with suppliers:

> So, if they're deemed to be breaching a contractual term they don't like it. Do I think we get all the incidents? We definitely don't … they get really worried about how seriously we would take things on a call I just had, one of them was saying, 'You know, I have reported incidents to … before, and they've not come down on me like a ton of bricks. They've actually been quite supportive and helpful.' So we do try to create a culture with industry of 'please tell us because we can do something about it then'. So, for you, for us and for others, if necessary, please don't keep it from us. We are reasonable. [P4]

Participants voiced concerns over their organisations' reticence regarding potential litigation or regulatory repercussions following incidents. This wariness influenced their documentation practices in post-incident reviews, where participants raised concerns that their incident response documentation may later be used in legal cases against the organisation. This cautious stance was extended to sharing incident information with external entities, with the fear of litigation constraining open communication with their customers, suppliers and peers.

The dread of legal or regulatory fallout was cited by over half of the participants as a major inhibitor to thorough incident investigations and subsequent actions. The negative effect of litigation concerns on the learning process was underscored by participant [P24]: "We're going to be thoughtful about what documentation we actually put together post this because of the potential of discovery. … It's litigation that has had the most chilling effect on enabling people to learn lessons." Training by legal teams has led incident response teams to restrict their records to only indisputable facts [P10, P24], instilling a hesitance to fully document root causes and lessons learned. As [P10] described, this training fostered "a sense of nervousness about writing down root causes and lessons … that sort of stops people from being as candid as they could about what happened."

While a handful of participants did engage in sharing cleansed lessons with regulators to aid the broader industry, this was not a widespread practice. The value of disseminating incident learnings for societal benefit was acknowledged, yet there was a consensus on the lack of safe forums for such exchanges. The need for a more mature industry approach that allows for open sharing without fear of repercussions was emphasised by participants, with [P7] suggesting the goal should be "the ability to share freely while knowing that it's not going to backfire in many ways."

4.2.2.3.2 Normative pressures

The consistency observed in the practices across the interviewed organisations indicates that normative pressures may have contributed to shaping their incident reporting and classification processes. Each organisation interviewed maintained a process to review significant incidents and produce reports presenting the lessons learned. However, the exploratory poll conducted earlier revealed that 13% of respondents indicated their organisations did not have a formal learning process. This discrepancy could be attributed to differences in the size of organisations participating in the exploratory poll—though the conference was targeted at large organisations, it did not define specific criteria—or it could reflect varying interpretations of what constitutes a formal process. Despite the

universal implementation of mandatory training on cyber security incident reporting, there was no formal evaluation of its effectiveness. Nonetheless, many organisations endeavoured to create an environment conducive to reporting by promoting a non-punitive culture.

Classification methods for incidents varied among organisations, with some utilising tiered systems—Gold, Silver, and Bronze—and others applying numerical scales such as 1-4 or 1-5. Approaches also differed in whether to separate data breaches from cyber-attacks or to consolidate them under a unified security incident category. Some participants aligned with general IT management procedures for incident prioritisation within their organisations, opted to leverage existing processes where feasible, as stated by [P28]: “I try and use as much of the IT process as I can and not reinvent the wheel.” While industry frameworks like ITIL[11] and NIST Special Publication 800-61 Revision 2 were not directly probed, several participants referenced them during the interviews (ITIL was cited by P12, P20, P24, P25, P28, P30; NIST cited by P5, P10, P14, P15, P19). Organisations followed a variety of practices in classifying cyber security incidents; some chose to align these with their broader IT incident classifications, while others maintained distinct categories for cyber security, highlighting the difficulty in standardising classifications given the unique aspects of each cyber incident.

Participants acknowledged that despite having established incident classification protocols, their organisations did not always conform to these standards, often influenced by internal politics or the need to prioritise certain incidents. The dynamic nature of incidents meant that classifications could evolve during the lifecycle of an incident, leading to the reclassification of incidents or, in some instances an event not eventually being classified as an incident. This was explained by [P18] who said, “We do have some that we will classify as a Priority 2 because it could be and then it dies down and is re-classified as a Priority 3, and then it won’t go into the post-incident process.” The classification of an incident is significant as it influences the extent of the post-incident investigation performed.

The assignment of incident classifications hinged on practitioners' judgement, with the focus on the nature of the response required over the learning potential from the incident. Classification played a critical role in determining the scale of response, the involvement of senior management, and the composition of the review team, which varied based on the business areas affected. [P22] illustrated this by stating, "It depends on the incident. For an HR system issue, HR would be integral to the discussion because they own the service."

The effort invested in learning from an incident, the participants in review meetings, and the publishing of outcomes were all influenced by how incidents were classified. Yet this classification process was highly subjective and lacked uniformity across organisations. [P33] highlighted this inconsistency, noting, "There’s a global shortfall in how we classify cyber security incidents, with emerging frameworks only just starting to address this." This variance underscores the inherent difficulties in generating reliable cyber incident statistics and accentuates the complexities in researching cyber security incidents.

4.2.2.3.3 Mimetic pressures

Organisations often adopt the practices of others in response to uncertainty—a phenomenon referred to as mimetic pressures in neo-institutional theory. These pressures were evident in how participants viewed learning from incidents, highlighting the struggle to apply lessons due to leadership's limited grasp of cyber risk and the dynamic nature of the field. The usefulness of referencing incidents at peer

[11] Information Technology Infrastructure Library (ITIL): ITIL is a set of detailed practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business. Originating in the 1980s by the UK Government’s Central Computer and Telecommunications Agency (CCTA), it is currently managed by AXELOS, a joint venture between the UK Cabinet Office and Capita plc. The latest version, ITIL 4, was introduced in 2019 and emphasises a more flexible, business-integrated approach to service management (AXELOS, 2019).

organisations to underscore risks and advocate for cyber security investment was reported by the participants. There was a consensus on the value of broader incident sharing to enhance organisational learning. Attempts to share incident insights with regulators, security agencies, and peers aimed to enhance collective learning, although high workloads often hindered frequent exchanges, as highlighted by [P19]: “You spread the knowledge that you get from the incidents. But this often doesn't happen because of the high workload.”

The desire for increased information sharing and learning from peers was pronounced, yet there was an acknowledgement that individuals often prioritise learning from incidents that directly affect them. While the significance of learning from incidents at other organisations was recognised, the immediacy and impact felt were less when those incidents were external to their own sector or geography. This influenced the urgency and engagement with learning opportunities, as encapsulated by [P10]: “If you're in Germany, an incident happens in Spain, you don't experience it in the same way.” Nonetheless, the type of incidents occurring within peer organisations played a role in shaping their threat perceptions, underscoring the interconnectedness of security across the industry (regardless of geography).

4.2.2.4 Challenges of uncovering incidents

Participants commented that the challenge of achieving full awareness of incidents within their organisations had been exacerbated by expanding data footprints and the increased connections to other organisations due to digitalisation. They were conscious of being in a continuous state of concern, knowing that a major incident was inevitable, especially if they had not encountered one recently [P18, P25]. This concern was partly due to the digital transformation, which has broadened the scope for potential cyber security threats. Several participants voiced a desire for better visibility into incidents, suspecting that more were occurring than they currently knew about. This awareness motivated them to actively search for potential issues, underlining the importance of proactively encouraging incidents to be reported.

With the growing recognition of the importance of incident reporting by employees, customers, and suppliers, there has been a cultural shift away from blaming individuals. Incidents are increasingly seen as learning opportunities for the entire organisation, not just for those directly involved [P23]. This shift has fostered a more compassionate approach, viewing those involved in incidents as victims and encouraging them to share their experiences to motivate others to report incidents [P18]. Reflecting on past practices, [P5] noted, “We used to have processes where an incident would happen, and then a report would go to a committee to decide if someone's remuneration should be cut because of the incident. We've taken a step away from that culturally.” [P29] memorably described this cultural evolution towards openness and improvement as “a culture that looks at an incident as an opportunity to grow and get better, rather than as an opportunity to cut someone's throat and advance your own career.”

Most interviewees strongly advocated for creating a workplace that views incidents as chances for organisational learning and improvement rather than for assigning blame or furthering personal agendas. Participants commented that this transformative approach towards incident management and response is becoming prevalent across the cyber security sector, influencing not only the treatment of employees but also the criteria for recruiting and dismissing Chief Information Security Officers (CISOs). A notable trend has emerged where organisations are increasingly valuing candidates with prior incident handling experience [P5, P17]. Despite recognising the substantial hurdles in cultivating a culture that encourages open communication and transparency, there is a firm commitment towards fostering this change [P5, P6, P9]. [P12] encapsulated the sentiment by stating, "The biggest single challenge so far has been to encourage a culture of openness and transparency amongst our people to admit failure."

4.2.2.5 Challenges of identifying the causes

In this study, participants shed light on the difficulties of pinpointing the exact causes of incidents within their organisations. Although many were confident in the scope of their investigative efforts, it was noted that no organisation had purposefully evaluated the effectiveness of their causal analysis. Often, investigations would identify a root cause as a singular system failure, neglecting to consider more nuanced factors like organisational culture or financial structures. As one participant put it, "We'd look at the control failure and we'd articulate it in the context of the control failure" [P5].

The need for a more comprehensive approach to analysing incident causes was recognised, with [P31] suggesting "that second level of really digging is certainly an improvement area we could make." However, practical challenges such as limited time and resources frequently restricted the exploration of broader, systemic issues. Highlighting this point, [P18] emphasised the importance of a holistic review processes, stating, "We've identified a significant number of vulnerabilities in our managed estate that says the patching process isn't working right... What this says is you need to take a step back and review the end-to-end process to say why?... And the trouble doing that is that it takes time."

Interviewees explained that incidents often have an emotional impact on their teams, and leaders need to encourage a return to these incidents to investigate underlying causes. The aftermath of severe incidents frequently left teams drained, resulting in a desire to return to normal operations and a lack of energy or resources to devote to delving into root causes. As [P4] noted, "We are under-resourced for everything that we need to do, and so running an incident [response] is a huge effort for us at times, and so we just move on to something else."

The success of post-incident reviews depended significantly on involving the right mix of individuals at the appropriate times. It was essential to include those with operational expertise alongside senior staff to ensure the development of valuable lessons and actionable measures. Highlighting the importance of diverse input, [P2] noted, “I'm a very big fan of having business representation because they do ask the right questions.” Nonetheless, arranging for such involvement was often difficult, given the limited availability of key personnel and the multitude of demands on their time.

Organisational politics and individual defensiveness emerged as significant obstacles to cause identification. The complex nature of cyber security incidents often leads to a culture of shifting blame or attributing faults to external factors to evade accountability. Fostering a culture focused on learning and improvement, rather than blame, is essential for overcoming these barriers. One strategy proposed was to involve the internal audit team in evaluating the quality of after-action reports, rather than just counting the occurrences of issues [P1].

There was a clear recognition of the benefits of examining incidents with lower impact severity ratings to discern patterns and root causes. Yet this approach hinged on the consistent categorisation of causes and the availability of dedicated data analysis resources. Many participants highlighted a gap in their organisations' ability to systematically track and analyse incident themes and trends, with [P7] noting, "But could we do better in terms of tracking themes or trends? Absolutely. I don't think we're there yet."

These insights underscore the intricate challenges in dissecting incident causes, pointing to the need for shifts in organisational culture, better resource distribution, and enhanced capabilities in trend analysis. This theme suggests that a comprehensive understanding of an incident's causes opens avenues for learning and subsequently enables an organisation to take steps to strengthen their security posture.

4.2.2.6 Challenges of implementing the lessons

The implementation of lessons learned from incidents presents a substantial challenge for organisations, as indicated by study participants. There was considerable variation in the mechanisms for tracking lesson implementation and accountability across organisations. In mature and heavily regulated sectors like finance, there exists a structured process for reporting progress on lesson implementation to senior risk committees [P5, P16, P20, P21, P33]. In contrast, some organisations saw the responsibility of the incident response team concluding with the issuance of a post-incident report and leaving action items to be managed locally without central oversight. As [P12] put it: "They tend to be passed out and left locally to manage." Meanwhile, other organisations adopted a central tracking system for actions, diligently following up until remediation was achieved, referred to by [P28] as "the non-automated nagware." It was noted that while immediate fixes were tracked, broader improvement actions often lacked effective monitoring [P10].

The initial drive to implement fixes identified after high-profile incidents frequently diminishes over time. The urgency and attention given during an incident tend to decrease once containment and recovery begin, especially among those not directly involved in the incident management, leading to a reduction in momentum for broader improvement efforts. This was encapsulated by P10: "You can get so fixated on the heat of the moment in an incident and the energy can wane. So, when you've contained and recovered, everybody's a little bit bored, tired or fatigued of that situation."

Addressing structural issues and committing to significant investments often encounters delays. Organisations tend to postpone major system overhauls or upgrades, a decision that can lead to heightened costs and compounded problems. [P32] captured this dilemma: "The longer you leave it to actually replace or redo a system, the more it's going to cost you. Therefore, it is even less likely to get done, which actually makes the problem worse … you sort of disappear down a bottomless spiral until something goes disastrously wrong … and you have no choice."

Prioritising cyber security investments emerged as a significant challenge, with participants pointing out the difficulty in securing funding for initiatives that do not directly demonstrate a return on investment (ROI). Yet incidents were viewed by some as opportunities to gain financial support for security improvements, leveraging the heightened awareness following an event. [P14] remarked, "Never let a good incident go to waste... you're just going to jump on the bandwagon… It's hard to prove ROI. It's hard to get people's attention… but when an incident happens, I think this is the time to strike."

Budgeting decisions often reflected the diverse experiences within security teams rather than a holistic evaluation of an incident's impact, leading to potentially skewed priorities. [P17] said, "People have a bunch of different experiences. Some people just come from patch management. So, they're going to think that is the most important thing." Additionally, the efficacy of lessons learned could diminish over time, with organisations reverting to previous practices or failing to adapt to evolving threats, thus highlighting the importance of continuous adaptation and vigilance [P30]. Systematic evaluations of the effectiveness of implemented lessons were rare, with the attention on project completion rather than on addressing the root cause of issues. "It was interesting to see how much we're focusing on the project, on meeting the deadlines, on getting stuff done versus actually, are we doing the right thing, have we actually fixed the problem?" observed [P6].

The variation in how organisations tracked the implementation of lessons learned from incidents was significant, yet a common theme emerged: few were rigorously evaluating the effectiveness of their actions. Even in cases where tracking mechanisms were well-established, the emphasis often lay more on completing tasks than on critically assessing whether those actions had genuinely addressed the

underlying issues [P5, P6, P11]. This focus on task completion over effective resolution highlights a gap in the post-incident learning process.

Leadership plays a pivotal role in overcoming these challenges, not just by ensuring actions are tracked but also by maintaining the momentum for change and insisting on evaluations that verify the impact of those changes. There is a pressing need for a shift towards a more reflective practice, where the success of actions taken in response to incidents is measured not by their completion but by their contribution to enhancing the organisation's security posture and resilience.

4.2.3 Practitioner interview discussion

4.2.3.1 Organisations' current learning from cyber security incidents

The practitioner interviews aimed to explore the two facets of RQ2: "How do organisations currently learn from cyber security incidents, and what challenges do they face in the learning process?" Regarding how organisations learn, the study unveiled more advanced incident learning practices than those reported in earlier studies (Grispos et al., 2015; He, Johnson, Lu, et al., 2014; He & Johnson, 2015; Lakshmi et al., 2021; Line et al., 2006, 2016; Tatu et al., 2018; Van der Kleij et al., 2017). This evolution may reflect the increasing frequency and complexity of cyber-attacks, alongside a broader acceptance of normative processes in more recent years. Despite the variation in industry sectors, there was a notable uniformity in incident learning practices, albeit with more structured action tracking observed in regulated sectors. This homogeneity across sectors indicates a professionalisation among cyber security practitioners and the prevalent adoption of normative processes, suggestive of isomorphic pressures.

The interview findings corroborate the neo-institutional theory, which posits that organisations often converge on similar practices under isomorphic pressures, adopting these methods more for their perceived legitimacy and to project an image of rationality, as described by Alvesson and Spicer (2019), rather than from evidence of their efficacy. Rae and Provan (2019) found that post-incident reviews serve an important social role, signalling the organisation's dedication to serious incident management. This ritual reassures stakeholders by demonstrating familiarity with established protocols, although the content of reports and recommendations often reflects and reinforces existing organisational power structures.

The data reveal that participants observed the recommendations identified during review sessions were notably influenced by the attendees, budget allocations among teams, and the Chief Information Security Officer's (CISO) prior experiences. Some noted that incidents were occasionally used to justify pre-existing investment plans, indicating that the adoption of practices is not solely based on their effectiveness but also shaped by various pressures. This observation lends support to the neo-institutional theory, which argues that organisational actions are not merely reactions to rational economic pressures but are influenced by broader organisational dynamics and norms.

Interviewees also highlighted that incident reports submitted to executives and risk committees often bypass detailed scrutiny of the learning process behind the lessons learned. This behaviour aligns with organisational defence mechanisms and the paradoxes highlighted by organisational learning theory. Reports to senior management are generally abstract, aimed at rationalising actions rather than examining the depth of learning (Argyris, 1999). While senior leaders aim to address issues, their approach, combined with the abstract nature of reports, inadvertently promotes a culture of defensiveness. Consequently, team members prioritise presenting single-loop solutions, focusing on actions within their control, rather than exploring deeper, systemic changes.

Senior leaders often refrain from questioning post-incident reports, fearing that doing so may unsettle their teams or expose their own contributions to systemic causes. Consequently, the actions outlined

in these reports may yield short-term gains, masking underlying issues that are likely to resurface (Argyris, 1999). These single-loop actions can be likened to a drug that alleviates symptoms, deterring the pursuit of necessary lifestyle changes. Argyris (1999) explains that this tendency often stems from management's limited awareness of the challenges associated with double-loop learning. In many organisations, the "undiscussability of the undiscussable" prevails, discouraging individuals from voluntarily questioning their own roles in incident causes (Argyris, 1999). This discovery underscores a potential lack of critical assessment and independent evaluation concerning the effectiveness of incident learning practices within organisations. As described by Meyer and Rowan (1977), such activities often take on a "ritual significance", serving to maintain appearances and validate the organisation.

Participants also emphasised the challenges of quantifying cyber risk and ensuring that organisational leadership fully comprehends its implications. The World Economic Forum (2023) found some cyber security professionals were not able to articulate risks in ways that could be understood and acted upon by senior leaders. This can result in cyber security risks not receiving the appropriate attention or resources required. Organisational learning theory suggests that these issues may result from not only a lack of knowledge but also highly skilled yet automatic defensive actions (Argyris, 1999). Leaders may not be as willing to recognise risks which result from their own shortcomings. As a means of conveying the seriousness of cyber risks and promoting awareness among leadership, organisations often shared examples of incidents that had impacted similar organisations. This practice aligns with the neo-institutional theory, as organisations seek to reduce uncertainty by imitating the experiences of others in similar contexts.

The organisations studied voiced significant concerns about the legal and regulatory implications of learning from incidents, mirroring the finding by Husák et al. (2023) that GDPR has led to a reduced willingness among organisations to share security-related data, even though the regulation does not prohibit such sharing. This highlights a tendency towards excessive caution, with organisations hesitating to delve deeper into the regulations to find compliant ways to share information. These behaviours reflect the coercive pressures of neo-institutional theory, influencing how organisations approach learning from incidents.

Despite a pronounced interest in lessons from incidents in other organisations, participants noted that such external incidents often do not receive the same level of priority or funding as those experienced directly. Yet examples were shared where investments in security were made in response to incidents affecting peer organisations, indicating that external incidents can indeed prompt internal resource allocation and security enhancements. This phenomenon illustrates the mimetic pressures described in neo-institutional theory, where organisations adapt based on observations of their peers.

The increasing focus on holding organisations accountable for data protection, coupled with the complex interdependencies within modern IT supply chains, can inadvertently stifle the exchange of valuable lessons, limiting the capacity for organisations to enhance their data protection efforts (Husák et al., 2023). There is an opportunity for regulators to play a more active role in facilitating information exchange among companies, ensuring that the act of sharing knowledge does not lead to penalties or increased regulatory scrutiny. While coercive pressures from multiple jurisdictions and diverse regulatory demands escalate, they do not necessarily translate to more effective practices, as noted by S. Khan et al. (2022). Some government bodies, like the UK's NCSC CISP[12] community—as mentioned by participants—have started to encourage threat intelligence sharing, yet there's a consensus that further actions are needed.

[12] National Cyber Security Centre (NCSC) Connect Inform Share and Protect (CISP) is a platform to facilitate UK-based cyber security practitioners to collaborate on cyber threat information in a secure and confidential environment: https://www.ncsc.gov.uk/cisp/home

Additionally, apprehensions about legal consequences have not only curbed suppliers' openness but also challenged organisations in acquiring timely incident information, thereby delaying impact assessments. This observation is in line with Friday et al.'s (2021) findings on supply chain dynamics, which highlighted that the contractual incentives for profit maximisation and service cost reduction proved counterproductive during crises. Such contractual incentives may hinder the objectives of service restoration and learning from incidents, as parties prioritise their immediate commercial interests.

Similar transparency issues in the supply chain were identified by Jaatun and Tøndel (2015) in the context of cloud computing and echoed in the examination of the Capital One cyber security incident by N. F. Khan et al. (2022). To tackle these transparency issues, it is vital to realign commercial incentives to encourage the open sharing of incidents and near misses. Current guidelines on securing the software supply chain, as advised by the Cybersecurity and Infrastructure Security Agency (2023),[13] lack detailed instructions beyond recommending the establishment of incident reporting and response mechanisms. This underscores the need for a more pronounced role to be played by governments and industry bodies in aiding organisations to construct more resilient supply chains.

The importance of establishing open communication channels with suppliers was a recurrent theme among participants, seen as essential for facilitating proactive measures and collaboration. Yet they also highlighted the inherent difficulty in sharing information prematurely, confronting the dilemma of whether to share immediately for quick dissemination or to wait until a clearer understanding of the incident is developed, as discussed by Ashraf et al. (2022). Despite these challenges, there was a consensus on the need for the industry to evolve towards more open sharing practices, advocating for early dissemination of incident information, albeit sometimes incomplete, to expedite collective learning. This approach acknowledges that acquiring a full understanding of an incident often unfolds over the course of an investigation. The necessity for further research into the dynamics of inter-organisational cyber security information sharing is reinforced by recent studies (Albakri et al., 2018; Wagner et al., 2019; Zibak & Simpson, 2019), which highlight the need to address these challenges comprehensively.

All organisations in this study implemented systems for classifying incidents, illustrating the influence of normative pressures. Despite this common practice, variations in classification systems were observed. Some participants noted intentional departures from standard classifications, reflecting a thoughtful evaluation of their classification strategies. This suggests an effort to consider the appropriateness of classification methods beyond mere compliance with industry norms, potentially reducing isomorphic pressures. However, the lack of a universally accepted taxonomy for classifying incidents complicates the sharing of incident data and best practices among organisations. Establishing a universally recognised, standardised taxonomy would not only facilitate information exchange but also enhance collective learning from incidents. Additionally, Ibrishimova (2018) highlights that limited transparency between organisations regarding cyber security incidents further obstructs the development of a universal taxonomy.

In summary, the research reveals how isomorphic pressures—normative, coercive, and mimetic—shape incident learning practices within organisations. Although this study does not quantify the relative impact of these pressures, it identifies their significant influence. Legal and regulatory concerns, the alignment of commercial incentives, variations in incident classification, the challenge

[13] The Enduring Security Framework (ESF) is a public-private partnership, cross-sector working group of the Critical Infrastructure Partnership Advisory Council (CIPA) to address the threats and risks to the security and stability of US national security systems: https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/Enduring-Security-Framework/

of accurately quantifying cyber risks, and disparate incident classifications underscore the complexities of incident learning. These findings also point to the difficulties organisations encounter in embracing the double-loop learning approach proposed by organisational learning theory (see Section 3.2.1). Overcoming these obstacles necessitates regulatory adjustments, the creation of standardised incident taxonomies, and a deeper insight into the forces that drive incident learning practices in organisations.

4.2.3.2 Challenges to learning from cyber security incidents

Addressing the second aspect of RQ2, which explores the barriers organisations encounter in learning from incidents, our interviews underscored the critical role of promoting an open culture and the importance of reporting incidents within organisations. Security awareness training on reporting illustrates normative practices, although some mandatory training is propelled by coercive pressures stemming from regulatory requirements, in line with findings by Hielscher et al. (2023). Despite many participants asserting their organisation's commitment to a blame-free culture, none had methodically verified this claim. The UK government cyber security breaches survey (2023) indicates that post-incident reviews serve to engage employees on cyber security matters. Participants recounted instances where individuals, having succumbed to phishing or other social engineering tactics, were treated as victims rather than culprits, sharing their experiences to motivate others to report incidents.

The recognition of the importance of a blame-free culture by participants echoes findings from prior research (Catino, 2008; Edmondson, 2018; Schilling & Kluge, 2009). Ballreich et al. (2023) stressed not only the need to cultivate a supportive culture but also the essential understanding among employees of what constitutes an incident and the correct reporting procedures. While this research is somewhat limited in scope, it highlights the need for deeper investigation into the views of those asked to report cyber security incidents. The effort to shift organisational culture, a challenge well-documented across various fields (Alvesson et al., 2016), merits additional exploration in the context of cyber security incident reporting. Furthermore, our participants pointed to challenges in the process of incident cause analysis, including selecting the right attendees, choosing the investigation methods, and managing the balance between the investigation's thoroughness and the resources required.

The concept of deep-diving into an incident's root causes, as advocated by organisational learning theory, is undoubtedly beneficial yet demands significant time and frequently conflicts with other priorities. The aftermath of an incident can leave individuals hesitant to participate in thorough inquiries to determine contributory causes. Organisations yet to evaluate the efficiency of their approach to understanding the causes might risk either excessive or insufficient resource allocation to these processes. Our interviewees observed that budget decisions often mirrored the preferences of the CISO rather than a comprehensive understanding of causes of incidents. Elliott and Macpherson (2010) observed that identified lessons tend to reflect the knowledge base of those leading the investigation, or even internal power dynamics. Manfield and Newey (2018) noted a propensity for depending on established practices over innovative solutions. Organisational learning theory suggests a natural inclination towards recommending solutions for visible errors without challenging the foundational policies or assumptions underlying more complex issues.

Navigating the complexities of post-incident investigations requires a nuanced understanding of both organisational dynamics and individual psychology. Argyris (1990) underlined the necessity of confronting organisational politics and personal defensiveness, while Tavris and Aronson (2020) pointed out the challenges posed by the unreliability of human memory, which allows individuals to rationalise their actions and adjust their recollections in a self-serving manner. Petrie and Swanson (2018) advocated for leadership that promotes systemic thinking, yet acknowledge the obstacle presented by a prevalent reductionist mindset in the business sector, which may hinder comprehensive understanding of incidents within complex IT environments. Such a mindset

complicates genuine organisational introspection about the decisions leading to incidents. The concept of double-loop learning challenges individuals to address uncomfortable truths, but organisational norms often deter this level of inquiry, promoting instead defensive behaviours that avoid confrontations, making it difficult to identify the causes contributing to an incident (Argyris, 1999).

For organisations, there is a critical need to move beyond superficial post-incident actions—such as policy updates or targeted training—that fail to address deeper systemic issues. Demjaha et al. (2019) and Kirlappos et al. (2014) stressed the importance of examining why security expectations are not met by individuals, suggesting that a singular focus on controls overlooks the multiplicity of contributory factors. Advocates of organisational learning from incidents, including Ahmad et al. (2012, 2020) and Shedden et al. (2010, 2011), championed the adoption of double-loop learning. This approach encourages probing beyond the superficial details of an incident to critically examine the underlying decisions and assumptions (Argyris, 1994), urging a shift from merely treating symptoms to addressing the fundamental conditions that allow security breaches to occur.

The translation of lessons learned from incident investigations into tangible organisational improvements presents a significant challenge. While frameworks like NIST Special Publication 800-61 Revision 2 presuppose that captured lessons will naturally lead to corrective actions, this is not an automatic reality within organisations. Elliott and Macpherson (2010) drew a clear line between the identification of lessons and their actual application in altering organisational practices. Edmondson (2002) pointed to the discrepancy between the appearance of reflective learning and the genuine implementation of change. Moreover, Manfield and Newey (2018) discussed how the concept of "bounded rationality"[14] among leaders constrains their willingness to integrate these lessons, especially in environments already undergoing substantial change.

The complexity of IT ecosystems and the push towards digitalisation compound the difficulty of enacting structural changes. Innovations like generative Artificial Intelligence (AI) and the Internet of Things (IoT) expand the footprint of IT systems which need to be protected and introduce new challenges in mitigating structural vulnerabilities. While adopting a "secure by design" philosophy is advocated, many organisations grapple with the constraints of legacy systems and the dynamic landscape of cyber threats, which can be hard to predict during the design and integration phases. Nevertheless, such new technologies can present opportunities for enhancing the implementation of actions derived from incident learning. McIntosh et al. (2023) demonstrate that, in certain scenarios, AI-generated policies not only outperform those crafted by humans but can also improve the effectiveness of staff training programmes, offering a pathway to more effectively action some of the simpler lessons learned from cyber security incidents.

Practitioners voiced concerns that senior leaders often lack a comprehensive understanding of cyber security risks and the necessary investments to mitigate these risks. This observation resonates with findings from the World Economic Forum (2023), which highlighted difficulties in securing leadership consensus on actions to address cyber threats. Participants pointed out the challenge of prioritising cyber security investments, especially when demonstrating return on investment (ROI) is challenging. Nonetheless, an increase in investment was often noted following significant incidents, aligning with research by Demjaha et al. (2019), which suggested that incidents could instigate a spike in funding. However, it was observed by some participants that investments might lean towards "security theatre" —initiatives that create the illusion of security without substantially enhancing it. Moore et al. (2016)

[14] Bounded rationality, as discussed by Manfield and Newey (2018), refers to the cognitive limitations that restrict leaders' ability to integrate all relevant lessons, particularly in complex or rapidly changing environments, which may hinder effective organisational learning.

also identified compliance with regulations as a primary motivator for cyber security budgeting, indicating the impact of coercive pressures on security practices.

A recurring issue highlighted was the shortage of skilled cyber security professionals. The lack of security experts often led to the prioritisation of urgent issues rather than reflective activities such as evaluating the learning process. Organisational learning theory stresses the importance of understanding the learning process itself (Drupsteen, 2014). While few participants reported repeat incidents, only a minority of organisations systematically evaluated the effectiveness of implemented actions in mitigating the contributory causes identified in post-incident reviews.

This research supports institutional theory, revealing that isomorphic pressures predominantly shape practices rather than evaluations of their effectiveness by individual organisations. Challenges identified in adopting effective organisational learning practices encompass establishing a blame-free environment, conducting comprehensive analysis of causes, addressing organisational politics and individual defensiveness, avoiding superficial post-incident actions, and ensuring the successful implementation and assessment of corrective measures. Addressing these issues calls for further research into the cultivation of supportive organisational cultures, and the implementation of proactive cyber security strategies that recognise the complexities of IT ecosystems.

4.2.4 Limitations

This research into cyber incident learning practices offers significant insights, yet it is important to recognise its limitations. The qualitative nature of this research provides an in-depth understanding of participants' experiences and perspectives but limits the generalisability of findings. The researcher's engagement in the research process and the interpretive nature of thematic analysis mean that the themes identified are influenced by personal perspectives; therefore, different researchers might interpret the data in alternative ways (Braun & Clarke, 2022). The study's sample size, involving 34 practitioners, aligns with common qualitative research practices but does not claim to statistically represent the broader population of organisations. According to Gibbs et al. (2007), who reviewed nearly 800 interview studies, there is considerable variation in sample sizes, often without explicit justification, typically ranging between 15 and 60 participants. While the sample size might seem modest, the depth of knowledge among participants about the subject matter underpins the validity of the insights gained. Nonetheless, reliance on professional networks and snowball sampling for participant recruitment could bias the sample, an acknowledged limitation of the methodology used. As O'Reilly and Parker (2013) emphasised, the adequacy of the sample should be evaluated based on data quality, not just participant numbers. Participant recruitment was facilitated through the researcher's existing industry network, a strategy that proved invaluable in accessing this often-elusive population.

The study's reliance on voluntary participation raises concerns about self-selection bias, where individuals with a keen interest in cyber security incident learning might disproportionately represent the views, potentially omitting a broader range of perspectives. Leaders, in particular, may present an overly positive self-image, influenced by social desirability bias, and their responses might reflect an idealised version of their actions, as Argyris (1994) noted regarding the "espoused theory of action" that may diverge from actions under stress. To counter these biases, the research employed strategies such as indirect questioning and requests for specific examples, coupled with assurances of confidentiality and carefully phrased enquiries (Bergen & Labonté, 2020). These approaches aimed to deepen the authenticity of the responses and mitigate bias impacts. However, the possibility that responses were shaped by interviewees' desire to conform to perceived social norms or professional expectations remains a limitation (Alvesson, 2003). Additionally, the data's reliance on individual accounts from a single representative per organisation, without external verification, underscores the

subjective nature of the findings. This methodology acknowledges the constructed reality of participants' experiences, a factor that both enriches and bounds the study's insights.

The interview structure was meticulously designed to elicit comprehensive discussions, providing insights pertinent to the research questions. However, it is crucial to recognise that the narratives shared during the interviews were shaped by the interviewees' perceptions, thus subjective, and not necessarily reflective of an objective reality (Alvesson, 2003). This research relies on the accounts of participants without external validation of these accounts. Pilgrim (2014) highlights the potential discrepancy between practitioners' perceived realities and the actual situation, prompting careful distinction in the analysis of interview data. While the methodology included recording and transcribing verbal exchanges, and despite incorporating visual cues from online video interactions or face-to-face interviews, the analysis predominantly focused on verbal information, which may overlook non-verbal expressions of significance.

The purposive sampling strategy was adopted to encompass perspectives from a broad spectrum of industries and organisational sizes. However, the sample size limits the ability to claim a statistical representation reflective of the wider practitioner community. Despite this, the interviews succeeded in capturing a diverse range of viewpoints and experiences, enriching the study with substantial depth within the practical confines of the research. Notably, the presence of 13 female participants, constituting 38% of the sample, surpasses the usual gender ratios observed in the cyber security sector, particularly at senior levels (Da Silva, 2023). This overrepresentation may be indicative of the researcher's network and gender influence. The strategic use of an existing professional network, augmented through broader engagement, ensured that selected participants met the inclusion criteria, bringing relevant expertise and insight to the research.

The scope of this study was intentionally focused on the perspectives of cyber security practitioners, omitting the views of other organisational stakeholders on how effectively the security function learns from incidents. This research aimed for broad applicability by engaging security professionals across diverse organisations. Future inquiries might benefit from including a selection of non-security business leaders within a smaller set of organisations. Such an approach would offer insights into the broader organisational perception and engagement in the learning process.

The research predominantly engaged UK-based participants, potentially limiting the applicability of its findings internationally, despite most surveyed organisations operating globally and many participants having responsibilities that extend beyond the UK. To validate the relevance of these findings in different geographical and legal settings, additional studies are warranted. Although the study purposively sampled across various industries, it included only a limited number of organisations from each sector, focusing on larger entities. Investigating potential sector-specific variations and extending the research to encompass smaller organisations could uncover valuable insights.

Given the dynamic nature of the cyber security field, this study’s findings represent a specific moment in time, with the risk of becoming quickly dated as organisational practices evolve. Longitudinal research that tracks the learning processes of multiple organisations over time would yield a more detailed picture of how organisational learning adapts to the changing cyber security landscape. Moreover, there is a need for more granular research to refine causal analysis methods into root causes and to understand the impact of social and political dynamics on learning practices. Ethnographic studies within organisations actively engaging in incident learning processes could provide additional depth. Highlighting isomorphic pressures and the hurdles in conducting thorough causal analyses, this study points to the necessity for further in-depth exploration to evaluate the true efficacy of organisational learning strategies and the tangible benefits of investing in learning from incidents.

4.3 Chapter conclusion

This chapter has detailed the insights gained from an exploratory poll and practitioner interviews, undertaken to address RQ2. It has shed light on the obstacles organisations encounter in their efforts to learn effectively from cyber security incidents, underscoring the critical need for a deliberate evaluation of their learning practices. The emergence of isomorphic pressures, as illuminated by this study, corroborates the principles of neo-institutional theory, highlighting the necessity of examining the influences on learning from incidents. Participants described the difficulties inherent in achieving the double-loop learning advocated by organisational learning theory, marking this investigation as one of the pioneering efforts to delve into these complexities.

For organisations to enhance their learning from incidents, it is necessary to evaluate the effectiveness of their learning processes, ensure a culture of psychological safety that encourages reporting, and develop robust networks to enable shared learning throughout their supply chains. The process of incident classification critically influences the selection of incidents for detailed learning. While there are instances of organisations exploring broader learning opportunities, such as engaging in peer collaborations and conducting simulation exercises, it is crucial to discern whether these practices are adopted as a result of mimetic pressures or are genuinely informed by an evaluation of the organisation's own learning needs. A considerable number of participants articulated a keen interest in learning from lower-level incidents and near-misses, aiming to identify recurring themes and tackle systemic challenges, although few are actually regularly performing this analysis currently.

To broaden the scope of insights gathered from incident learning processes, organisations are encouraged to incorporate a diverse range of perspectives in post-incident reviews. Engaging various teams can deepen the analysis of contributory causes and foster lessons with broader organisational ownership of addressing the issues. There is a need for further studies to assess the benefits of this diversity in participation in post-incident reviews for a comprehensive understanding of incident causes. Wider participation needs to be weighed against competing organisational priorities to assess the benefits of investing the time in learning from incidents.

The tendency of organisations to prioritise immediate operational needs often detracts from their capacity to question existing assumptions and investigate the root causes of incidents sufficiently thoroughly. Leaders play a pivotal role in creating a culture where questioning and innovation are valued, enabling the identification and implementation of significant improvements to security measures. This study has revealed instances where there was a hesitancy to acknowledge deep-seated causes and a shying away from identifying challenging lessons. The reluctance to confront these issues often stems from a fear among individuals of being blamed for the problems or being held accountable for fixing them. To surmount this issue, there is a suggestion for the adoption of systematic causal analysis tools and the engagement of skilled facilitators. These measures can help to reveal underlying systemic issues and promote a culture oriented towards proactive learning and improvement.

This research underscores the critical need for organisations to advance beyond basic symptomatic solutions and cursory reviews following incidents. It advocates for a deeper analysis of contributory causes and the adoption of lessons that lead to significant enhancements in security measures. While this study reveals progress in organisational learning from incidents, surpassing findings from prior research, it also identifies substantial areas for further improvement.

In summary, the findings stress the importance for organisations to rigorously assess the effectiveness of their incident learning practices and actively tackle the challenges inherent in this process. Such efforts will not only bolster cyber resilience but also promote a culture of ongoing enhancement, equipping organisations to navigate the dynamic cyber security environment more effectively. The insights gained contribute to the expanding literature on the integration of neo-institutional and

organisational learning theories within the realm of cyber security, laying groundwork for future research and practical application. The following chapter leverages the themes extracted from the interviews to formulate actionable recommendations for practitioners, to be used by them to refine their approach to learning from cyber security incidents.

5 Developing preliminary recommendations to enhance organisational learning from cyber security incidents

Building on the themes from the thematic analysis of practitioner interview data in the previous chapter, Chapter 5 addresses RQ3: "What new approaches to improve learning from cyber security incidents can be recommended?" It examines the challenges and barriers identified by participants and considers the implications for organisations, focusing on both incident learning and overall security posture. Drawing on the limited literature in cyber incident learning as well as insights from other relevant fields, it proposes initial recommendations aimed at strengthening organisational learning practices for incident management.

5.1 Approach to formulating preliminary recommendations

The practical implications of this research are intended to guide key roles within organisations responsible for learning from cyber security incidents. For each theme identified from the practitioner interviews, the analysis outlines how roles such as CISOs, Heads of Incident Management, Senior Leaders, and Audit and Risk Committees can take targeted action. For example, CISOs should lead efforts to enhance incident reporting culture, while Senior Leaders are responsible for ensuring cross-departmental engagement in post-incident reviews. By clearly aligning each recommendation with relevant roles, this research provides actionable guidance for improving organisational learning. They were carefully crafted to ensure practicality, offering clear and straightforward guidance that practitioners in these roles can easily implement. By leveraging the insights from interview findings and the evidence gathered through the literature review (Chapter 2), the recommendations are designed to be both comprehensible and actionable for those responsible for driving improvements in organisational learning from incidents.

The preliminary recommendations were reviewed to assess their adequacy in addressing the identified challenges. This review process included a clear explanation of each recommendation and why it was made, focusing on making them easy to understand and use for practitioners. The objective was to articulate the recommendations in a manner that was both clear and actionable. The conciseness of the recommendations was also a key consideration, to facilitate their validation in the Delphi survey phase of the study, detailed in Chapter 6.

5.2 Analysis of themes, associated implications and preliminary recommendations developed

This section delves into each theme identified from the practitioner interviews, moving beyond description (as covered in Chapter 4) to examine the factors within the organisation that allow these challenges to persist. It consults relevant literature to understand where similar challenges have been addressed. The analysis is expanded to assess the implications of each challenge for the organisation, considering how these challenges limit the potential benefits of learning from incidents and restrict enhancements to the organisation's cyber security resilience. Building on the analysis, this section will propose six preliminary recommendations, explaining how the suggestions address the barriers to learning found in the interviews.

5.2.1 Isomorphic pressures on organisational learning practices

5.2.1.1 Analysis of the isomorphic pressures on organisational learning practices

Every organisation interviewed had a practice of learning from incidents and all had some form of security awareness training, which they believed would result in people reporting incidents to the internal security team. They all undertook analyses to determine the causes of incidents and produce lessons learned. This suggests there is a standardisation of practices driven by isomorphic pressures. Organisations often adopted cyber security practices under isomorphic pressures without evaluating

their effectiveness (Al-ma'aitah, 2022). Remarkably, despite widespread adherence to common practices, none of the organisations had evaluated the effectiveness of these practices for their specific contexts, highlighting the influence of isomorphic pressure. Although there were variations in how incidents were classified and selected for review, as well as in the allocation and tracking of actions, these differences do suggest some level of conscious adaptation or choice within the organisations.

Participants described significant coercive pressures that shape their learning practices. These pressures are beneficial in fostering a serious attitude towards cyber security incidents but adversely affect collaboration with suppliers and peers, as well as the scope of causes captured in reviews. A recent study by Arce et al. (2024) supports this finding, noting that organisations are cautious about documenting lessons learned due to fears of litigation. That study, focusing on US companies, cites a judicial ruling requiring Capital One to release a post-incident report by Mandiant to plaintiffs as a key factor contributing to this caution (Stone, 2020). Arce et al. (2024) highlighted the detrimental impact of such fears on industry-wide learning. Other global surveys by security firms confirm the tendency to keep incidents secret to avoid repercussions (Help Net Security, 2024; Security Magazine, 2023).

Many organisations follow industry standards and guidance, with cyber security frameworks incorporating steps for learning from incidents, as discussed in Section 2.1. Supply chain risks further motivate organisations to adopt and certify compliance with frameworks. In the UK, government procurement processes encourage adherence to Cyber Essentials and Cyber Essentials Plus certifications.[15] Participants perceived more mature organisations as possessing greater cyber security resilience, with maturity assessed against these standard frameworks. While these frameworks provide a degree of certainty amidst increasing threats and serve as a defence against criticism, they may not always represent the optimal approach for every organisation's circumstance but are at least defensible.

Normative pressures are evident as organisations consistently conduct post-incident reviews for their most serious incidents, although the classifications of high-severity incidents vary. Cavusoglu et al. (2015) suggested that the homogeneity of these practices is driven by normative pressures. Interviews revealed a standardised approach to producing post-incident reports with actions, a practice not deliberately designed but rather adopted as the default by legitimate organisations. Dimaggio and Powell (1983) explained that such practices arise as well-intentioned, rational individuals strive to professionalise their organisations, leading to consistency.

Mimetic pressures are also significant. Audit and Risk Committees often expect post-incident reports for serious incidents. Jeyaraj and Zadeh (2020) found that organisations adopt similar responses to manage uncertainty. In cyber security, where visibility into the effectiveness of others' practices is limited, this could lead to embracing sub-optimal practices. When organisations have suffered an incident, they want to demonstrate control despite the disruption. Following a standard process can be a mechanism for "social catharsis" (Boin & Hart, 2003). Tripathi (2022) suggested that organisations often emulate those they perceive as leaders in innovation as a strategy to accelerate their own development. This approach is particularly relevant in the realm of cyber security, where the swift escalation of threats compels organisations to rapidly adopt established practices from others, using imitation as an expedient means to remain responsive in a fast-evolving landscape.

Cavusoglu et al. (2015) found that regulators significantly influenced cyber security practices by setting expectations about reporting processes and actions, fostering similar practices across organisations.

[15] The Cyber Essentials and Cyber Essentials Plus schemes are UK government-backed initiatives to help organisations protect against cyber threats. Cyber Essentials provides basic certification, Cyber Essentials Plus includes an independent assessment https://www.ncsc.gov.uk/cyberessentials/overview.

For example, SEC,[16] ICO,[17] and NIS 2[18] have rules regarding the notification of data breaches. Westphal (1997) noted that interlocking directorships also promote the adoption of practices used by other organisations. Although all participants recognised the necessity of learning from incidents, it was evident that this had not been a prior focus. The normative and mimetic pressures lead organisations to go through the motions of learning from incidents without critically evaluating whether their specific practices yield the anticipated benefits.

5.2.1.2 Associated implications of the isomorphic pressures on organisational learning practices

Coercive pressures diminish the sharing of information and the capturing of incident causes during investigations. Without honest reflection and sharing, the conditions enabling incidents are unlikely to be addressed. By adopting practices followed by others without critically evaluating their efficacy in their own contexts, practitioners risk wasting resources on ineffective activities and missing opportunities for meaningful learning. For instance, while organisations standardise investigations for the most severe incidents, Ahmad et al. (2012) underscored the importance of considering the learning potential relative to an incident's severity, which might not always align with the highest severity categorisation.

Line and Albrechtsen (2016) advocated for organisations to adopt transparency and a non-blaming approach, resisting the inclination towards procedural proliferation to foster effective learning from incidents. The work of Heraghty et al. (2018) in safety incident investigations showed that investigation practices significantly influence future safety strategies, underscoring the importance of deliberately designing post-incident reviews to enhance the future strategy. Isomorphic pressures may cause organisations to view learning practices as merely indicative of learning having occurred. Argyris and Schön (1978) described “deuterolearning” as a continuous improvement approach that involves evaluating the effectiveness of learning processes, advocating for its adoption to enhance organisational learning.

5.2.1.3 Preliminary recommendation - Evaluate the effectiveness of the learning process

None of the participant organisations had explicitly assessed their ability to learn from incidents. Boin et al. (2008) emphasised that few organisations recognise the difficulty of drawing the correct lessons from an incident. Drupsteen (2014) highlighted that issues can arise at every step of the learning process. Without evaluating their learning practices, organisations remain unaware of areas which need improvement. Learning how to learn is a vital step in maximising the benefits of post-incident activities (Drupsteen, Groeneweg, et al., 2013). Margaryan et al. (2018) devised a toolkit to help organisations enhance their learning practices, explaining that adults need to engage in self-evaluation and be empowered to improve both their organisation's practices and their personal development.

---

[16] SEC Breach Notification Rules: According to the U.S. Securities and Exchange Commission (SEC) rules, public companies are required to disclose any material cybersecurity incident that could impact the company’s operations, financial condition, or reputation. Disclosure must be made within four business days of determining that the incident is material. This includes providing relevant details about the nature, scope, timing, and anticipated impact of the breach on the company’s financial performance and operations. See U.S. SEC Release No. 33-11138 (2023) for additional details.

[17] ICO Breach Notification Rules: Under the UK's Information Commissioner's Office (ICO) requirements, organisations must report data breaches involving personal data to the ICO within 72 hours of becoming aware of the breach, in accordance with the General Data Protection Regulation (GDPR). Organisations that fail to report in a timely manner may face significant fines. See GDPR Article 33 and ICO guidance on personal data breach reporting.

[18] Directive on Security of Network and Information Systems (NIS 2): NIS 2, adopted in 2022, enhances the EU's cybersecurity framework. It sets stricter security and reporting rules, including a 24-hour initial notification and full incident report within 72 hours, for essential sectors like healthcare, energy, and digital infrastructure.

The organisations interviewed prioritised learning from incidents classified as having high severity. When analysing the causes of incidents, organisations should evaluate whether their learning practices have been sufficient or if missed learning opportunities contributed to the incident. Without such evaluation, it is difficult to determine whether the investment in learning is effective or if additional investment is required. Rae and Provan (2019) cautioned organisations against mistaking the mere performance of a post-incident review as proof of learning. Baze (2021) used the capability model to underscore the need for organisations to enhance their capacity to learn from incidents. These insights highlight why it is recommended that the owner of the post-incident review process regularly evaluate the effectiveness of the learning process within their organisation.

Preliminary recommendation 1: Evaluate the effectiveness of the learning process
Regularly assess the efficacy of your organisation's incident learning process. Analyse incident trends to identify if prompt action on underlying causes could have prevented certain incidents. Evaluate the allocation of time and resources to the learning process, ensuring it receives adequate priority from teams throughout the organisation. If necessary, take proactive measures to optimise the organisation's learning from incidents.

5.2.2 Challenges of uncovering incidents

5.2.2.1 Analysis of the challenges uncovering incidents

Identifying incidents involves two crucial groups. Firstly, those within the company, where cultivating an internal culture that encourages open reporting is essential. Secondly, learning from incidents reported by external sources, such as suppliers, peers, or even customers, who may report incidents or suspicious activities. These external insights can offer valuable lessons. However, the willingness to share information (on incidents and lessons), both internally and externally, is often hampered by the fear of repercussions, the challenge of prioritising reporting amidst other responsibilities, and the practicalities of having appropriate mechanisms for sharing incident details.

The reluctance to report incidents is a well-documented issue across various domains, highlighting the significance of fostering a culture where discussing mistakes is encouraged. Research indicates that psychological safety is a foundation for open reporting and the exchange of ideas and concerns (Edmondson, 2004) Despite the limited exploration of this aspect within the cyber security field, Alotaibi et al. (2019) have drawn upon findings from safety research, which suggest several factors diminish an individual’s inclination to report. It is essential for individuals to feel that reporting an incident is safe and free from blame (Dekker, 2012; Drupsteen, Groeneweg, et al., 2013). Swuste et al. (2020) further clarified this point by asserting that "learning and blaming do not mix", highlighting a prevalent corporate tendency to focus on assigning blame rather than engaging in reflective analysis and reporting. Johnson (2002) argued for a culture where information is shared openly without fear of recrimination, where blame is assigned only when justified, thereby encouraging individuals to more readily accept responsibility.

Research has also investigated personal hesitations around admitting mistakes. Goffman (2003) highlighted how individuals continuously strive to manage others' perceptions by controlling the information shared with them. Brinsfield (2013) identified additional barriers beyond fear that prevent employees from speaking up, noting that managers with an "open door policy" might overestimate the effectiveness of their communication channels, as they are unable to hear the silence. Senge et al. (1999) cautioned that some employees, having spent extensive periods in environments dominated by fear, intimidation, and silence, find it difficult to imagine and create alternative, healthier workplace dynamics. Argyris and Schön (1978) discussed managers' fear of receiving feedback, pointing out their desire to avoid embarrassment, threats, and feelings of incompetence. Salviotti et al. (2024) observed

that managers, while intending to encourage open communication, may not due to the pressures of delivering more with fewer resources.

Johnson (2002) advocated for anonymous reporting systems to encourage individuals hesitant to voice concerns for fear of betraying colleagues. Leroy et al. (2012) suggested that leaders can foster a culture of reporting by prioritising safety and creating a psychologically safe workplace. This could potentially apply to cyber security where reporting is encouraged when an organisation has a culture of prioritising cyber security and fostering a psychologically safe workplace. Organisations that are under-resourced might unintentionally signal that they are too overwhelmed to address minor issues, which can discourage reporting and could lead to significant consequences if these issues escalate. Connolly and Wall (2019), in their study on ransomware, found that staff concerns about disciplinary actions and the pressures on IT teams can increase the likelihood of mistakes, potentially exacerbating the risk of incidents.

The suppliers' hesitation to report incidents experienced due to contractual obligations, regulations, and the threat of litigation has been less extensively explored. Schneier (2000) in *Secrets and Lies: Digital Security in a Networked World* (2000) contrasted the current state of security reporting with the efficacy of air safety reporting systems, highlighting the deficiencies in information security incident reporting. The success of aviation incident reporting systems has served as a model for other sectors—including rail, offshore operations, and healthcare—as noted by Johnson (2002). Despite the more established nature of safety incident reporting, under-reporting is still a significant issue, attributed not only to the fear of blame or being perceived as betraying colleagues but also to the lack of action in response to reported issues, as identified by Bishop (2003) and Sanne (2008).

In one of the few cyber security studies in this area, Ahmad et al. (2012) discovered that due to concerns of the repercussions, formal reporting of incidents was discouraged by senior leaders unless they saw benefit to the organisation through formal prosecution. A more recent study by Briggs et al. (2017) also highlighted ongoing challenges with poor incident reporting within the cyber security domain. Their findings suggest that individuals are more inclined to report issues if they perceive a personal benefit, though they recommend further research, given that their study was based on a small group of students participating in a simulated exercise.

For individuals to take action, they need to perceive it as worthwhile. They must recognise the importance of security and understand their role in maintaining the organisation's security. Specifically, in terms of incident reporting, they need to believe that their efforts in communicating an incident will result in meaningful action. This underlines the importance for organisations to provide updates to individuals who report incidents, detailing the investigation and resolution outcomes. For suppliers, it is crucial that their cooperation is acknowledged, fostering a trusted relationship. The utility of reporting must be evident to staff; otherwise, their likelihood of reporting future incidents diminishes. It is, therefore, vital that individuals who report issues receive consistent feedback on the status of their report. Johnson (2003) emphasised the importance of keeping staff "in the loop". For suppliers, learning may be hindered by differing resources available for learning and objectives that are not aligned between organisations (Friday et al., 2021). Hence, it is essential for organisations to ensure contract clauses with suppliers clearly define expectations and the consequences of sharing lessons.

Regarding reporting mechanisms, employees, customers, and suppliers must be clear on what incidents to report, whom they should notify, and when and what response they should anticipate. As Tan et al. (2003) indicated, the lack of a clear definition of what constitutes a cyber security incident could result in some anomalies being overlooked and not reported. For instance, organisations might expect a core supplier to report any near misses during their weekly calls and to contact the organisation immediately in the event of serious incidents, with the assurance of assistance in

response. For employees, these mechanisms are often outlined during training, but perceptions are also shaped by observations of how others are treated. In organisations employing a diverse workforce, including office personnel and field workers who may have limited access to IT, such as those in hospitality and construction, multiple reporting channels are necessary. For suppliers, distinctions may be made between key suppliers, who are crucial to operations, and those of lesser importance. Customer reporting should be straightforward, emphasising the importance of their notifications for their own security and that of others, especially if suspicious activities could be adapted by attackers to target other customers. The approach to achieving this will vary by industry and customer type, whether they are other corporations or individual consumers.

5.2.2.2 Associated implications of the challenges uncovering incidents

There is no chance for an appropriate response or learning opportunity if an incident is concealed by employees. This also deprives other employees of the chance to learn from their colleague's mistakes. Sveen et al. (2007) observed that effective learning leads to the detection of more incidents, creating a virtuous cycle of increased awareness and learning. Conversely, inadequate learning results in fewer reported incidents, establishing a vicious cycle of diminished learning effectiveness. It is crucial for practitioners to be aware of others' errors that led to incidents, as this understanding enhances the value seen in reporting their own incidents. This principle is vital both within organisations and within industries. Training employees to promptly report suspicious files, directories, or emails is crucial for early detection of incidents, as noted by Shaikh and Siponen (2023). Johnson (2003) cautions that encouraging reporting requires organisations to have the necessary resources to follow up on reported incidents adequately.

Being unaware of an attack on a supplier can leave an organisation vulnerable, either to the spread of the attack or to being unable to respond appropriately and timely if their data were compromised in an incident at a supplier's end. This also means the supplier might miss out on potential additional support or expertise in managing the incident. With stringent reporting obligations under regulations such as the SEC, ICO, and NIS2 rules, it is critical for organisations to be notified if an incident at a supplier involves their data. Lin et al. (2023) suggested that mutual support among suppliers in learning from incidents could enhance the resilience of the entire ecosystem.

Heinrich (1928) was arguably the pioneer in advocating for organisations to address minor incidents and near-misses as a strategy to mitigate the risk of more severe incidents. Dekker and Pruchnicki (2014) have argued that organisations can drift into failure, while Vaughan (2005) highlighted how they can increasingly normalise risk-taking. The value of near-miss reporting is well recognised in safety research, which has seen a significant increase in studies over the last decade (Gnoni et al., 2022). However, there is still no clear definition of what constitutes a near-miss or the most effective way to learn from such events (Gnoni et al., 2022; Trussler, 2020). Some regard near-misses as useful indicators of vulnerabilities that, once addressed, can avert more serious incidents (Azadegan et al., 2019; Fabiano & Currò, 2012; Krausmann & Necci, 2021). Azadegan et al. (2019) demonstrated that organisations could significantly learn from near-miss events, suggesting that these incidents provide valuable insights for improving organisational resilience and safety practices.

Therefore, the following two recommendations are put forward: First, demonstrate an openness to hearing about incidents by fostering an environment where reporting is encouraged and supported. This ensures that all employees feel secure sharing their experiences without fear of retribution, enabling a culture of transparency and trust. Second, promote knowledge sharing among peers and within the supply chain to enhance overall ecosystem resilience. This collaborative approach allows organisations to learn from each other and jointly mitigate risks, creating a more robust defence against future incidents.

5.2.2.3 Preliminary recommendation - Demonstrate an openness to hearing about incidents

Furnell (2008) explained that effective learning leads to more detected incidents and even greater learning, creating a virtuous circle. Conversely, poor learning results in fewer detected incidents and a vicious cycle of diminished learning. Building an environment receptive to incident reporting and learning from them can foster a culture of innovation. This openness to learning from incidents, including near misses, enhances an organisation's security posture and cultivates a mindset of continuous improvement among employees. However, a significant challenge is ensuring that all reports are acknowledged and acted upon, particularly in organisations with limited resources where prioritising and managing feedback can be overwhelming.

Johnson (2002) examined reporting systems in the UK rail and healthcare industries, which attempted to replicate the perceived success of aviation reporting systems. He identified concerns such as unrealistic expectations, inadequate investigations, and flawed identification of required actions. Sanne (2008) also identified limitations in incident reporting systems, noting that different etiologies shape both the classification of incidents and their reporting patterns. He observed that non-reporting is common when people do not see the benefits or fear social consequences like shame, blame, or disciplinary action.

Ballreich et al. (2023) highlighted the need to foster a culture that treats cybercrime victims benevolently. Instead of using the term "psychological safety" which may not be fully understood by all, the term "receptive responses" was used to denote openness to hearing reports and providing feedback to reporters. This decision was supported by research in 2023, which found that only 16% of over 200 HR directors correctly understood the meaning of "psychological safety" in a multiple-choice question (Dobra-Kiel, 2023). While many interviewees believed they had an open culture, they had not assessed it formally and noted that some suppliers failed to inform them of incidents. Assessing the willingness to report incidents was thus incorporated into the recommendation. Johnson (2003) cautioned that an increase in reported incidents may be due to either a genuine rise in incidents or improved reporting practices.

Incidents can be reported by customers, employees, peers, and suppliers. Organisations must find effective ways to manage this process by leveraging technology, streamlining reporting mechanisms, or seeking external support. This will help ensure that the cycle of reporting, learning, and improvement becomes sustainable. Multiple reporting channels should be established to cater to various stakeholders, including non-office-based workers and small suppliers, and these channels must be clearly communicated to ensure awareness.

This is why it is recommended that organisations demonstrate an openness to hearing about incidents and actively check for barriers to reporting. Ensuring that employees, customers, peers, and suppliers feel comfortable sharing their experiences without fear of blame or disciplinary action is essential. By fostering a culture that encourages transparency and continuously assessing potential obstacles, organisations can identify and remove barriers to incident reporting. This inclusive approach helps maintain a continuous cycle of learning and improvement that strengthens the organisation’s overall security posture.

Preliminary recommendation 2: Demonstrate an openness to hearing about incidents
Organisations should foster a culture that encourages incident reporting by customers, employees, peers, and suppliers. This can be achieved through various means, such as establishing multiple reporting channels, formalising contracts and policies, providing training, facilitating discussions, and demonstrating receptive responses to shared incidents. Assessing stakeholders' understanding and motivation to report incidents can help identify knowledge gaps and improve reporting practices.

5.2.2.4 Preliminary recommendation - Promote knowledge sharing with peers and supply chain

For post-incident activities to be effective, the lessons must be disseminated beyond the immediate post-incident review meetings. However, researchers like Ahmad et al. (2012), and He and Johnson (2017) discovered that post-incident reports are often not shared widely and are not fully comprehensible to those outside the incident response teams. He, Johnson, Lu, et al. (2014) found that these reports typically provide little analysis of causal factors and are not presented in a useful format. Moreover, organisations may hesitate to share sensitive details within these reports out of concern that such information could be exploited by malicious insiders. Limiting the distribution of sensitive findings is often necessary to mitigate the risk of those with internal access misusing the information to launch future attacks or manipulate systems. While the balance between transparency and security is challenging, it is essential that reports are accessible enough to facilitate learning while protecting against unintended misuse.

Each organisation can benefit from learning lessons from others, as they will receive more insights if they share their own. Line et al. (2006) highlighted the importance of sharing lessons across all organisational levels, including suppliers and contractors and emphasised the need for organisations to strengthen collaboration with their industry peers and suppliers to bolster resilience against cyber-attacks. Similarly, Lin et al. (2023) noted that sharing learning practices and incident experiences reinforces the resilience of organisational networks. However, Tan et al. (2003) discovered that, in certain industries, organisations fear their incident reports to authorities may be used against them.

Many industries have confidential information-sharing forums, such as the National Cyber Security Centre (NCSC) Trust Groups[19] and the Financial Services Information Sharing and Analysis Center (FS-ISAC).[20] Over-reliance on legal terms in contracts may lead to defensiveness, which can hinder collaboration. Trust is crucial for information-sharing, and it develops over time through relationship-building. Organisations should consciously cultivate strategic supplier relationships rather than assuming they will evolve naturally. Ryciuk and Nazarko (2020) explained that trust in relationships is partly based on shared experiences of cooperation, where partners exchange information and insights. A willingness to share cyber incident information with partners can even enhance relationships with strategic IT vendors, which provides broader benefits to the IT function. Knight and Nurse (2020) found that blaming suppliers, as Ticketmaster did following their 2024 security breach, can lead to negative perceptions of the attacked organisation.

While concerns about confidentiality, reputational risk, and potential legal consequences may make organisations hesitant to share lessons from incidents, these challenges should not prevent them from finding ways to do so in a controlled and constructive way. The risks associated with transparency can be mitigated through structured frameworks that allow organisations to exchange valuable insights while protecting sensitive details. Encouraging an environment where learning from incidents is prioritised—through trusted industry forums, anonymised reporting mechanisms, and carefully structured legal agreements—can help alleviate fears of negative repercussions. By proactively addressing these barriers, organisations can strengthen relationships with key partners, improve their own incident response capabilities, and collectively enhance cyber resilience.

---

[19] The NCSC Trust Groups are collaborative forums that bring together experts from government, academia, and industry to share threat intelligence and cyber security best practices. Established to foster open communication and trust, these groups support the collective resilience of organisations across various sectors in the UK.

[20] Financial Services Information Sharing and Analysis Center (FS-ISAC): This is a global forum where financial institutions share cyber threat information and best practices confidentially to enhance collective security. FS-ISAC serves the banking sector by facilitating trusted communications and providing a secure platform for members to report and discuss cyber threats.

Preliminary recommendation 3: Promote knowledge sharing with peers and supply chain
Engage in active participation and foster a culture of sharing lessons learned with peers and suppliers. Encourage the dissemination of valuable insights from near misses, low-severity incidents, and more significant events. Emphasise collaboration and assistance rather than resorting to contractual penalties when working with suppliers. Cultivate trusted relationships by promoting openness and, where appropriate, establish legal frameworks that facilitate the sharing of non-competitive information. Support the establishment of local and industry groups facilitated by government and security agencies, such as the National Cyber Security Centre (NCSC) Trust Groups, to enable collective learning and collaboration.

5.2.3 Challenges of identifying the causes

5.2.3.1 Analysis of the challenges of identifying the causes

Organisations reported opportunities to improve their identification of underlying causes. A significant challenge arises from the limited availability of the right personnel, as teams are often stretched thin. The emotional toll of incidents also discourages individuals from investing time in comprehensive analyses. Consequently, conducting post-incident reviews is reserved for only the most significant incidents to prioritise the use of resources. Despite recognising the value of regularly reviewing incident data to identify trends and assess the effectiveness of controls, many organisations lack the available resources with the required data analytical skills.

Participants highlighted the benefits of involving business leaders and other stakeholders in post-incident reviews to elicit better actions and ensure greater ownership. Vastveit et al. (2015) observed variability in the underlying causes and actions suggested by individual incident managers during post-incident reviews at a refinery. A robust post-incident review should include individuals with divergent thinking skills, as homogeneity in thinking can lead to overlooked or excluded evidence, concentrating only on familiar factors or preconceptions about causes (Bishop, 2003).

The composition of participants during a review shapes the analysis and the lessons drawn. Both Ahmad et al. (2012) and Jaatun et al. (2009) recommended broadening participation in the review process. Interviewees also stressed the importance of involving business leaders to grasp the broader context and priorities, and those who possess a comprehensive view across teams and an understanding of historical decision-making that may have contributed to the incident. In healthcare settings, post-incident activities include listening to individuals describe their actions and feelings during the incident, acknowledging that people generally follow expected procedures, yet a confluence of factors often creates the conditions for incidents (Edmondson, 2018).

Only two organisations from those interviewed had specialised teams with defined methods for identifying causes and lessons. Research by Papastergiou et al. (2019) criticises current approaches for their inadequacy in revealing the underlying causes of cyber security incidents. Further research indicates that organisations are prone to attributing simplistic causes and lack deep insights into contributory conditions (Jaatun et al., 2009; Shedden et al., 2010, 2011). Jaatun et al. (2009) found an excessive focus on technical issues, with organisational and human factors often overlooked. Renaud and Goucher (2012) observed that blaming non-compliance by users is a convenient way for organisations to move past an incident without addressing deeper issues.

Cyber security research frequently represents incident causes as being due to “human error”—industry surveys report that 42% to 80% of cyber security incidents are attributed to human mistakes (Evans et al., 2019). However, these statistics often lack clarity on how incidents are determined to result from “human error” so this may oversimplify the underlying causes. Heraghty et al. (2018)

argued that, despite widespread academic recognition that incidents typically arise from complex system interactions, many reports still cite “human error” as a primary cause. Cook (1998) emphasised that incidents are rarely the result of a single root cause; instead, they emerge from multiple contributing factors, where no single failure on its own is sufficient to cause the incident. In contrast to the traditional engineering paradigm prevalent in cyber security, Shaty (2021) advocated for recognising the complexity of IT systems. These systems, supplied by a variety of vendors and embedded within complex organisational processes, give rise to a network of decisions and interactions that, rather than isolated human mistakes, collectively lead to incidents.

By comparing reviews from three official public reports on the same event, Wrigstad et al. (2017) demonstrated how causes are constructed. They noted that none of the reports discussed the interaction between humans and technology, tending instead to attribute incidents to staff behaviour rather than to the work environment that encouraged such behaviour, and they caution that simply replacing individuals does not address the real causes that influence behaviour. Catino (2008) noted a reluctance during post-incident reviews to explore the underlying conditions that led to human choices.

Rasmussen (1998) warned that the goals of individuals conducting post-incident reviews influence the information sought, whether to allocate responsibility or to identify system improvements. The learning derived depends on the context, as different groups may choose various timeframes and focus on different aspects of the incident (Tamuz et al., 2011). Johnson (2002) cautioned that those investigating incidents may limit their examination of potential causes to what they expect to see, which can be mitigated by appropriate investigatory techniques.

Without methodologies or skilled facilitators, people may avoid confronting shortcomings in their own decision-making processes, as the contributory causes are ambiguous and distributed across multiple teams, making it easy to evade accountability. NIST Special Publication 800-61 Revision 2 suggests the use of skilled facilitators. However, as Meyer and Rowan (1977) observed, employing external consultants sometimes serves more to enhance the perceived legitimacy of a process than to add direct value.

The CREST guidance (Creasey, 2013) elaborates on causal analysis techniques, recommending various tools such as Failure Mode and Effects Analysis (FMEA), Current Reality Tree (CRT), Fault Tree Analysis, the Five-Whys Approach, Why-Because Analysis (WBA), and Cause-and-Effect (Fishbone) Diagrams. Some theorists argue that these tools are too mechanistic and fail to account for the complexity and interactions that can enable incidents (Hollnagel et al., 2006; Leveson, 2004). Rasmussen’s (1997) hierarchical socio-technical framework, AcciMap,[21] and Leveson’s (2004) Systems-Theoretic Accident Model and Processes (STAMP) model offer more systemic approaches encouraging a broader consideration of factors contributing to an incident. Salmon et al. (2012) found STAMP suitable for classifying technical control failures but less effective for complex human decision-making and organisational contributory causes, whereas AcciMap was a useful tool for analysing incidents with multiple causes but difficult to aggregate and summarise to identify patterns. The adoption of even basic tools in analysing the causes of cyber security incidents would represent progress for many organisations. Evans et al. (2019) noted that once organisations begin investigating the underlying causes of cyber security incidents, using the methods from the safety field, many more human causes are revealed.

[21]AcciMap derives from "Accident Mapping" as the framework visually represents how decisions and actions at different hierarchical levels contribute to risks and incidents. The Accimap framework has since been widely adopted and extended, building on Rasmussen's original 1997 model (Waterson et al., 2017).

In safety research, biases in analysing incident causes have been extensively explored (Bishop, 2003). These include hindsight bias, where facts evident after the incident are assumed to have been apparent beforehand; political bias, where the views of one individual or organisation are given undue weight due to their status; sponsor bias, where the investigator has responsibilities that could be impacted by the analysis; professional bias, where investigators avoid questioning the performance of fellow professionals or their own professional bodies; recognition bias, where investigators identify causes that are most familiar to them; and confirmation bias, where analysts interpret evidence to support pre-determined hypotheses. Johnson (2002) discussed the challenges of understanding causes due to Hausman's causal asymmetry,[22] where it is difficult to trace back from an incident to its cause.

Morrison and Milliken (2000) noted that often employees are aware of issues but fear voicing the truth to their leaders. Grispos (2016) explains that understanding the causes of cyber security incidents requires an open, honest, and accountable culture that acknowledges human fallibility. Conklin (2016) suggests that, to better understand the underlying causes, post-incident reviews should focus on how incidents occurred rather than why. He et al. (2022) recommended asking questions such as “What went wrong?”, “What went well?”, and “What could be improved?” to help identify the root causes of incidents and develop more targeted actions for future improvement. Lindberg et al. (2010) found a lack of evidence from studies about the effects of various methodologies and organisational structures for understanding the causes of incidents, which has hindered prevention of future incidents.

The lessons from post-incident reviews are typically captured in some form. How these lessons are discussed and distributed within organisations varies. In some cases, these are captured only in incident reports held by the management team. For most organisations, a report is issued and distributed to specific groups. No participants mentioned whether they had verified if the reports met their stakeholders' requirements, although several discussed them as part of regular governance forums. He and Johnson (2017) found that post-incident reports were often not easily understood by those outside the cyber security function, and stakeholders needed assistance to digest the findings.

5.2.3.2 Associated implications challenges of identifying the causes

Organisations may not involve the most appropriate individuals in their post-incident reviews, limiting the scope of causes considered, as different stakeholders bring varied perspectives. If only the incident response team is involved, the lessons may be restricted to technical findings and improvements to the response process, without considering broader, more far-reaching lessons. If the participants in the post-incident review are not carefully chosen, they may focus more on moving on from the incident than on adopting a curious mindset to explore the causes. This can also mean that other groups required to implement recommendations may not feel ownership of the lessons if they have not been involved in the review and do not understand their importance. Organisations are not giving sufficient thought to how the outcomes of post-incident reviews are absorbed by the organisation and whether their format is effective. Without this verification, there is no way to ensure that the lessons are adopted.

Without specified techniques or the use of trained facilitators, it is likely that only technical causes will be considered, or incidents will be blamed on “human error”. Renaud (2012) found that blaming users was convenient but meant that organisations did not investigate whether their expectations were appropriate given the resources they had provided. Other underlying issues that could have contributed will not be explored, such as legacy infrastructure, governance issues, or management of suppliers. Vastveit et al. (2014) found that safety post-incident reviews focused on the immediate

[22] Hausman’s causal asymmetry refers to the idea that causes explain their effects, but effects do not explain their causes. This principle, outlined by Hausman (1998), underscores the directional nature of causal relationships and is fundamental to distinguishing causation from correlation.

causes and rarely identified causes outside their own teams, which meant that underlying issues, such as resourcing and skills, were not being tackled. They recommend that those conducting post-incident reviews should be given training to help identify underlying causes. Fiol and Lyles (1985) found that organisations which only performed single-loop learning tended to be lower-level learning organisations focused on routines or rules. This can leave organisations identifying low-severity lessons, such as changes to policies or processes, which can add to the workload without really making a difference to the cyber resilience of the organisation. Such an approach risks only narrow lessons being learned and only specific issues being addressed, which leaves an organisation vulnerable to similar incidents in the future.

Organisations that are not reviewing lower severity incidents (i.e. ones they do not conduct post-incident reviews for) are missing out on identifying patterns that could indicate systemic causes. This may mean they are slow to respond to emerging trends that necessitate a pivot in how they tackle the risks. It could also trap them in a cycle of responding without addressing the underlying causes (Gonzalez, 2005). This could result in an inefficient use of resources and a negative reinforcing cycle until a serious incident occurs.

The analysis above makes clear the need for two crucial recommendations. Firstly, organisations should ensure effective participation in post-incident reviews. Involving the right stakeholders with diverse perspectives in these reviews helps expand the range of potential causes considered, providing a more comprehensive understanding. Engaging key personnel, business leaders, and other stakeholders creates a sense of ownership, encouraging them to contribute constructively to post-incident evaluations. This participation ensures that the lessons learned are shared, understood, and effectively integrated into future security strategies.

Secondly, organisations must delve into underlying causes and trends. By moving beyond superficial analyses and avoiding simplistic attributions such as “human error”, organisations can identify systemic issues that are often the true roots of incidents (beyond merely the technical aspects). Deep investigations can reveal patterns and trends that may highlight the need for strategic pivots in risk management. This enables organisations to escape the reactive cycle of only addressing immediate technical fixes and instead allows them to develop long-term, strategic measures that bolster overall cyber resilience.

5.2.3.3 Preliminary recommendation - Ensure effective participation in post-incident reviews

Several interview participants emphasised the importance of involving business leaders in incident investigations to fully understand contributory causes and gain their insight and ownership of lessons learned. Barton et al. (2016) found that greater senior management involvement in cyber security led to better organisational assimilation of security needs. Lukic et al. (2010) argued that learning must involve not only the workers directly performing the tasks but also management, ensuring that leaders have the opportunity to challenge systemic issues. Line (2015) noted that including various groups in post-incident reviews brings diverse perspectives and enhances the understanding of security. Such diversity in participants can help address biases identified by Bishop (2003) while fostering richer idea generation for lessons learned.

These findings underscore the importance of the recommendation to ensure effective participation in post-incident reviews. By involving key stakeholders with seniority and authority, organisations can gain comprehensive insights into the causes and potential remedial actions. It is the responsibility of the Head of Incident Management, or whoever is arranging the post-incident review, to ensure that participants with the appropriate seniority are present to make authoritative decisions and influence change. Participants with the appropriate attitude, social skills, and a collaborative mindset will strengthen the review process (Zietsma et al., 2002). Finally, discussing post-incident reports in

impactful governance forums ensures that their findings are understood and drive meaningful improvement actions across the organisation.

Preliminary recommendation 4: Ensure effective participation in post-incident reviews
Facilitate the involvement of key stakeholders in post-incident reviews to gain comprehensive insights into the causes and potential remedial actions. Engage individuals with seniority and authority to enact necessary changes. Consider participants with the right attitude, social skills, and a collaborative mindset. Ensure that post-incident reports are discussed in impactful governance forums, where their findings and recommendations can drive meaningful actions and improvements.

5.2.3.4 Preliminary recommendation - Delve into underlying causes and trends

Each organisation has its own culture and level of maturity in investigating the causes of incidents. Rollenhagen et al. (2010) found that few organisations had dedicated incident investigators, and those responsible for investigations often lacked training. As a result, investigation methods varied between organisations, leading to inconsistent and incomplete identification of potential causes. Lundberg et al. (2009) highlighted that investigation manuals often reflect organisational assumptions about how incidents occur. While these manuals can provide a valuable framework for beginners or act as a reference for experienced facilitators, their rigid structures can limit creative thinking in novel situations (Klein, 2009).

Argyris (1999) argued that effective learning requires hard data, explicit inferences, and publicly testable conclusions. Alternatively, Catino (2008) suggests that no single, ultimate cause exists for incidents, which result instead from dynamic interactions within a system. Vastveit et al. (2015) found that individual managers tended to shift blame onto other departments for incident causes. Street and Ward (2019) discovered that assigning people specific roles in a meeting can alter their decision-making criteria. This suggests that appointing individuals as facilitators focused on uncovering underlying causes may lead them to act differently than they would in their usual operational role.

Organisations can determine the most suitable investigation procedures by understanding what techniques are favoured for other investigations within the organisation, such as those used for safety or fraud, as stakeholders are often already familiar with these methods. However, it is equally important to evaluate whether these existing approaches are effective for cyber security incidents. While leveraging familiar techniques can help streamline investigations, trying a new approach specifically tailored to cyber security incidents could be beneficial and may later be expanded to cover other types of incidents. What is essential is that organisations consciously assess the effectiveness of their analysis of the cause of incidents and adapt them to improve outcomes.

Organisations can benefit from guidance on how to investigate incidents, provided that such frameworks align with their culture and ways of working. Heraghty et al. (2018) called for more research into post-incident analysis to offer practitioners better guidance. Therefore, this recommendation refrains from prescribing specific investigation procedures. Instead, it emphasises the need for organisations to determine the most suitable approach for investigating incident causes and identifying contributory factors, whether through trained facilitators, specialised tools, or external parties. These techniques can encourage a broader evaluation of contributory factors and potential lessons.

Delving deeply into underlying causes and trends helps reveal systemic factors, such as accountability gaps, legacy infrastructure, or process inefficiencies that, when addressed, can prevent future incidents. Moreover, analysing lower-level incidents can reveal emerging trends and patterns, enabling organisations to refine their strategies and reduce the risk of recurrence. Moreover, analysing lower severity incidents can reveal emerging trends and patterns, enabling organisations to refine their strategies and reduce the risk of recurrence.

Preliminary recommendation 5: Delve into underlying causes and trends
Determine the most suitable approach for investigating incident causes and identifying contributing factors. This may involve leveraging a trained facilitator, employing specific tools or techniques, or engaging a specialised unit or external party. These methods can help reveal contributory factors that, when addressed, have the potential to prevent future incidents, such as process inefficiencies, accountability gaps, legacy infrastructure, governance issues, prioritisation challenges, supplier relationships, or monitoring tool deficiencies. Additionally, analyse lower-level incidents to identify emerging trends and patterns.

5.2.4 Challenges of implementing the lessons

5.2.4.1 Analysis of the challenges of implementing the lessons

This challenge is intricately linked to the previous discussion on identifying causes. As described by Lundberg et al. (2010), the principle of "what-you-find-is-what-you-fix" is not always true and it can often limit organisational responses. Participants admitted that the fear of being held accountable for implementing challenging actions deters the recording of lessons, especially those connected to more structural issues like poor IT architecture or a reckless organisational culture. Lundberg et al. (2010) cautioned against assuming a straightforward rationality from causes to remedial actions, as people tend to limit their commitments to feasible solutions. This was evident in the comprehensive action tracking processes described by participants, where there was a notable hesitation to identify lessons that might be challenging to fully resolve.

Industry standards such as NIST Special Publication 800-61 Revision 2 and ISO 27035-2 generally assume that once lessons are identified, they will be implemented. However, these standards do not explicitly address the management and testing of these implementations. The latest version of the NIST Cyber Security Framework 2.0 notably adds a new overarching governance function to the existing framework components—Identify, Protect, Detect, Respond, and Recover. This addition urges leaders to foster a culture of accountability and continuous improvement and recommends collaborative, lessons-learned sessions with critical suppliers—although it stops short of explicitly governing the implementation of these lessons.

The distinction between the mere identification of lessons and their actual implementation has been explored by researchers like Edmondson (2002) and Elliott and Macpherson (2010), who argued that true learning only occurs when lessons are successfully implemented, transforming organisational practices (Duchek et al., 2020). Similarly, Lindberg et al. (2010) asserted that genuine risk modification only occurs once recommendations are enacted.

Interviewees cited the lack of skilled resources, time, and funding relative to other priorities as major impediments to implementing lessons. They believed it is challenging to prioritise investments in cyber security when returns are not easily quantifiable and senior leaders lack a comprehensive understanding of cyber risks. However, Demjaha et al. (2019) found that companies often increase their cyber security investments significantly following a major incident, although linking these investments directly to the lessons learned can be elusive. This suggests that investments may be more

about demonstrating that security is being taken seriously after an incident than addressing specific vulnerabilities identified in post-incident reviews.

Another challenge lies in ensuring that actions are not only implemented but are also effective against the identified risks. Participants noted a greater emphasis on demonstrating that actions were completed rather than directly testing their effectiveness in mitigating risks. This echoes findings by Drupsteen et al. (2013) for safety incidents, where the focus was on completion rather than the efficacy of actions in preventing future incidents. Where testing occurred, it was typically limited to technical controls rather than broader actions such as user training effectiveness.

Nevertheless, some interviewees felt that lessons were implicitly tested by the absence of repeat incidents or through general testing and audits which might indicate unresolved issues. Yet admissions were made that some organisations experienced repeat incidents because actions had either not been implemented due to competing priorities or had degraded over time as the memory of the incident faded. This suggests that actions were not implemented sustainably or that addressing cyber security risks was not prioritised within the organisation. Drupsteen et al. (2013) and Vastveit et al. (2015) highlighted that the opportunity for learning is often lost during the reporting and evaluating stages, where organisations fail to maintain focus on implementing recommended measures.

5.2.4.2 Associated implications of the challenges of implementing lessons

Unless leaders promote a culture of tackling challenging causes, those involved in incident reviews may only identify causes and actions they believe are manageable. Robust action tracking systems may inadvertently communicate an expectation that individuals will demonstrate completion of actions, leading to a focus on easily addressable lessons rather than those that are most critical for enhancing organisational security.

Addressing significant lessons often requires sustained senior sponsorship, as these efforts may necessitate multiple attempts over time to effectively address the root causes of incidents. Without such encouragement and recognition of progress, teams may abandon the arduous task of addressing systemic issues in favour of simpler, more urgent activities. As Edmondson (2023) explained, while it may seem straightforward for leaders to recognise and champion the resolution of systemic problems, in practice, it is quite challenging.

If organisations fail to evaluate whether implemented actions have genuinely enhanced cyber resilience, they risk recurring similar incidents. This prevents them from assessing the effectiveness of their learning practices and continuously improving their incident response strategies. Argyris's and Schön's (1978) concept of "in-deutero learning" (learning to learn), highlighted the importance of assessing the impact of lessons to avoid wasteful practices in post-incident reviews that do not effectively enhance security. This ties back to the initial theme of isomorphic pressures influencing organisational learning practices, where evaluating the effectiveness of lessons can aid organisations in refining their learning processes.

The analysis above emphasises the need for two crucial recommendations. First, organisations must champion the effort to address structural causes of incidents. This requires leadership to set the agenda, promoting a culture that values tackling systemic issues even if they appear less tangible, such as technical debt of legacy systems or ingrained cultural problems. It also means empowering individuals to take personal accountability and pursue these challenging goals while providing sustained support and recognition of progress.

Second, organisations need to drive the implementation of lessons and conduct rigorous testing to ensure effectiveness. This involves developing action registers and tracking forums that monitor

progress and identify obstacles, along with testing methodologies like red teaming[23], simulation exercises, and internal audits. Testing should not be limited to technical controls but extend to verifying new governance structures and ensuring adherence to updated training. Together, these recommendations will help organisations bridge the gap between identifying lessons and actually implementing them.

5.2.4.3 Preliminary recommendation - Champion addressing structural causes

Individuals often avoid addressing structural causes, particularly if they anticipate being blamed for unsuccessful outcomes. It is essential for leaders to clearly communicate the expectation of tackling these deep-rooted issues. Leaders must first acknowledge the need for change, which may be more readily accepted by new or recently promoted leaders who can attribute existing problems to their predecessors (Boin et al., 2008). Furthermore, leaders should not only allocate the necessary resources to address structural causes but also foster an environment where such efforts are expected, understood to require time, and acknowledged even if they initially fail. This approach is necessary to prevent post-incident reviews from becoming mere rituals and the subsequent lessons learned reports from turning into what Elliott and Macpherson (2010) described as "fantasy documents"—created to give an illusion of learning rather than genuinely addressing the shortcomings that facilitated the incident and the challenging issues that need resolution to prevent future occurrences.

Furthermore, leaders should create clear goals and provide a supportive atmosphere that mitigates the fear of blame, allowing employees to take direct accountability (Vakola & Bouradas, 2005). It is vital that leaders recognise all progress, including understanding which strategies do not work, as valuable learning outcomes (Cannon & Edmondson, 2005). Hekneby and Olsen (2024) have found that, in organisations where learning is effective, leaders encourage experimentation and continuous improvement, acknowledging that real progress may require time and multiple attempts. This persistence in recognising and learning from each step is vital for successfully addressing and resolving structural causes.

Preliminary recommendation 6: Champion addressing structural causes
Leadership should emphasise the importance of addressing structural causes of incidents, even when the actions required may be less tangible, such as addressing cultural issues or resolving long-standing technical debt. This is particularly crucial in cases where individuals may be hesitant to take personal accountability for an incident as they cannot guarantee closure. Handling the expectation of addressing structural causes will vary depending on the organisation's maturity and size, but it requires senior leadership to set the agenda and recognise progress.

5.2.4.4 Preliminary recommendation - Drive the implementation of lessons and testing

The understanding of what went wrong during an incident is merely the initial step in the learning process. The real transformation occurs when these insights lead to tangible changes within the organisation (Duchek et al., 2020; Evenseth et al., 2022; Lindberg et al., 2010). However, the challenge often lies in the follow-through. Vastveit et al. (2015) noted the difficulty organisations face in monitoring the progress of implementing lessons once the immediate impact of the incident fades.

To address this gap, it is crucial to establish robust mechanisms for tracking and validating the effectiveness of corrective actions. While traditional standards and procedures from bodies such as the Institute of Internal Auditors (IIA) and the American Institute of Certified Public Accountants (AICPA) focus on auditing internal activities, financial reporting, and assurance services, they also underscore the importance of testing the effectiveness of actions taken to address findings. Although

[23] Red teaming involves assembling a group of experts who adopt the tactics and perspective of potential adversaries to test the organisation's security measures.

these organisations may not specifically mention innovative testing methods like red teaming or simulation exercises, these practices are invaluable in confirming lessons have been learned and improvements made to an organisation's security posture.

By simulating real-world attack scenarios, red teaming helps identify weaknesses or gaps in the organisation's response strategies derived from post-incident reviews. Similarly, simulation exercises create realistic scenarios that are particularly effective for testing lessons about improving an organisation's response and recovery to incidents. This helps refine its preparedness and response capabilities. Additionally, internal auditors can play a vital role by testing both technical and non-technical actions, such as verifying the functionality of new governance structures or ensuring adherence to updated training protocols, to confirm their effectiveness.

Furthermore, internal auditors can play a critical role by verifying that corrective actions are not only implemented but are also functioning as intended and adequately address the causes of the incident. This comprehensive approach ensures that the organisation not only responds to past incidents but also enhances its resilience against future threats. By establishing such rigorous testing and tracking mechanisms, organisations can ensure lessons learned are demonstrable improvements.

Preliminary recommendation 7: Drive the implementation of lessons and testing
Ensure the actions identified in post-incident reviews are followed through and actually implemented. Depending on the organisation, establish suitable action registers and tracking forums to monitor progress and overcome any obstacles that arise. Additionally, it is important to conduct appropriate testing to validate that the implemented actions effectively address the identified causes. This can include activities such as red teaming, simulation exercises, or internal audit testing. It is equally important to test non-technical actions, such as verifying the proper functioning of new governance structures and ensuring adherence to updated training guidance.

5.3 Chapter conclusion

This chapter contributes to addressing RQ3, that explores what new approaches can be recommended to improve learning from cyber security incidents. While it lays the foundation by analysing themes from practitioner interviews and developing preliminary recommendations, RQ3 will only be fully addressed after the validation steps discussed in the forthcoming chapter. Table 12 provides a summary of the themes and the preliminary recommendations developed from the analysis. This table serves as a quick reference to understand how each theme has been addressed throughout the chapter.

Table 12 *Themes, associated implications and preliminary recommendations*

Themes	Preliminary recommendations
Isomorphic pressures on organisational learning practices	1. Evaluate the effectiveness of the learning process
Challenges of uncovering incidents	2. Demonstrate an openness to hearing about incidents 3. Promote knowledge sharing with peers and supply chain
Challenges of identifying the causes	4. Ensure effective participation in post-incident reviews 5. Delve into underlying causes and trends

Themes	Preliminary recommendations
Challenges of implementing the lessons	6. Champion addressing structural causes 7. Drive the implementation of lessons and testing

The preliminary recommendations advocate for establishing a proactive learning environment, emphasising openness in incident reporting, fostering a culture of transparency and trust, and enhancing knowledge sharing within and beyond organisational boundaries. This approach is vital for strengthening overall cyber resilience. The importance of involving a diverse range of stakeholders in post-incident reviews is also highlighted, showing that effective participation is critical for a comprehensive understanding of incident causes. Additionally, the chapter underscores the need to delve into underlying causes and trends, enabling organisations to move beyond immediate fixes and develop strategic long-term responses. Strong leadership is required to champion these efforts and to track their effectiveness, ensuring that they adequately address the root causes. Furthermore, the necessity for organisations to ensure the thorough implementation and testing of corrective actions is addressed.

In conclusion, this chapter presents the initial recommendations aimed at enhancing learning-from-incidents practices. These recommendations provide a basis for the subsequent empirical validation, which is essential to confirm their effectiveness and applicability in the real-world cyber security landscape. Chapter 6 will detail this process through a Delphi study with cyber security practitioners, aimed at refining and substantiating the strategies proposed in this chapter.

6 Validation of recommendations through a Delphi study

To address RQ3, "What new approaches can be recommended to improve learning from cyber security incidents?", this phase of research expanded on the preliminary recommendations outlined in Chapter 5, Section 5.2, with the goal of validating them. This was achieved through a Delphi study, which sought to confirm these recommendations by gathering insights from professionals with real-world experience in organisational learning from cyber security incidents.

This chapter explores the details of the Delphi survey, covering its implementation and subsequent analysis. A full introduction to the Delphi method, outlining its historical context and its relevance in addressing the research questions of this study was discussed in Chapter 3. In this chapter, we explain how this study applied the Delphi research technique, outlining participant recruitment, survey design, response rates, consensus levels, and the evolution of recommendations based on participant feedback. Major themes are examined, findings are compared with existing literature and theories, and any disagreements among participants discussed. The updated recommendations, practical implications, and participant feedback are presented, followed by a discussion on the implications of the findings, the limitations, generalisability, and potential areas for further research.

6.1 Delphi study methods

6.1.1 Design of the Delphi study

This Delphi survey consisted of two rounds, each designed to refine and validate the preliminary recommendations developed in the prior research phase. Recent cyber security Delphi studies, such as those by Chaudhary (2024) and Goode et al. (2018), have also used two rounds, demonstrating its practical effectiveness in refining consensus without overburdening participants. There is no consensus on the ideal number of rounds, as studies use this technique for different purposes. Linstone et al. (1975) found three rounds to be the most effective in their study, where the first round gathered initial input followed by two rounds of scoring. They suggested additional rounds might hinder results. Keeney et al. (2006) suggested an open-ended first round might place a strain on participants to complete the survey and, as this study sought the views of senior and busy practitioners, an open-ended first round was not deemed suitable. McKenna (1994) labelled Delphi surveys where an initial input from literature or a prior research phase is provided as “reactive Delphi”. A similar modification has been suggested by other scholars (Hanafin, 2004; Hardy et al., 2004; Keeney et al., 2006). Two rounds also have the advantage of not forcing respondents to feel pressured into agreeing just so they can stop receiving future surveys to complete. Additionally, this study already possessed the valuable data and themes gathered from the interviews, making the second round in this study essentially equivalent to the third round in the Linstone et al. (1975) study. Therefore, the Delphi survey was structured into two rounds, striking a balance between potential dropout rates and achieving a higher level of consensus.

In the Delphi study, participants were encouraged to reflect on the feedback and results from the first round during the second round, allowing them the opportunity to revise their opinions based on the group’s collective insights. This iterative process is a key feature of the Delphi method, as it fosters deeper reflection and can lead to more refined consensus. Therefore, it was expected that participants might change their minds between rounds as they engaged with the feedback provided by other respondents.

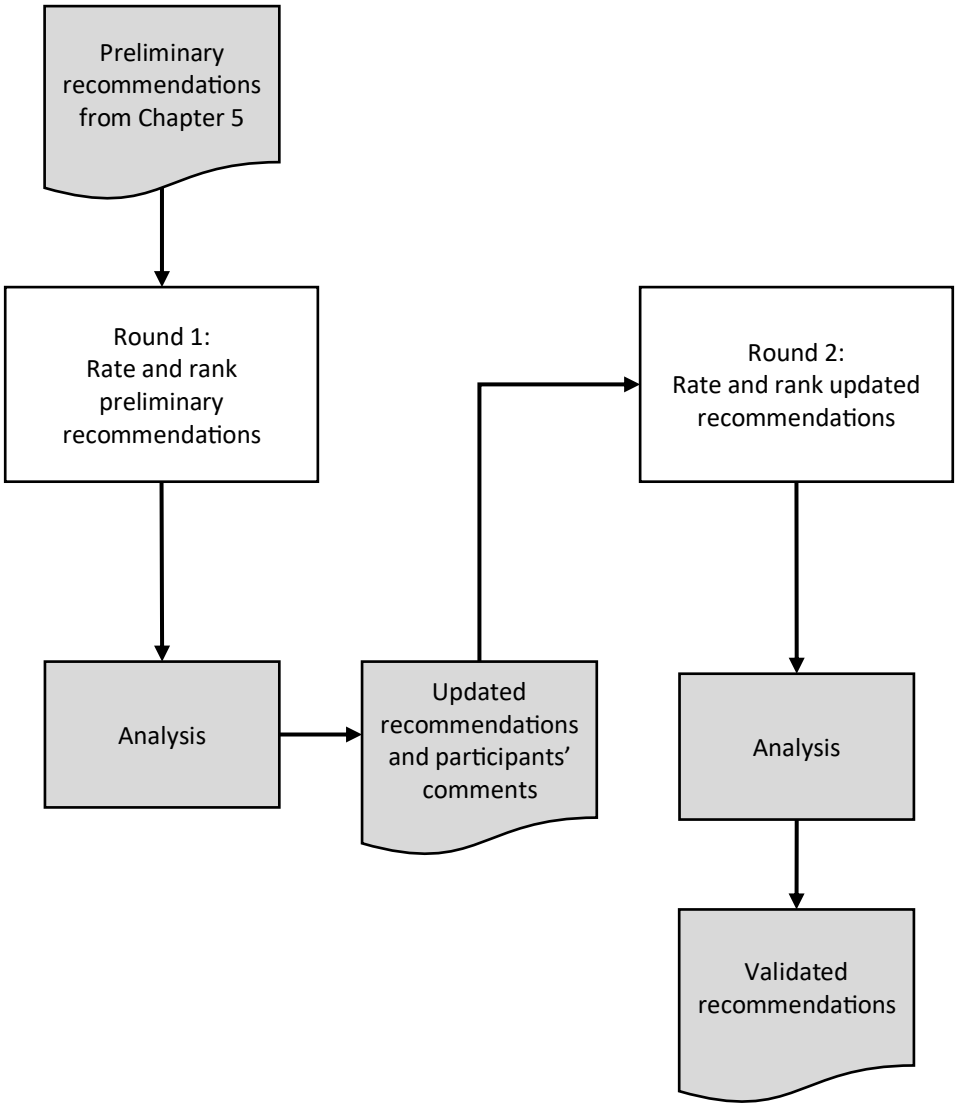
The survey was administered through the Qualtrics software, beginning with an introductory question that presented the participant information and asked them whether they consented to take part in the research study. This initial question outlined the study's objectives, and it was underscored that participation was entirely voluntary and could be withdrawn at any stage. It was made clear that if they withdrew their participation after the second round there would be a chance their anonymous

responses would already have been incorporated into the design of the second survey. If participants did not choose to proceed, a note of thanks for their response was displayed, marking the end of their participation. Those who provided consent proceeded to the full survey. To encourage participation the survey needed to be both user-friendly and time-efficient. The Qualtrics software allows the achievement of those goals and provided surveys that could be conveniently accessed online, including via mobile phones.

In both rounds the survey was structured into five sections:

1. Participant information sheet and consent
2. Participant background
3. Preliminary recommendations presented in a random order to score on a Likert scale
4. Preliminary recommendation forced ranking
5. Feedback collection

Figure 13 *The Delphi study depicting the two rounds*



Prior to commencing the main survey rounds, a pilot test was undertaken involving four experts—two who had participated in the initial interviews and two who had not. This pilot aimed to evaluate the

survey's logistics and questions. Notably, no revisions were needed, as the pilot testers were pleased with the survey structure and format.

Participants' key background dimensions were collected, including aspects such as their organisation's size, industry, role, years of experience in cyber security, and confirmation of their expertise in learning from incidents. If questions were not answered they were reminded to provide details but were still allowed to proceed if they did not complete a question.

Next, participants were asked to rate the preliminary recommendations using a Likert scale. A five-point Likert scale was employed, with the midpoint designated as zero, to allow an interval or quasi-interval scale of measurement (Clayton, 1997). There has been significant debate on the use of Likert scales—both on whether to include a midpoint and on the range of options offered. As Chyung et al. (2017) explained, there are conflicting studies on the optimal Likert scale and researchers need to carefully consider the questions posed and the target audience when designing surveys. Given that this survey was conducted with busy experts, the five-point scale was selected as it is quicker to complete than a 7- or 10-point scale and would present well on a mobile device. Admittedly, this choice involves a trade-off, as it sacrifices some of the precision offered by scales with more anchoring points. Considering the overarching aim to prioritise recommendations and concurrently capture qualitative insights into participants' rationales behind their ratings, the design choice is appropriate for this study.

As posited by Chyung et al. (2017), such a midpoint can sometimes act as a "dumping ground" category, especially when respondents are unfamiliar with the subject matter or believe a strong opinion to be socially undesirable; whereas, in the case of this survey, where participants are well-versed in the subject and responses are submitted anonymously, the inclusion of a midpoint option allows for those who did not have a strong opinion on the recommendation's suitability for their organisation to express their perspective without coercing them into adopting a definitive positive or negative stance.

Participants were required to assign a score to each recommendation to progress with the survey. Additionally, they were prompted to provide a rationale, consisting of a minimum of 50 characters if they attempted to move forward without supplying one. If participants still chose not to provide a comment, they were permitted to continue, ensuring their scores were captured even if they were hesitant or unable to give the rationale for their ratings. Keeney et al. (2006) recommended providing the opportunity to comment to avoid premature closure of ideas or forcing participants to conform to the existing information.

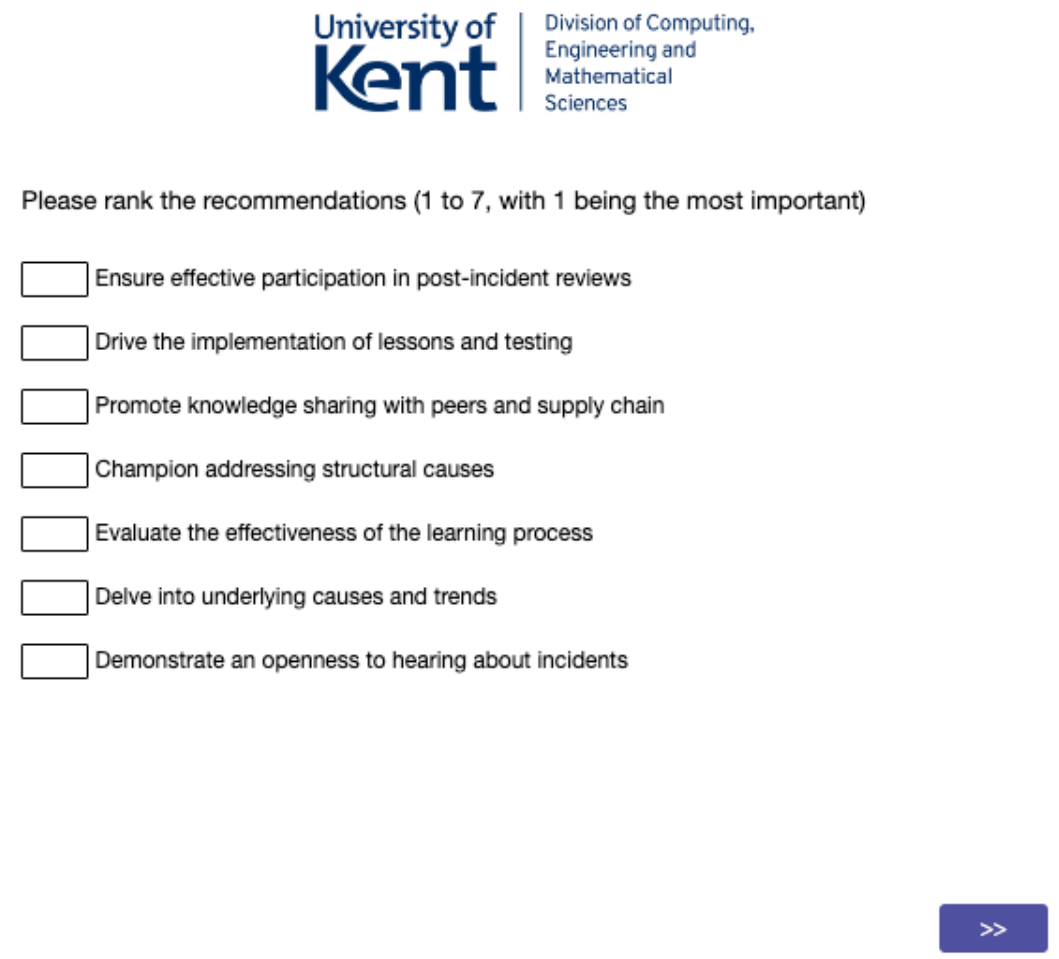
Participants were then directed to rank the preliminary recommendations in order, where 1 was deemed the most important and 7 the least. The survey design ensured that participants could not proceed until each recommendation had been assigned a distinct rank. Safeguards were implemented to prevent participants from assigning the same ranking to multiple recommendations. Following this ranking task, participants were prompted to revisit the recommendations and invited to share their insights on whether any recommendations appeared to be missing. Finally, they were asked if they had any additional feedback regarding the survey. While gentle reminders were provided to encourage completion of these fields, participants were not hindered from submitting the survey if they chose not to provide input in these final feedback sections.

6.1.1.1 Round 1

In the first round, the participants were shown information about taking part in the research and asked to provide their consent. Upon successful consent, they were requested to provide their background details. The preliminary recommendations (as per Chapter 5) were presented and they were asked to score them and then rank them (see Figure 14). At the end, participants were prompted to revisit the recommendations and invited to share their insights on whether any recommendations appeared to

be missing. Data from the first round was used to update the recommendations presented in the survey in the second round.

Figure 14 *Screenshot of the ranking which participants were asked to perform (note: recommendations were presented in a random order for each participant)*

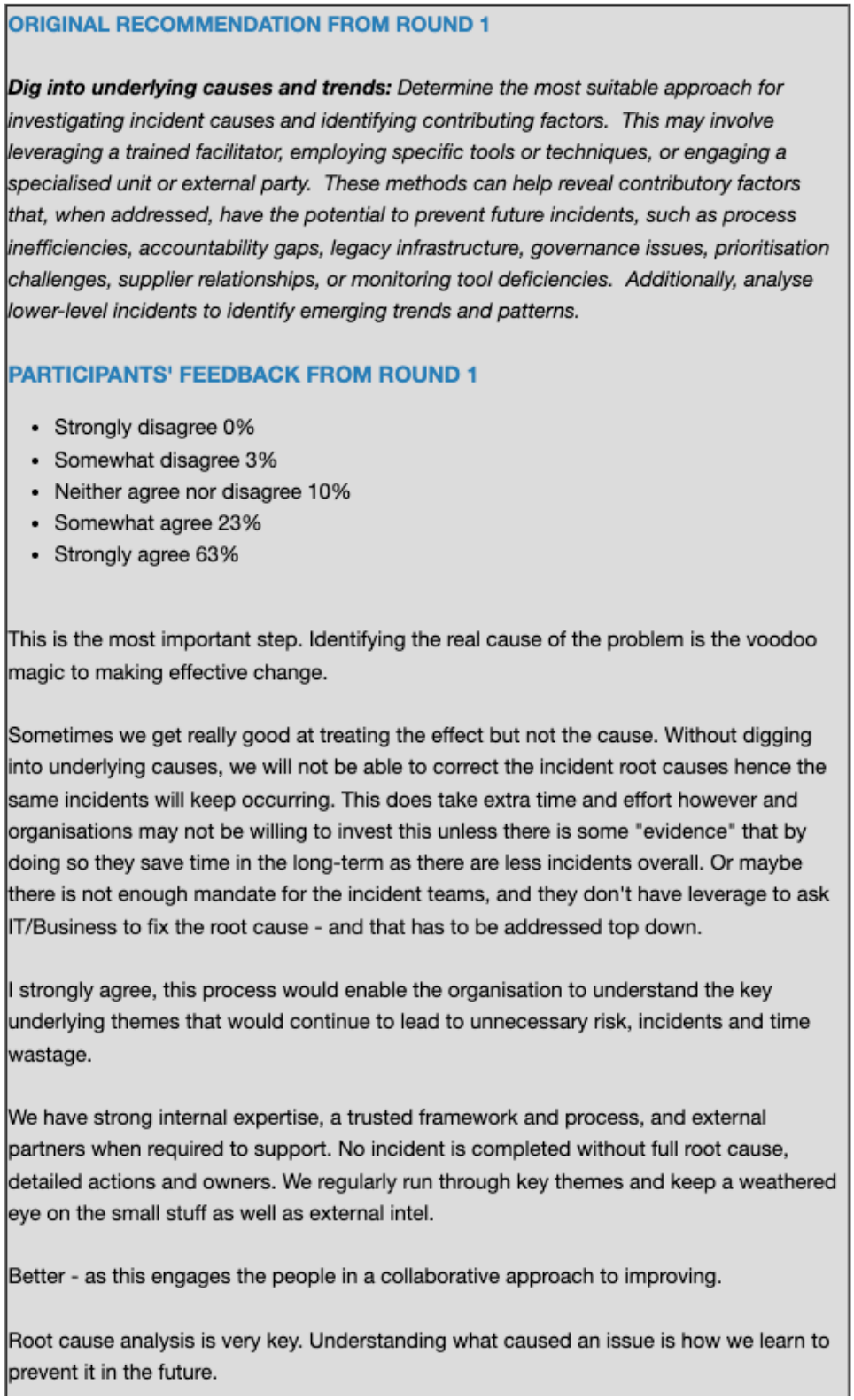


6.1.1.2 Round 2

The second round was administered in the same way as the first, but with a few additions. The participant information documentation this time explained this was the second round. Participants were reminded their participation was voluntary and again asked to confirm their consent. Additionally, it provided participants with summarised statistics derived from the initial round, such as the total number of participants and the quantity of comments received. Such feedback is a vital part of the Delphi process, as it is the only communication between the panel members (McKenna, 1994). The updated recommendations were presented alongside the unaltered comments submitted by participants during the initial round, along with the computed average (mean) score assigned to each recommendation.

These comments were presented verbatim below the rating, maintaining their original form—whether a single sentence, a paragraph, or multiple paragraphs—so that participants could review them according to their preference (see Figure 14). This design choice aimed to strike a balance, allowing participants to read the feedback at their discretion, while also enabling a smooth transition to subsequent questions. Again, the participants were prompted to provide a rationale for their assigned scores, they were forced to give a rating but only reminded to give a rationale. The survey was anonymous, therefore respondents were not provided with their own previous score.

Figure 15 *Screenshot of Delphi survey round 2 showing some of the feedback from round 1 (note feedback continued over multiple screens)*



ORIGINAL RECOMMENDATION FROM ROUND 1

Dig into underlying causes and trends: *Determine the most suitable approach for investigating incident causes and identifying contributing factors. This may involve leveraging a trained facilitator, employing specific tools or techniques, or engaging a specialised unit or external party. These methods can help reveal contributory factors that, when addressed, have the potential to prevent future incidents, such as process inefficiencies, accountability gaps, legacy infrastructure, governance issues, prioritisation challenges, supplier relationships, or monitoring tool deficiencies. Additionally, analyse lower-level incidents to identify emerging trends and patterns.*

PARTICIPANTS' FEEDBACK FROM ROUND 1

- Strongly disagree 0%
- Somewhat disagree 3%
- Neither agree nor disagree 10%
- Somewhat agree 23%
- Strongly agree 63%

This is the most important step. Identifying the real cause of the problem is the voodoo magic to making effective change.

Sometimes we get really good at treating the effect but not the cause. Without digging into underlying causes, we will not be able to correct the incident root causes hence the same incidents will keep occurring. This does take extra time and effort however and organisations may not be willing to invest this unless there is some "evidence" that by doing so they save time in the long-term as there are less incidents overall. Or maybe there is not enough mandate for the incident teams, and they don't have leverage to ask IT/Business to fix the root cause - and that has to be addressed top down.

I strongly agree, this process would enable the organisation to understand the key underlying themes that would continue to lead to unnecessary risk, incidents and time wastage.

We have strong internal expertise, a trusted framework and process, and external partners when required to support. No incident is completed without full root cause, detailed actions and owners. We regularly run through key themes and keep a weathered eye on the small stuff as well as external intel.

Better - as this engages the people in a collaborative approach to improving.

Root cause analysis is very key. Understanding what caused an issue is how we learn to prevent it in the future.

Based on the feedback in round 1, one of the recommendations was removed in round 2. (Details on why it was removed are given in Section 6.2.3.) Instead of ranking it, participants were asked if they agreed with its removal and were asked to provide their rationale. Subsequently, participants were once more presented with the revised recommendations, displayed in a random order, this time with the aggregated ranking results from round 1, and were tasked with re-ranking them. Following this, they were prompted to share any additional comments or feedback.

6.1.2 Participant selection and recruitment

The quality of a Delphi study depends on having expert participants who have the appropriate experience and expertise to provide valuable viewpoints. It is therefore critical to ensure participants are both appropriate and available. Formal models have been suggested to determine the ideal participant size or expertise for Delphi surveys. These suggest more experts improve the accuracy but assume the questions are based on facts and there is an equal distribution of expertise and an aggregation of individual opinions (Linstone et al., 1975). De Loë et al. (2016) found, in the studies they assessed, the panel size varied enormously—from 10 to 1,274 people. They found the larger the panel the higher the dropout rate and smaller panels tended to be used for targeted studies with specialised experts. In this thesis' research, the target panel size for the first round was a minimum of 30 and to maintain at least 15 for the second round, as the recommended panel size for a homogenous set of experts is 15-30 (Clayton, 1997). This study had 31 participants in the first round and 21 in the second round, which meets the targets set.

Participants in this Delphi study comprised of cyber security practitioners with expertise in security incidents, selected based on inclusion criteria outlined in Table 13. Those who participated in the earlier interview research phase were invited, and additional participants were recruited through the researcher's professional network. McKenna (1994) found starting with one-to-one interviews enabled personal reminders and enhanced response rates in the Delphi survey. As in the interview study, a purposive sampling technique was used to ensure a mix of size of organisation and industry representation. Invitations were sent to those practitioners who met the criteria. Individual email or personal LinkedIn message invitations were sent to practitioners to encourage their participation. To ensure good uptake, participants were provided with at least three weeks to complete the survey, and reminder emails were sent before the deadline.

Table 13 *Delphi survey participant inclusion and exclusion criteria*

Included	Excluded
• Organisations with over 250 employees • Organisations operates in the UK • Participant works in cyber security and has experience of the incident management process in their organisations • Participants selected from different sectors • Organisations has experienced at least one cyber security incident	• Organisations with no more than 250 employees • No operations in the UK • Participant not in a cyber security role or lacks relevant insight • Multiple participants from the same division of an organisation already included • Organisations which have never experienced a cyber security incident

6.1.3 Delphi survey data analysis

The data received from the completed online surveys was automatically compiled through the Qualtrics software and statistical data analysis was conducted using Microsoft Excel and SPSS software. These software packages were licensed by the University of Kent, and the data was only accessible to the researcher and their direct supervisory team. There is a wide range of quantitative techniques used by researchers to analyse the results of Delphi studies (de Loë et al., 2016). For this study, the purpose of the Delphi survey was to validate the recommendations. Therefore, it was vital to understand the

level of agreement with recommendations, which ones were considered the most important, and to analyse the written feedback to understand if the recommendations should be amended or replaced.

The 5-point Likert scale, originally introduced by Likert (1932), is often considered to represent interval data. This interpretation assumes an equal distance between ratings, making both the mean and median appropriate measures of central tendency. Given that the Likert scale employed in this study possesses a midpoint, it adheres to the characteristics of an interval scale, making it appropriate to use means and standard deviations (Chyung et al., 2017). However, there has been debate among academics regarding the assumption of equal distances between the ratings, with some arguing that it is valid and others suggesting that it may not be appropriate (Harpe, 2015).

Older textbooks quoted the Stevens-Siegel-Senders rule, which recommends using parametric measures for interval data with a normal distribution and nonparametric measures for ordinal data or situations where a normal distribution is not assumed (Harpe, 2015)—but this has also been challenged within the statistical community. Empirical studies, as observed by Franc et al. (2023), have indicated that the choice between parametric and nonparametric measures has minimal impact on research findings. A practical consideration highlighted by Harpe (2015) is the recommendation to use nonparametric measures when the data is skewed, especially in cases where respondents use only four of the five available points on the Likert scale. However, there is no empirical evidence presented to demonstrate this is necessary. The findings by Franc et al. (2023) suggest the simple mean and standard deviation are sufficient.

The underlying objective of the Delphi survey was twofold: first, to prioritise the recommendations, and second, to evaluate the extent of consensus achieved regarding these recommendations, with the intent of gauging their potential as comprehensive guiding principles applicable to a range of organisations. To this end, the arithmetic mean was calculated to show the recommendations with the highest degree of support and agreement. The standard deviation was calculated to show the spread of values from the mean. The standard deviation can be sensitive to outliers and assumes a normal distribution (i.e. around 95% of the data points fall within two standard deviations of the mean). Furthermore, to counteract any concerns around potential skewing caused by extreme values, the interquartile range ($IQR = Q3 - Q1$) was calculated (Anderson et al., 2020).

The analysis of the qualitative feedback provided during the Delphi study followed a structured approach to ensure the data was thoroughly reviewed and incorporated into refining the recommendations. Participants submitted over 9,500 words of feedback in round one and over 6,000 words in round two. Each round's comments were carefully read and coded, allowing for the identification of key themes and areas of consensus or disagreement. Over a hundred of the comments were simple agreements with the recommendations, and these were noted but did not contribute significantly to further refinement.

The coding process was instrumental in aligning feedback that, although provided in response to a specific recommendation, was relevant to other recommendations. This was particularly important because the recommendations were presented randomly to participants, leading to situations where comments intended to suggest improvements for one recommendation were better suited to another. While participants had the option to navigate back and forth between questions to amend their responses, it was not possible to track whether this occurred.

As with the interview study, participants in the Delphi study were assigned anonymous identifiers (e.g., [P1], [P2]). While there was some overlap in participants between the two studies, the survey was conducted anonymously, and identifiers were randomly assigned within each dataset. This means that a participant labelled [P1] in the Delphi study does not necessarily correspond to [P1] in the interview

study. This approach maintains participant confidentiality while allowing for clear referencing of responses in the analysis.

The coding and analysis of this feedback enabled an iterative process, where the recommendations were updated based on relevant insights across all responses, ensuring that no pertinent suggestion was overlooked. As a result, the final recommendations reflected the collective feedback, thoughts, and expertise of the practitioners, incorporating their practical wisdom into the refinements. This approach ensured that the recommendations were grounded in real-world experiences and aligned with the needs of the professionals involved in the study.

6.2 Delphi survey results

This section shares the response rates and the scores by recommendation for each round, as well as the ranking of importance. It discusses the attrition from the first round and its potential impact on the results. It presents the level of consensus achieved in each round. It discusses the feedback from the participants and how the recommendations were updated for round two.

6.2.1 Delphi survey respondents

The participant organisations were predominantly large, with a majority having over 1,000 employees, and some exceeding 50,000 employees. Responses from these large organisations are valuable due to their likely exposure to a considerable number of incidents, providing the necessary experience to respond to the survey. Including smaller organisations in the sample enhances the understanding of how recommendations may apply to entities with fewer resources. However, further research specifically targeting smaller organisations would contribute to a more nuanced understanding of the suitability of the recommendations to their specific context.

The response rates (see **Table 14**) of 66% in round 1 and 62% in round 2 reflect a credible level of engagement from our expert participants. In each round, there were some respondents who began the survey but did not complete it by the deadline. The responses from these participants were excluded from the analysis. In addition, one participant failed to confirm they had sufficient knowledge, despite reporting they had 14 years' experience in cyber security, and then completed the survey, which may have indicated they misunderstood the initial question. However, this participant's responses were excluded from the analysis and their comments were not shared with the other participants in round 2. The participants from the first round were invited to participate in the second round.

Table 14 *Delphi survey response rates*

Participants	**Round 1 (R1)**	**Round 2 (R2)**
Invited	47	*34
Consented to participate	35	25
Did not confirm they had sufficient knowledge of the topic	(1)	-
Completed the participant information but did not answer the core survey questions	(3)	(4)
Completed the survey	31	21
Response rate	**66%**	**62%**

**An invite was not sent to one participant who had suffered a family bereavement.*

The iterative nature of the Delphi method often encounters challenges in maintaining participant engagement over multiple rounds. Given the complex and demanding nature of the senior roles in the cyber security domain held by participants, obtaining such response rates is satisfactory. The response rates, although slightly reduced in the second round, remained robust.

Tables 15-18 provide summaries of the demographics of the Delphi survey participants, including the size of their organisations, industry sectors, roles, and their personal years of experience working in cyber security, respectively (see Appendix F for further details). The diverse representation increases the chances of a broad perspective. Notably, the majority of participants, in both rounds, held senior roles in cyber security, with many serving as CISOs or Heads of Security. The “Other” category in roles indicates the varied and evolving nature of roles in this relatively new cyber security profession. The range of years of experience demonstrates the participants' expertise, contributing to the credibility of their feedback on the recommendations. While there is a good mix of industries represented, future studies could delve deeper into each sector for a more comprehensive sector-specific analysis.

Table 15 *Employees in the Delphi survey participants' organisations*

Employees	**R1 Count**	**R2 Count**
Less than 1,000	6	3
1,000 to 50,000	18	12
More than 50,000	7	6
Total	**31**	**21**

Table 16 *Industry sector of the Delphi survey participants' organisations*

Sector	**R1 Count**	**R2 Count**
Finance and insurance	10	5
Industrial, energy, transport and logistics	10	5
Services, retail, tourism and entertainment	7	7
Government, public bodies and non-for-profits	4	3
Total	**31**	**20**

Note: In round 2, one response did not provide an industry sector, but did complete the rest of the survey.

Table 17 *Roles of the Delphi survey participants*

Role	**R1 Count**	**R2 Count**
CISO or Head of Security	18	12
CIO or Head of IT	3	2
Other	10	7
Total	**31**	**21**

Table 18 *Delphi survey participants years of experience working in cyber security*

Years of experience	R1	R2
Mean	17	18
Median	17	17

6.2.2 Overview of recommendation scoring and ranking

The participant scoring for the recommendations presented in both rounds of the Delphi survey is illustrated in Figure 16 and Figure 17. Humphrey-Murto et al. (2017) explain there is no universally agreed measure of consensus for Delphi studies but typically would be 70% agreed or strongly agreed. This was achieved for all recommendations in both rounds. Focusing on the results in round 2, there were only 5 individual ratings of “neither agree nor disagree” across 3 updated recommendations. In contrast, there were 25 ratings of “somewhat agree” and 88 ratings of “strongly agree”, affirming widespread support for the recommendations.

Notably, only two participants expressed dissenting views by scoring several recommendations as “somewhat disagree” or “strongly disagree” in the second round. The rationale behind their disagreement is not entirely clear from their comments. For example, in response to the recommendation to “Demonstrate an openness to hearing about incidents” [P16]’s feedback was “In my experience, employee reporting programmes work well and help identify issues that would've otherwise gone unnoticed.” And [P20]’s feedback was, “Reporting should always be encouraged, and training plans should ensure they contain information about how to do it. However, it is important to distinguish reporting of incidents and mistakes vs those that can be attributed to conduct issues.” Regardless, their perspectives deserve careful consideration. It is conceivable that they may have misunderstood the scoring system or chosen not to disclose the full reasons for their scoring in the provided rationale. The “strongly disagree” responses of these two participants result in lower scores for agreement and a higher standard of deviation for the second round. Nevertheless, all comments, including those from the participants who dissented, were thoroughly considered in the process of updating the final recommendations.

For each recommendation, the arithmetic mean and the median were computed, acknowledging the susceptibility of the mean to distortion caused by a small number of extreme ratings. The median represented a “strongly agrees” score. The mean is lower in both rounds due to a few “strongly disagrees” scores (as discussed above) decreasing the average. The standard deviation was calculated to show the spread of values from the mean. The results demonstrate a low variability with strong consistency indicating the majority of participants agreed with the recommendations. The differences between the rounds were calculated. This showed there was greater variation in the second round, with higher standard deviations, particularly for some recommendations. This reflects a couple of participants strongly disagreeing with the recommendations and the effects are more pronounced with a smaller number of participants in the second round.

Figure 16 *Delphi study recommendation scoring results in round 1*

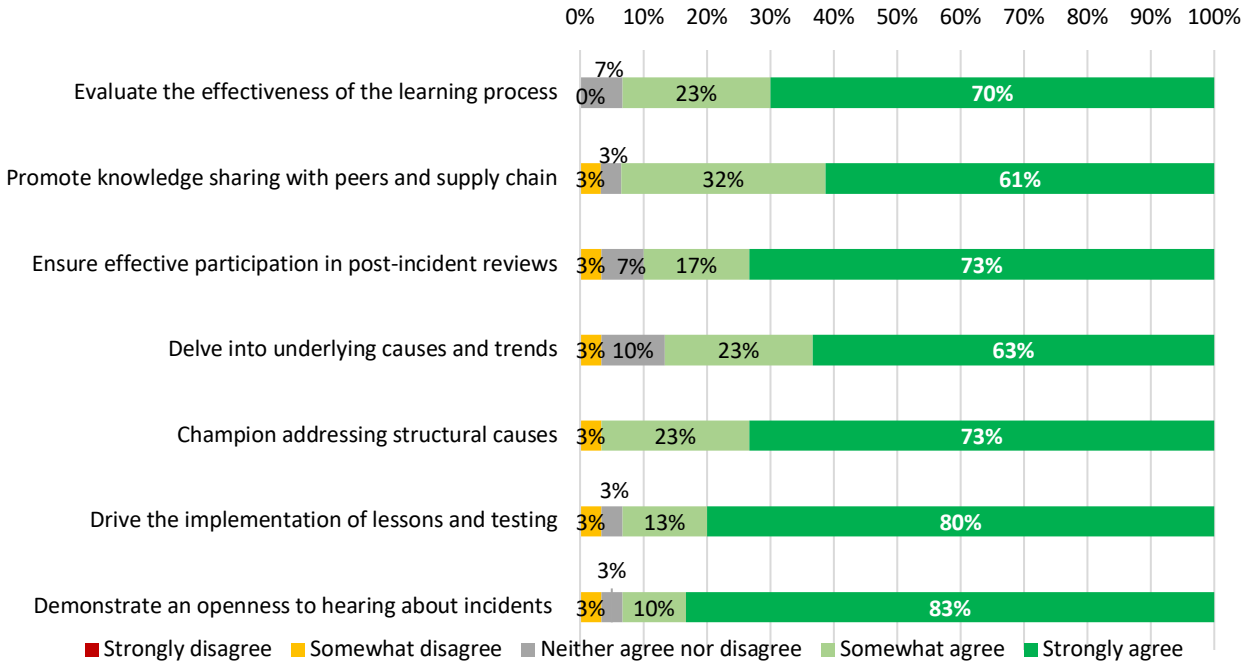


Figure 17 *Delphi study recommendation scoring results in round 2*

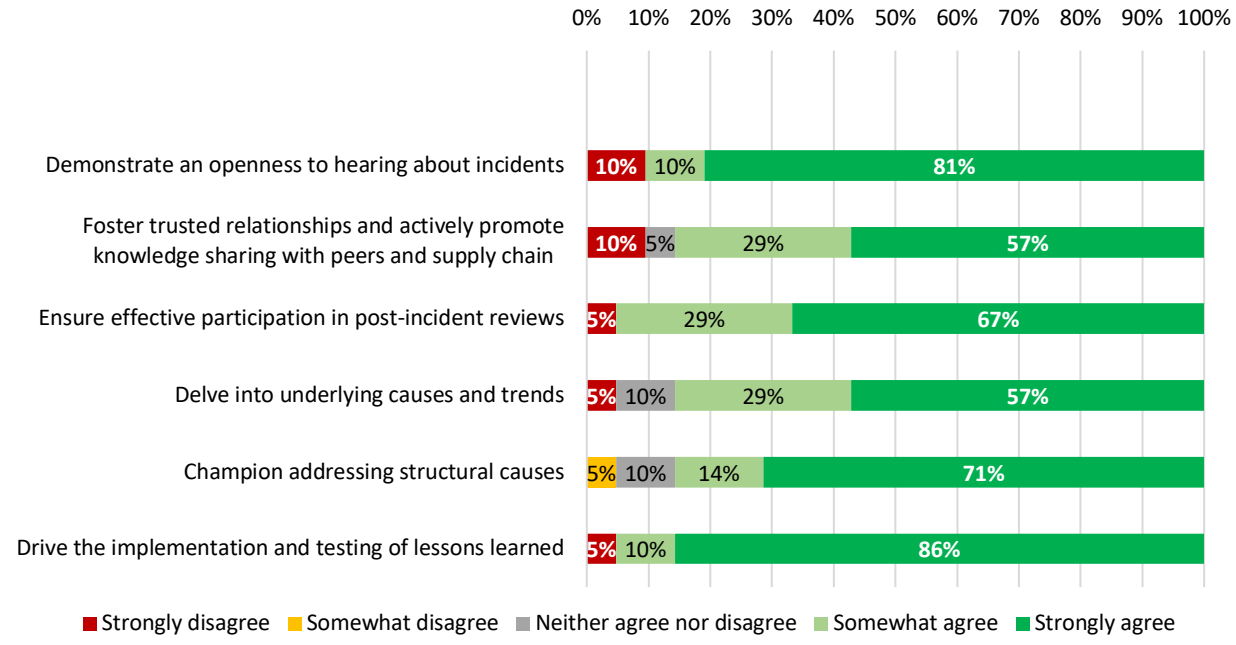


Figure 18 *Delphi study recommendations ordered according to the average ranking starting with the highest priority in round 1*

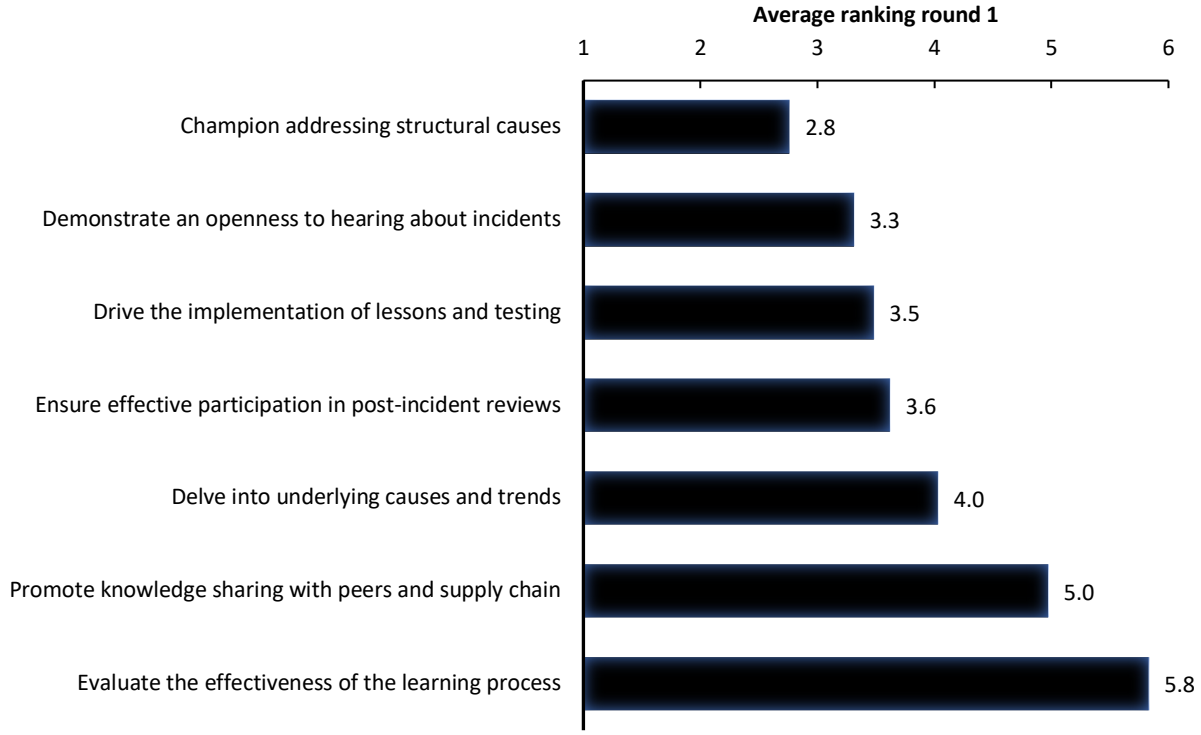
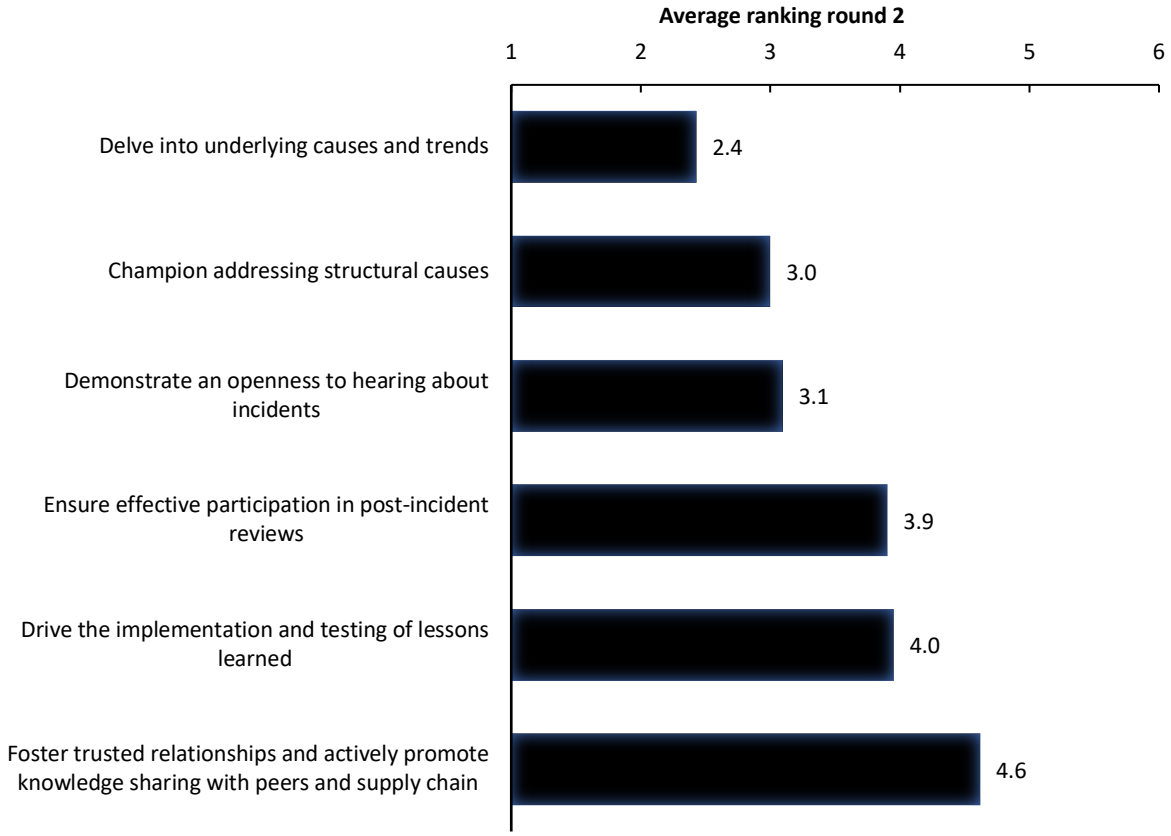


Figure 19 *Delphi study recommendations ordered according to the average ranking starting with the highest priority in round 2*



In addition to providing Likert scale ratings, participants were asked to rank the recommendations. The mean rankings (see Figure 18 and Figure 19) indicate that in round 1 “Champion addressing structural causes” had the highest mean ranking (2.8); in the next round it was ranked the recommendation with the second highest importance (3.0), just behind “Delve into underlying causes and trends” (2.4), while “Evaluate the effectiveness of the learning process” had the lowest mean ranking (5.8). This lowest ranking recommendation was dropped in round 2 (see further explanation as to the rationale for this below). “Foster trusted relationships and actively promote knowledge sharing with peers and the supply chain” had the lowest mean ranking in round 2 (4.6).

As shown in **Table 19**, every recommendation was ranked as the least important by at least one participant. Notably, all recommendations, except for “Drive the implementation and testing of lessons learned,” were ranked as the most important by at least one participant, although this recommendation was ranked second by some. Interestingly, “Drive the implementation and testing of lessons learned” also had the lowest standard deviation, suggesting higher agreement among participants regarding its ranking. In contrast, “Foster trusted relationships and actively promote knowledge sharing with peers and the supply chain,” which had the lowest average ranking, exhibited the highest standard deviation, indicating greater variation in participant opinions about its importance.

This ranking data is deterministic, as participants were required to assign a unique rank to each recommendation, preventing ties. Due to the lack of a natural linear order in the data, many common statistical analyses are unsuitable. Therefore, non-parametric tests are necessary to analyse this type of data. The rankings are inherently ordinal, reflecting relative importance, with each participant providing multiple observations by ranking each recommendation. Kendall’s W, a non-parametric measure, was used to assess whether there was a consensus in the rankings or if the results could be attributed to chance (El-Gazzar et al., 2016). This method is appropriate as it does not require the data to be normally distributed. It evaluates whether the recommendations were ranked similarly across participants. The null hypothesis—that the recommendations were ranked randomly—would result in $W = 0$, whereas the alternative hypothesis, indicating perfect agreement among participants, would result in $W = 1$.

A formal a priori power calculation was not conducted, as Delphi studies do not typically rely on statistical power in the traditional sense. Instead, the sample size was guided by accepted methodological practice, which recommends expert panels of 15–30 participants (Keeney et al., 2006). In this study, the two Delphi rounds included 29 and 21 participants respectively, and the analysis using Kendall’s Coefficient of Concordance (W). Table 20 shows the calculated values of 0.239 in Round 1 and 0.182 in Round 2. While these indicate weak-to-moderate agreement among participants, the statistically significant p-values ($p < .001$ and $p = .002$) suggest that the panel size was sufficient to detect non-random agreement in the ranking of recommendations.

Table 19 *Delphi recommendation ranking descriptive statistical results*

Recommendations (ordered by average ranking)	Average ranking		Std Deviation		Minimum ranked		Maximum ranked	
	R1	R2	R1	R2	R1	R2	R1	R2
Delve into underlying causes and trends	4.0	2.4	1.7	1.6	1	1	7	6
Champion addressing structural causes	2.8	3.0	1.9	1.6	1	1	7	6
Demonstrate an openness to hearing about incidents	3.3	3.1	2.2	1.7	1	1	7	6
Ensure effective participation in post-incident reviews	3.6	3.9	1.9	1.6	1	1	7	6
Drive the implementation and testing of lessons learned	3.5	4.0	1.3	1.1	1	2	7	6
Foster trusted relationships and actively promote knowledge sharing with peers and supply chain	5.0	4.6	2.0	1.8	1	1	7	6
Evaluate the effectiveness of the learning process	5.0	-	1.3	-	3.0	-	7	-

Table 20 *Delphi recommendation ranking test statistics results*

Test statistics	Results R1	Results R2
Number of participants	29	21
Kendall's Coeficient of Concordance	0.239	0.182
Chi-Square	41.645	19.095
Degrees of freedom	6	5
p-value	<0.001	0.002

6.2.3 Results by recommendation

6.2.3.1 Evaluate the effectiveness of the learning process

This recommendation emerged as the lowest ranked in the first round, despite a notable 93% of participants somewhat or strongly agreeing with its merit, see
Table **21**. The predominant sentiment in the comments was that, while the recommendation was ideal, it was perceived more as a "nice to have" rather than a critical priority. "That would be the perfect approach. In reality, however, many companies neither have the necessary knowledge nor the capacity," one participant [P5] observed, highlighting the gap between ideal practices and operational realities. Another participant echoed this sentiment, acknowledging that, while organisations might not currently be ready to implement such measures, the ability to "quantify the efficacy of the learning and tweak processes and metrics accordingly" would be highly beneficial.

Round 1 recommendation: Evaluate the effectiveness of the learning process
Regularly assess the efficacy of your organisation's incident learning process. Analyse incident trends to identify if prompt action on underlying causes could have prevented certain incidents. Evaluate the allocation of time and resources to the learning process, ensuring it receives adequate priority from teams throughout the organisation. If necessary, take proactive measures to optimise the organisation's learning from incidents.

Table 21 *Quantitative Delphi survey results for recommendation: Evaluate the effectiveness of the learning process*

	Average	Median	Standard deviation	Q1	Q3	IQR	Somewhat agreed	Strongly agreed	Ranking
Round 1	4.6	5.0	0.8	4.0	5.0	1.0	23%	70%	7th

Some respondents felt that the learning process inherently includes an evaluation, as the success of any learning would be “proved out” by the effectiveness of responses to subsequent incidents. Some also included elements of this evaluation process as suggestions for other recommendations particularly in investigating the causes to understand if lessons from previous incidents had been learned. Others believed that the “tone from the top” plays a more significant role in shaping the organisational culture, thereby influencing the efficacy of learning more profoundly than the recommendation itself might achieve.

Following participant feedback, the first preliminary recommendation was removed in the second round, with the descriptions of the remaining recommendations revised to integrate aspects of evaluation. Participants were informed of this decision (and the scores and comments from the first round) but were not asked to re-score the removed recommendation. Instead, they were asked about their agreement with its removal. Six explicitly supported the decision to remove it, while one openly disagreed. Two other responses were more neutral, not explicitly stating their stance on the removal, and others did not respond. As there was only one respondent who disagreed with the removal of the preliminary recommendation, it was left out of the final set of recommendations.

This nuanced feedback underscores the complex balance between aspirational goals and the practical constraints faced by organisations. It highlights a recognition among practitioners of the importance of continuous learning and process improvement yet acknowledges the challenges in prioritising such initiatives amidst operational demands. The decision to remove the recommendation reflects a pragmatic response to participant feedback, aiming to focus on actionable and prioritised measures that align more closely with the current capabilities and readiness of organisations.

6.2.3.2 Demonstrate an openness to hearing about incidents

This recommendation gathered substantial support, with 83% in the first round and 81% strongly agreeing during round 2, see Table 22. It was ranked in the top three in both rounds. Although the average score and standard deviation decreased in round 2, this is the impact of the two respondents who strongly disagreed (as discussed above); the majority strongly agreed. The inter-quartile range of zero demonstrates good consensus.

Round 1 recommendation: Demonstrate an openness to hearing about incidents
Organisations should foster a culture that encourages incident reporting by customers, employees, peers, and suppliers. This can be achieved through various means, such as establishing multiple reporting channels, formalising contracts and policies, providing training, facilitating discussions, and demonstrating receptive responses to shared incidents. Assessing stakeholders' understanding and motivation to report incidents can help identify knowledge gaps and improve reporting practices.

Round 2 recommendation: Demonstrate an openness to hearing about incidents
Encourage a workplace culture that fosters openness, making it easy for customers, employees, peers, and suppliers to report incidents and near-misses. Consider supporting multiple formal and informal reporting channels and incorporating reporting requirements into contracts and policies to enable sharing without negative repercussions. To encourage your employees, provide engaging and context-specific training that clearly outlines their roles and responsibilities in the reporting process. It's essential to acknowledge shared incidents, praise reporting even of mistakes, efficiently triage reports, and provide feedback on actions taken to the individuals who reported them. Evaluate stakeholders' understanding and motivation to report incidents to ensure that your organisational culture is genuinely perceived as open and to continually improve your reporting practices.

Table 22 *Quantitative Delphi survey results for recommendation: Demonstrate an openness to hearing about incidents*

	Average	Median	Standard deviation	Q1	Q3	IQR	Somewhat agreed	Strongly agreed	Ranking
Round 1	4.7	5.0	0.8	5.0	5.0	0.0	10%	83%	2nd
Round 2	4.5	5.0	1.2	5.0	5.0	0.0	10%	81%	3rd

Following the initial round of feedback, the recommendation was refined to specifically include the encouragement of mistake reporting and ensuring feedback is given to those who report. Additionally, the suggestion to incorporate reporting requirements in contracts, initially mentioned for the second recommendation, was integrated into this one for a more relevant fit with the reporting theme. Comments emphasised the training needed to promote reporting, with a particular emphasis on tailoring it to the diverse needs of different groups. Consequently, the recommendation was updated to reflect the need for context-specific training tailored to various stakeholders. In round 1, concerns were raised about smaller teams being overwhelmed by the volume of reports. The description in round 2 was updated to include the importance of effective triage. Given the strong support for this recommendation and the feedback from participants, no further changes were deemed necessary after round 2.

That this recommendation was agreed with so strongly echoes the finding from the first exploratory poll where “embracing a ‘no-blame’ culture and creating psychological safety to share mistakes / dilemmas” was the highest-scoring item to help organisations learn more from incidents. The consensus in this Delphi study underscored the significance of creating an environment characterised

by openness and psychological safety. Many respondents emphasised the importance of a 'blame-free' or 'safe' environment, where individuals felt comfortable admitting mistakes. Edmondson (2023) demonstrated that the level of psychological safety in the workplace is closely linked to the learning environment. Some participants expressed confidence that their organisations had already established a culture where “people are not afraid to report issues for fear of being blamed.” However, achieving this kind of culture is not easy, as Argyris (1999) pointed out. Organisations often claim to encourage issue reporting but send contradictory signals when they avoid discussing the undiscussable. These are organisational defensive mechanisms which make discussing mistakes or uncertainties taboo to avoid the embarrassment or threat confronting them would pose.

Practical aspects of implementing this recommendation were widely commented upon. Training and communication with employees were highlighted to ensure they knew what to report, to whom, and how. Tailoring training to suit diverse groups of employees was also seen as beneficial. Additionally, there were suggestions to automate phishing reporting to simplify the process for users—a practice identified in the earlier interview research. Some participants mentioned that maintaining accountability remains critical. Edmondson (2018) explained that there is a common misconception that fostering psychological safety results in leniency, while research shows that the opposite is true, with higher psychological safety linked to higher performance standards. Creating an environment where employees feel safe reporting incidents is crucial for building a culture of openness and accountability. This recommendation calls on CISOs, Senior Business Leaders, and HR Teams to demonstrate an ongoing commitment to psychological safety. By fostering a blame-free culture, organisations can ensure that incidents are not hidden due to fear of repercussions.

The involvement of HR teams is particularly important to embed policies that encourage incident reporting and to ensure that employees feel supported throughout the process. Additionally, Heads of Incident Management must ensure that open lines of communication are maintained between teams and that there is continuous feedback on how incident data is used to drive improvements. A few participants expressed concerns about regulators and the legal implications of transparency, citing the recent legal action against the CISO of Solar Winds[24] as pressure which discourages openness about incidents.

6.2.3.3 Foster trusted relationships and actively promote knowledge sharing with peers and supply chain

This recommendation received the lowest scores in both the first and second rounds of the Delphi survey, with only 61% strongly agreeing in the first round and 57% in the second, marking it as joint lowest, see Table 23. Furthermore, it was ranked 6th in importance, indicating the least prioritisation in the second round. Despite a majority indicating agreement, a notable portion (32% in round 1 and 29% in round 2) expressed only somewhat agreeing, revealing some hesitancy towards full endorsement.

[24] US Securities and Exchange Commission press release: https://www.sec.gov/news/press-release/2023-227

Round 1 recommendation: Promote knowledge sharing with peers and supply chain
Engage in active participation and foster a culture of sharing lessons learned with peers and suppliers. Encourage the dissemination of valuable insights from near misses, low-severity incidents, and more significant events. Emphasise collaboration and assistance rather than resorting to contractual penalties when working with suppliers. Cultivate trusted relationships by promoting openness and, where appropriate, establish legal frameworks that facilitate the sharing of non-competitive information. Support the establishment of local and industry groups facilitated by government and security agencies, such as the National Cyber Security Centre (NCSC) Trust Groups, to enable collective learning and collaboration.

Round 2 recommendation: Foster trusted relationships and actively promote knowledge sharing with peers and supply chain
Cultivate trusted relationships and encourage active engagement with peers and suppliers to facilitate the exchange of valuable lessons learned. Promote the dissemination of insights gained from near misses, minor incidents, and more significant events. Create opportunities for the sharing of non-competitive information through structured forums. Highlight the importance of early incident sharing in contractual agreements and collaborate closely with suppliers, ensuring contractual penalties only serve as a measure of accountability for intentional negligence. Contribute to local and industry groups facilitated by government and security agencies, such as the National Cyber Security Centre (NCSC) Trust Groups, to foster collective learning and collaboration.

Table 23 *Quantitative Delphi survey results for recommendation: Foster trusted relationships and actively promote knowledge sharing with peers and supply chain*

	Average	Median	Standard deviation	Q1	Q3	IQR	Somewhat agreed	Strongly agreed	Ranking
Round 1	4.5	5.0	0.8	4.0	5.0	1.0	32%	61%	6th
Round 2	4.2	5.0	1.2	4.0	5.0	1.0	29%	57%	6th

After the initial round, both the title and description of the recommendation were revised to underline the significance of trust in enabling information sharing and emphasising the establishment of the right relationships with suppliers. An addition highlighted the necessity of contractual penalties to ensure accountability for negligence, acknowledging that “many companies fall victim to cyber-attacks despite investing in protective measures.” It also introduced the importance of early incident lifecycle information sharing by suppliers and adjusted the description to advocate for structured information sharing to maximise the value of participation in forums.

Despite recognising the necessity of the recommendation, many respondents expressed concerns about the effort required and its applicability across all suppliers or industries. “The bad guys are happy to share information,” one respondent noted, emphasising the general agreement on the benefits. The dependency on suppliers was acknowledged, with one pointing out that “the ecosystem is only as strong as its weakest link.” The applicability of such suggestions to all suppliers was questioned by another, who stated, “I would have selected 'strongly agree' except that... my experience tells me to only trust certain suppliers and establishing that trust takes time and effort on both sides.”

Building relationships with suppliers was highlighted as a significant endeavour, crucial not only as part of sound IT practices but also as an essential preparatory step for incident management. One respondent encapsulated the sentiment, stating, “You don't want to be engaging with teams for the first time right in the middle of a major incident.” While participants acknowledged the necessity of having the right contractual clauses, they pointed out that these clauses alone were insufficient to

foster the desired level of collaboration, which requires mutual investment from both parties. The complexity of supplier relationships was underlined by another comment, noting that, “The relationship with suppliers and third parties is always complex as commercial agreements tend to give one of the parties the upper hand and perhaps this is worth exploring as a topic in itself.” Friday et al. (2021) found parties tended to optimise for their own short-term gain, limiting the learning in supply chains. Kumar et al. (2016) emphasised the important role culture plays on enabling supply chain collaboration. Despite revisions in the second round, comments persisted on the challenges of achieving a balance between contractual obligations and the benefits of collaboration and information sharing.

The effort required to share information with industry peers was another concern raised, with one respondent remarking, “working collaboratively with industry is hard.” The discussion touched on the time investment necessary, and the potential risks associated with disclosing competitively sensitive information, despite the description explicitly saying to share only non-competitive information. Husák et al. (2023) found nervousness about sharing any information increased after the introduction of new regulations, even if the regulations did not specifically cover the information being shared. Opinions diverged on whether maintaining a secure posture constituted a competitive advantage—some viewed it as such, while others disagreed, reflecting the diversity of perspectives across different organisational contexts. The results in this survey did not indicate any industry sector pattern to these comments. This would need further exploration with more participants.

Industry-specific variations in the culture of sharing were highlighted, with positive examples cited in sectors like finance and energy. Yet another respondent observed, “It's easier in certain ‘collaborative’ sectors such as higher education or government than in ‘competitive’ sectors where there would be less appetite to disclose what could be perceived as a weakness.” The level of cyber security maturity within a sector was deemed a significant factor in its propensity for collaboration, with comments highlighting reluctance in some sectors due to concerns about reputation risk and compliance focus.

Senior Leadership Teams and Regulatory Bodies also have a role in advocating for broader industry collaboration and aligning security practices with national security guidelines. In many cases, government agencies or regulators, such as the UK’s National Cyber Security Centre (NCSC), provide forums for collaboration, and organisations can take advantage of these platforms to exchange knowledge and build resilience across the supply chain. The role of regulators or agencies in facilitating forums for information sharing received mixed feedback. While some participants found value in NCSC trust groups, others expressed dissatisfaction with the feedback mechanism, one participant observing that “the NCSC rarely feeds back when things are reported.” This variance in experiences suggests a need for further investigation into how such bodies can effectively contribute to the cyber security ecosystem's resilience.

In summary, practitioners recognised the value of the recommendation but also the difficulties in its implementation. Given the interconnected nature of today’s business environment, fostering collaboration and building trusted relationships with external partners, including suppliers and industry peers, is vital for improving security resilience. This recommendation targets CISOs and Supplier Managers, who are responsible for initiating and maintaining these relationships, as well as Legal Teams to ensure that contracts facilitate information sharing and collaboration on incident response. The complexity of establishing trusted relationships and the considerations needed for contractual frameworks were acknowledged, with one respondent summarising the challenge: “I would have ideally liked to select Strongly Agree, but there is the practicality of making this feasible considering time limitations—it is a good measure to have in place but needs some practical considerations to make it less of a tick box exercise and to promote a behavioural and cultural shift.”

Reflecting these insights, the final recommendation was revised to underscore the need for effort and strategic prioritisation to balance collaborative benefits against the required investments.

6.2.3.4 Ensure effective participation in post-incident reviews

In the first round of the Delphi survey, 90% of participants either somewhat agreed or strongly agreed with the recommendation, a figure that increased to 96% in the second round, see Table 24. However, there was a shift towards more "somewhat agreeing" responses, with the equivalent of one fewer respondent strongly agreeing than in the first round. The recommendation consistently ranked 4th in importance across both rounds, with the standard deviation also remaining unchanged at 0.9, indicating a broad consensus among participants.

Round 1 recommendation: Ensure effective participation in post-incident reviews
Facilitate the involvement of key stakeholders in post-incident reviews to gain comprehensive insights into the causes and potential remedial actions. Engage individuals with seniority and authority to enact necessary changes. Consider participants with the right attitude, social skills, and a collaborative mindset. Ensure that post-incident reports are discussed in impactful governance forums, where their findings and recommendations can drive meaningful actions and improvements.

Round 2 recommendation: Ensure effective participation in post-incident reviews
Particularly for incidents involving intricate causes or recurring patterns, involve senior leaders, subject matter experts, system owners, and individuals responsible for implementing changes in post-incident reviews. This will enhance awareness of risks, promote comprehension, and inspire ownership of corrective actions. Consider optimising group dynamics, including the possibility of hosting separate stakeholder meetings to facilitate open discussions on causes and generate bold action plans. Discuss post-incident findings in impactful governance forums to drive meaningful actions and improvements. Evaluate the allocation of time and resources to the learning process, ensuring it receives the appropriate priority for your organisation.

Table 24 *Quantitative Delphi survey results for recommendation: Ensure effective participation in post-incident reviews*

	Average	Median	Standard deviation	Q1	Q3	IQR	Somewhat agreed	Strongly agreed	Ranking
Round 1	4.5	5.0	0.9	4.3	5.0	0.8	17%	73%	4th
Round 2	4.5	5.0	0.9	4.0	5.0	1.0	29%	67%	4th

Participants highlighted the important nature of this recommendation, noting that, when it is done well, it can "foster mutual understanding top to bottom." However, challenges were acknowledged, such as meetings being poorly attended or not effectively conveying root causes, leading to "knee-jerk reactions." A common concern was the presence of a defensive mindset during post-incident reviews, where the focus might shift to self-preservation at the expense of collective learning. This reflects the tendency described by Argyris (1990) and more recently by Tavris and Aronson (2020). It was suggested that the reviews "must be open and not avoid self-criticism", while also cautioning against using them as a means to undermine individuals for political gains within the organisation. Elliott and Macpherson (2010) found such reviews can be used by some as a vehicle for political gain within an organisation. The importance of a strong, independent lead for the review was emphasised, alongside the potential benefit of having an external facilitator to ensure a safe environment for open discussion.

The involvement of senior leaders was deemed essential for elevating awareness and ensuring the identification of all causes, as well as for providing support for remediation actions. CISOs, Heads of Incident Management, Legal Teams, and Senior Leaders must ensure that the right people are involved in these reviews to provide comprehensive insight into what occurred and how to prevent recurrence. “If actions are agreed at too low a level, they will never make the prioritisation list,” one participant observed. The necessity of engaging stakeholders with the right authority and business context knowledge to prioritise actions effectively was also highlighted. As Demjaha et al. (2019) found incidents can trigger organisations to invest in security.

The value of post-mortem reviews in bridging technical and business understandings of incidents was recognised, with one respondent describing the opportunity they provide for leaders to grasp the business impact fully. Yet thoughtful consideration given to the selection of senior participants for these reviews was advised to avoid stifling openness among junior staff. Amendments made for the second round, suggesting “the possibility of hosting separate stakeholder meetings, meetings to facilitate open discussions on causes and generate bold action plans” drew mixed reactions. Concerns were raised about the necessity of “bold” action plans for every incident and the risk of diluting the message through multiple meetings. Overall, the feedback centred on the importance of selectively involving the appropriate individuals in post-incident reviews. This approach is vital for enhancing understanding of risks, ensuring meaningful lessons are learned, and securing ownership of necessary actions for effective lesson implementation. The recommendation was updated to reflect these concerns.

6.2.3.5 Delve into underlying causes and trends

In the second round of the Delphi survey, this recommendation was ranked as the most important, although the average score saw a slight decrease, see
Table **25**. This was due to a larger proportion of respondents selecting “somewhat agree” rather than “strongly agree.” These respondents generally saw the recommendation as crucial but disagreed with specific aspects, such as involving independent facilitators or senior personnel in post-incident reviews. Despite these reservations, the overall ranking rose from 5th in the first round to 1st in the second, suggesting the recommendation's importance resonated broadly across participants, potentially influenced by reflections or feedback from round one.

The marked increase in ranking suggests that participants’ perceptions of the recommendation evolved between the rounds as a result of group reflection, exposure to peer views, or the refinement of the statement itself. This type of shift is not unusual in Delphi studies, where the iterative process allows participants to reconsider their initial views in light of anonymised group feedback. Although the average score decreased slightly due to greater use of “somewhat agree,” the elevated rank highlights growing consensus around the relative importance of this recommendation compared to others. This could indicate a reframing of how participants interpreted the underlying purpose of delving into root causes, recognising greater value when pragmatically scoped. The revised phrasing in Round 2, which acknowledged resource constraints and proposed focusing on selected incidents, this potentially contributed to this increase by making the recommendation more realistic and adaptable across different organisations.

Round 1 recommendation: Delve into underlying causes and trends
Determine the most suitable approach for investigating incident causes and identifying contributing factors. This may involve leveraging a trained facilitator, employing specific tools or techniques, or engaging a specialised unit or external party. These methods can help reveal contributory factors that, when addressed, have the potential to prevent future incidents, such as process inefficiencies, accountability gaps, legacy infrastructure, governance issues, prioritisation challenges, supplier relationships, or monitoring tool deficiencies. Additionally, analyse lower-level incidents to identify emerging trends and patterns.

Round 2 recommendation: Delve into underlying causes and trends
For incidents characterised by multiple or intricate causes, or recurring patterns, commit to comprehensive cause investigations and identifying contributory factors. Consider if enlisting a skilled facilitator, inviting diverse perspectives, applying specialised tools or methodologies, or collaborating with external experts with experience from other organisations would be of benefit. These strategies can enhance incident response and unearth contributory elements that, once addressed, hold the potential to prevent future incidents. These elements may encompass process inefficiencies, accountability gaps, legacy infrastructure, governance discrepancies, prioritisation dilemmas, supplier relations, or monitoring tool limitations. Additionally, use these investigations as opportunities to engage and train SOC analysts, enabling them to gain valuable experience and insights. Furthermore, routinely analyse incident metrics and trends, including lower-level incidents to detect emerging trends and recurring patterns, assess whether rectifying underlying causes could have averted certain incidents.

Table 25 *Quantitative Delphi survey results for recommendation: Delve into underlying causes and trends*

	Average	Median	Standard deviation	Q1	Q3	IQR	Somewhat agreed	Strongly agreed	Ranking
Round 1	4.4	5.0	1.0	4.0	5.0	1.0	23%	63%	5th
Round 2	4.3	5.0	1.0	4.0	5.0	1.0	29%	57%	1st

The recommendation sparked considerable debate among respondents. For some, it was seen as essential, a "no-brainer" for improving security, whereas others considered it idealistic, hindered by practical constraints of time and resources. The use of independent facilitators divided opinions sharply; they were viewed by some as significantly beneficial, while others perceived potential drawbacks. No clear patterns emerged from the analysis concerning participants' industry sectors, organisation sizes, or years of experience. A future broader study might uncover specific correlations.

The reluctance to strongly agree was often attributed to negative experiences with such review processes, with concerns ranging from over-analysis and blame to a narrow focus on specific issues. Despite these reservations, the necessity of conducting thorough root cause analysis was recognised, albeit infrequently performed well in practice. “It amazes me how little root cause analysis is performed in the incident space,” one participant reflected, pointing to the tendency of many organisations to treat it as a as a “tick box exercise” without dedicating sufficient time for a thorough job. Following feedback, the second round's description was refined to advise organisations to carefully select incidents for in-depth investigation. Still, resource constraints remained a concern, as echoed in comments like, “I agree, but I don't have the resource to do this properly.”

By focusing on root causes, organisations can implement changes that address deeper vulnerabilities, reducing the risk of future incidents. The success of this approach requires Senior Leaders to support comprehensive investigations and allocate the necessary resources to delve deeper into the causes, while Incident Response Teams and Audit Committees ensure that findings are communicated across departments and incorporated into risk management frameworks.

The introduction of independent facilitators to mitigate bias and ensure impartiality received mixed reactions. Some participants praised the approach, noting, “incidents are often chaotic... getting true lessons learned can often be difficult if an independent facilitator is not used,” thereby showing an appreciation of how facilitators can help navigate the complexities of post-incident analysis. This was further supported by the decision to augment the description for round 2, incorporating the feedback that “using experts to assist in this also allows for learnings from other companies or industries to be shared,” highlighting the additional benefit of cross-industry insights. However, others voiced concerns about potential distrust and resentment towards external involvement. Comments such as “Engaging external parties could result in distrust and a feeling of fear, with team members perceiving the engagement as a means of identifying problem areas within people and therefore close themselves off to the exercise,” illustrate the nuanced stance on the involvement of facilitators, balancing the value they bring against the challenges of integrating them into sensitive review processes.

Following feedback from the first round, the proposal to train Security Operations Centre (SOC) analysts sparked a varied response in the subsequent round, signalling the need for further refinement of this recommendation. One participant noted the redundancy of such training for organisations with an outsourced SOC, while another remarked, “SOC analysts should stick with technical discovery, we need a different level of resource to consider non-technical root causes,” highlighting the complexity of addressing root causes beyond the technical scope. This feedback underscores the necessity of tailoring the recommendation to accommodate diverse operational models.

The feedback also touched upon the strategic approach to incident management, contrasting the need for prevention with the efficacy of rapid response. Broad consensus emerged around the importance of scrutinising lower-level incidents, with participants recognising the significant value in identifying latent risk areas through pattern analysis. Moreover, several participants argued that the aim should not solely be to prevent all incidents, suggesting that in some instances, a swift and effective response could offer a more practical and efficient solution. This insight that not all incidents can be averted was integrated into the recommendation's wording.

6.2.3.6 Champion addressing structural causes

This recommendation was deemed of the highest importance in the first round and retained second place in the ranking in the second round, underscoring how crucial the practitioners viewed it. With a high agreement rate of 96% in the first round dropping slightly to 85% in the second, and consistently low standard deviations, there was a strong consensus on its criticality for organisations, see Table 26.

Round 1 recommendation: Champion addressing structural causes
Leadership should emphasise the importance of addressing structural causes of incidents, even when the actions required may be less tangible, such as addressing cultural issues or resolving long-standing technical debt. This is particularly crucial in cases where individuals may be hesitant to take personal accountability for an incident as they cannot guarantee closure. Handling the expectation of addressing structural causes will vary depending on the organisation's maturity and size, but it requires senior leadership to set the agenda and recognise progress.

Round 2 recommendation: Champion addressing structural causes
Senior leaders should emphasise the importance of addressing structural causes of incidents, even when the actions required may be less tangible, such as addressing cultural issues, enterprise architecture deficiencies, or resolving long-standing technical debt. These are challenging to tackle and may take time, so it is often necessary to enhance the detection, response, and recovery measures in the meantime. Senior leaders need to operate within the context of their organisation to set the expectation that structural causes can be improved over time, particularly where individuals may be hesitant to take personal accountability for an incident as they cannot guarantee closure. This may require executive sponsored transformation initiatives, coupled with a growth mindset that entails an ongoing evaluation of the organisation's learning and improvement processes as they evolve through incident experiences.

Table 26 *Quantitative Delphi survey results for recommendation: Champion addressing structural causes*

	Average	Median	Standard deviation	Q1	Q3	IQR	Somewhat agreed	Strongly agreed	Ranking
Round 1	4.7	5.0	0.7	4.3	5.0	0.8	23%	73%	1st
Round 2	4.5	5.0	0.9	4.0	5.0	1.0	14%	71%	2nd

One respondent encapsulated the feedback's essence, stating, “This is critical but VERY difficult to do.” This reflects the challenging nature of effectively addressing the issue, with another adding, “doing anything less will just result in perpetual firefighting.” The broad support stemmed from the recognition that "It’s important to eliminate structural root causes instead of fixing symptoms" and that it is necessary to "identify the strategic causes which cause a vulnerability to go unnoticed or un-remediated." However, there was hesitancy to fully commit, with one participant noting the difficulty of realisation within their organisation, leading to a “somewhat agree” score.

The emphasis on senior leadership's involvement was a consistent theme throughout the feedback, underscored as both essential for initiating meaningful action and identified as a challenge in acquiring adequate executive support. This duality was captured by one participant's reflection: "Whilst this is a good recommendation as worded...senior leaders may be hesitant to take personal accountability for security incidents." This underscores the nuanced challenges in aligning leadership's commitment with operational realities. Despite these concerns, respondents overwhelmingly acknowledged the essential role of senior leadership in two key areas: shaping organisational culture and addressing technical debt. These areas were identified as pivotal for senior leaders to actively support,

demonstrating how their engagement is necessary not just in strategic direction setting but also in ensuring meaningful progress in tackling the structural causes of security incidents. This supports findings by Gale et al. (2022) who studied board members' engagement on cyber security.

In response to the varied feedback and to address the concerns raised, the description of the recommendation was refined for the second round of the Delphi survey. Participants had underscored the importance of not only highlighting the need for senior leadership's proactive engagement but also addressing broader organisational challenges. The refined recommendation included a focus on enhancing the broader enterprise security architecture. Additionally, the incorporation of a "growth mindset" into the recommendation was a direct response to feedback suggesting the need for organisations to adopt more adaptive and learning-focused attitudes towards security incident management.

The feedback from both rounds highlighted the importance of senior leadership not just in endorsing policies but in actively shaping an organisational culture that prioritises continuous improvement and openness to learning from incidents. Such sentiment echoes findings from prior research exploring how a culture of learning is fostered (Catino, 2008; Edmondson, 2018; Schilling & Kluge, 2009). It recognises the need for leadership to navigate these challenges with a balance of strategic oversight and a commitment to fostering an adaptive, resilient organisational culture. Even though some respondents hesitated to fully agree due to the difficulty of achieving this in their organisations the existing description already reflects this challenge and therefore no future updates to this recommendation are proposed.

In practice, the Audit and Risk Committees will play an essential role by holding organisations accountable for identifying these structural issues and ensuring that the necessary changes are implemented. HR and Organisational Development teams should also be involved in assessing how organisational culture, workforce skills, and operational structures contribute to security vulnerabilities.

6.2.3.7 Drive the implementation and testing of lessons learned

This recommendation received strong endorsement from practitioners, highlighting its perceived importance with 93% agreeing (somewhat or strongly) in the first round and an impressive 96% in the second round, making it the highest-scoring recommendation, see Table 27. Despite its high approval, its ranking slipped to fifth in the second round, a shift that remains unexplained but was only marginally behind the fourth place.

Round 1 recommendation: Drive the implementation of lessons and testing
Ensure the actions identified in post-incident reviews are followed through and actually implemented. Depending on the organisation, establish suitable action registers and tracking forums to monitor progress and overcome any obstacles that arise. Additionally, it is important to conduct appropriate testing to validate that the implemented actions effectively address the identified causes. This can include activities such as red teaming, simulation exercises, or internal audit testing. It is equally important to test non-technical actions, such as verifying the proper functioning of new governance structures and ensuring adherence to updated training guidance.

Round 2 recommendation: Drive the implementation and testing of lessons learned
Ensure that action items identified in post-incident reviews are not only documented but also executed promptly. Use suitable governance forums within your organisation to make the progress of these actions transparent to senior leadership, prioritising them as needed. In cases where resources may be limited, consider implementing interim mitigating measures to address critical issues until the full resolution is feasible. Furthermore, validate the effectiveness of implemented actions through rigorous testing, encompassing activities like red team exercises, simulations, and internal audits. Ensure testing also encompasses non-technical factors, such as assessing the functionality of new accountability structures and confirming adherence to updated training protocols.

Table 27 *Quantitative Delphi survey results for recommendation: Drive the implementation of lessons and testing*

	Average	Median	Standard deviation	Q1	Q3	IQR	Somewhat agreed	Strongly agreed	Ranking
Round 1	4.7	5.0	0.8	5.0	5.0	0.0	13%	80%	3rd
Round 2	4.7	5.0	0.9	5.0	5.0	0.0	10%	86%	5th

Practitioners' feedback reflected the ongoing challenge of resource constraints, with several indicating their reluctance to strongly agree due to the lack of resources to commit fully to the recommendation. "Time and resources will dictate the level of investment and dedication this exercise affords," one participant remarked, illustrating the practical limitations faced. This echoes findings by Manfield and Newey (2018) who found employees were constrained in their ability to consider new practices when they were already stretched. Another highlighted the difficulty in securing support for programme managers in tight economic conditions, suggesting the integration of these roles into the incident lifecycle management process from the start as a strategic approach to circumvent funding challenges for softer skills later on.

The consensus on the necessity of testing changes to ensure they effectively address the identified causes was strong, with practitioners recognising that systems and processes naturally degrade over time. "Testing, retesting, and understanding the process and people surrounding technology solutions can be just as important as the solutions themselves," was a viewpoint that emphasised the holistic

approach needed. Reflecting this, the recommendation's title was slight tweaked in the second round for clarity on the importance of testing implemented lessons. Feedback also prompted an update to the description, emphasising prioritisation and the consideration of interim measures where resources are constrained, with one participant noting, "Prioritisation will also be necessary in all cases you need to fix the biggest and most impactful issues first."

Governance emerged as an important theme for ensuring the implementation of agreed actions, with comments highlighting the risk of apathy and fatigue diluting momentum post-incident. Elliott and Macpherson (2010) highlighted this danger between identifying the lessons and actually ensuring changes were implemented. The importance of action tracking and governance was stressed to maintain focus and ensure effective closure of actions. One insightful comment explored the psychological barriers to post-incident engagement, suggesting a prevalent desire to “move on” and a reluctance to dwell on past events, compounded by a fear of blame or shame. Such comments are aligned with the research by Edmondson (2018).

The suggestion to create a programme of sponsored work with independent governance, such as a board audit committee, was proposed by several participants to safeguard the continuity and focus of post-incident remediation efforts. Experience was cited to illustrate the short corporate memory regarding incidents and the risk of diminishing support for prolonged remediation projects. Risk management teams should ensure that any lessons learned are incorporated into broader risk assessments, and Audit Committees need to provide the necessary oversight to track the progress of implementing these lessons and ensure the implemented changes are truly reducing the risk of similar incidents in the future. One participant articulated the value of appointing a Cyber Partner to complement internal efforts with external expertise and perspective. This suggestion was added into the final recommendation description.

Significantly, the necessity of integrating substantial changes into strategic transformation programmes was mentioned, with a call for higher placement of action ownership within the organisation to enable effective decision-making and real solutions, rather than superficial fixes. This feedback encapsulates the complexities of implementing this recommendation, underlining the need for a strategic, well-governed approach that accommodates resource limitations and psychological factors influencing post-incident response and remediation.

6.3 Discussion of the Delphi survey results

In the analysis of comments against the two theoretical frameworks, the influence of neo-institutional theory was notably evident, especially the impact of coercive pressures on encouraging openness in incident reporting and fostering trusted relationships for knowledge sharing within peer groups and supply chains. Concerns were raised about the expanding legal and regulatory frameworks, perceived by some as barriers to collaboration. Yet a comparable number of participants saw legal clauses and regulatory bodies as facilitators of information exchange, a viewpoint supported by Al-ma’aitah (2022), who found that coercive pressures could enhance cyber security efforts. The necessity of contractual clauses for serious supplier engagement in security and early incident collaboration was highlighted. Despite observing variations in the effectiveness of collaboration across sectors, the study's limited industry-specific sample size offered no definitive patterns, suggesting a need for further research with broader samples to explore sectoral distinctions. Openness and sharing were valued by participants, yet identified challenges included delays and complications arising from timing, political, or classification issues.

Reflecting on the organisational learning theory, the Delphi participant feedback emphasised that incident learning might encounter obstacles such as organisational politics and cultural barriers. The critical role of senior leadership and governance in fostering an effective learning environment was

underscored, with the need for top-down support, both sponsorship and cultural, highlighted as vital yet challenging to establish. The presence of a blame culture within an organisation was seen as a significant impediment to progress, with fears of repercussions leading to a reluctance to disclose issues openly. Practitioners acknowledged the importance of addressing root causes but noted the requirements of skill, time, and attention for effective learning.

There was a noticeable concern among respondents about their capacity to implement the recommendations within their organisations, despite agreement with the principles. The need to be selective about which incidents to learn from, with concerns about over-committing resources in an already stretched environment was clear. This observation diverges from earlier recommendations by researchers, including Ahmad et al. (2012) and Bartnes et al. (2016), who advocated for organisations to learn from all incidents, not just those of high severity. This approach now appears less feasible, possibly reflecting a time when incidents were fewer and more manageable. However, participants recognised the value in analysing patterns and trends, suggesting a broader approach to incident learning. "Lower-level incidents might still be important to do a root cause analysis on," one participant observed, pointing to the potential for lesser-impact incidents to offer valuable insights. The feedback reflected a genuine motivation among practitioners to learn from incidents, albeit constrained by practical limitations such as politics, time, technical debt, skilled resources, or budget within their organisations.

6.4 Limitations of the Delphi study

In this Delphi survey, over 47 practitioners were invited, with 31 participating in the first round and 21 in the second. Although the response rates were commendable, the reduction in participation between rounds suggests a potential for self-selection bias. This bias might stem from practitioners with a particular interest in incident learning being more likely to engage with the survey. Future studies could explore methods to mitigate this bias, such as implementing a sponsorship system within organisations to encourage participation or using a random selection process with incentives to attract a broader range of respondents. Nonetheless, any strategy to increase participation must be carefully designed to avoid introducing new biases, especially considering the busy and high-demand nature of security professionals.

The research focused on validating recommendations with experts from large UK-based organisations. To broaden the applicability of the findings, additional research across various countries and smaller enterprises would be needed. Further research would be invaluable for exploring the recommendations' relevance across different organisational contexts and sectors, especially those with mixed opinions on topics like external consultancy use and peer collaboration viability.

The Delphi study method hinges on experts forecasting the practicality of recommendations within their organisations. Yet, as Linstone et al. (1975) highlighted, accurately predicting outcomes in complex systems is challenging for humans. Moreover, there might be a divergence between the experts' stated opinions and the recommendations they would practically endorse in their professional activities (Argyris & Schön, 1978). Future iterations of this study could clarify scoring instructions to emphasise evaluating the merit of recommendations independently of the feasibility of immediate implementation. Additionally, distinguishing between aspirational goals and the practical obstacles encountered by practitioners could offer deeper insights into the feasibility of achieving these recommendations. This survey begins the exploration of cyber security practitioners' perspectives on these recommendations on how to improve learning from incidents. Further research is needed to assess the acceptance, practicality, and impact of the proposed recommendations fully.

6.5 Final recommendations

This section presents the list of final recommendations which have been updated based on the feedback from the Delphi survey participants.

Final recommendation 1: Demonstrate an openness to hearing about incidents
Encourage a workplace culture that fosters openness, making it easy for customers, employees, peers, and suppliers to report incidents and near misses. Consider supporting multiple formal and informal reporting channels and incorporating reporting requirements into contracts and policies to enable sharing without negative repercussions. To encourage your employees, provide engaging and context-specific training that clearly outlines their roles and responsibilities in the reporting process. It's essential to acknowledge shared incidents, praise reporting even of mistakes, efficiently triage reports, and provide feedback on actions taken to the individuals who reported them. Evaluate stakeholders' understanding and motivation to report incidents to ensure that your organisational culture is genuinely perceived as open and to continually improve your reporting practices.

Final recommendation 2: Foster strategic trusted relationships and prioritise effective collaboration with peers and suppliers
Strengthen and prioritise trusted relationships with industry peers and suppliers to facilitate the sharing of insights from cyber security incidents and near misses. Highlight the importance of exchanging non-competitive information in structured forums and integrating early incident sharing into contractual agreements, with penalties specifically designed for cases of intentional negligence. Commit to active participation in local and industry groups, such as those supported by agencies like the NCSC, to promote collective learning. Organisations need to recognise the substantial effort needed to establish meaningful collaborations and strategically balance this against the benefits of information sharing.

Final recommendation 3: Ensure effective participation in post-incident reviews
Particularly for incidents involving intricate causes or recurring patterns, involve senior leaders, subject matter experts, system owners, and individuals responsible for implementing changes in post-incident reviews where appropriate. This can enhance awareness of risks, enable effective prioritisation, and inspire ownership of corrective actions. Consider who needs to be in the review meetings to ensure robust action plans are generated. Discuss post-incident findings in impactful governance forums to drive meaningful actions and improvements. Evaluate the allocation of time and resources to the learning process, ensuring it receives the appropriate priority for your organisation.

Final recommendation 4: Delve into underlying causes and trends
For incidents characterised by multiple or intricate causes, or recurring patterns, commit to comprehensive cause investigations and identifying contributory factors. These elements may encompass process inefficiencies, accountability gaps, legacy infrastructure, governance discrepancies, prioritisation dilemmas, supplier relations, or monitoring tool limitations. Consider if enlisting a skilled facilitator or an external expert, or applying specialised tools or methodologies would be beneficial. These strategies can aid identifying lessons which hold the potential to prevent or enhance the response to future incidents. Furthermore, routinely analyse incident metrics and trends, including lower-level incidents to detect emerging trends and recurring patterns, assess whether rectifying underlying causes could have averted certain incidents or if there are opportunities to improve the detect and response capability.

Final recommendation 5: Champion addressing structural causes
Senior leaders should emphasise the importance of addressing structural causes of incidents, even when the actions required may be less tangible, such as addressing cultural issues, enterprise

architecture deficiencies or resolving long-standing technical debt. These are challenging to tackle and may take time, so it is often necessary to enhance the detection, response, and recovery measures in the meantime. Senior leaders need to operate within the context of their organisation to set the expectation that structural causes can be improved over time, particularly where individuals may be hesitant to take personal accountability for an incident as they cannot guarantee closure. This may require executive sponsored transformation initiatives, coupled with a growth mindset that entails an ongoing evaluation of the organisation's learning and improvement processes as they evolve through incident experiences.

Final recommendation 6: Drive the implementation and testing of lessons learned
Ensure that action items identified in post-incident reviews are not only documented but also executed promptly. Use suitable governance forums within your organisation or strategic partners to make the progress of these actions transparent to senior leadership, prioritising them or embedding within other transformation programmes as needed. In cases where resources may be limited, consider implementing interim mitigating measures to address critical issues until the full resolution is feasible. Furthermore, validate the effectiveness of implemented actions through rigorous testing, encompassing activities like red team exercises, simulations, and internal audits. Ensure testing also encompasses non-technical factors, such as assessing the functionality of new accountability structures and confirming adherence to updated training protocols.

6.6 Chapter conclusion

This Delphi survey served to validate the recommendations, drawing on the expertise of professionals in the field who provided critical feedback. This input was instrumental in refining the recommendations, culminating in an updated list that lays a solid foundation for both future research and immediate application by practitioners. A recurring theme in the feedback was the challenge of dedicating sufficient effort towards meaningful learning from incidents. This underscores the notion that, without strategic investment and careful consideration, learning from incidents risks becoming a perfunctory exercise, without genuine value.

The diversity of opinions among the participants highlighted the absence of a universal solution; what works for one organisation may not suit another. This variability emphasises the necessity for organisations to tailor the recommended practices to their unique circumstances and the specific nature of incidents they encounter. The findings point towards the need for a flexible approach, allowing organisations to selectively implement the aspects of the recommendations that align most closely with their needs and objectives.

Across the two rounds of the Delphi study, the recommendations were refined to reflect expert feedback, improve clarity, and enhance feasibility. Most recommendations were retained but updated in Round 2 to address concerns raised in the first round and to allow greater flexibility in implementation. For example, the recommendation to “Delve into underlying causes and trends” rose in prominence and was revised to acknowledge divided opinions about the value of independent facilitators. While some participants emphasised their benefits for objectivity and insight, others raised concerns about trust and the impact on the dynamics of the post-incident review meetings. This divergence suggests the need for further research to better understand how context influences the perceived value of external facilitation in post-incident learning.

The recommendation to “Demonstrate an openness to hearing about incidents” was expanded to incorporate elements from the dropped evaluation recommendation, particularly the importance of assessing stakeholders’ motivation and understanding. It also addressed new concerns raised in Round 1 feedback, including the importance of tailoring training to different stakeholder groups and ensuring

that reporting systems are designed in ways that avoid overwhelming teams with high volumes of reports. Similarly, the “Ensure effective participation in post-incident reviews” recommendation was augmented to include evaluation of time and resource allocation.

The recommendation “Evaluate the effectiveness of the learning process” was removed after Round 1. Although this concept aligns with wider organisational learning literature, it received the lowest ranking in Round 1 and its removal was supported by participants in Round 2. Feedback from participants indicated they viewed it as abstract or difficult to act on, particularly when compared to more tangible practices. However, its core themes were not lost, as elements were integrated into other recommendations. Even so, further research is needed to explore why expert practitioners deprioritised this activity—whether due to lack of perceived value, the difficulty of measurement, or limited organisational incentives to reflect systematically on learning practices.

In general, several recommendations were adapted to allow greater flexibility in how they might be implemented across different organisational contexts. Round 1 feedback highlighted concerns about the feasibility of fully implementing all aspects of the recommendations, particularly in resource-constrained environments. In response, Round 2 versions were revised to give practitioners more room to tailor actions based on organisational maturity, available capacity, and specific threat landscapes.

7 Discussion

Learning from incidents provides organisations with an opportunity to enhance their response capabilities and implement measures to prevent similar occurrences. However, industry standards offer little detailed guidance on the best practices for learning from such incidents. The systematic literature review in Chapter 2 demonstrated that, while there has been some research into learning from incidents, it is not recent and predominantly focuses on understanding the causes rather than studying the barriers to effective learning practices.

This research aimed to assist organisations in mitigating the risks posed by cyber security incidents by investigating how to enhance learning from post-incident reviews. Through a series of interviews with organisations, this study explored current practices and identified challenges to effective learning. The findings contribute to the development and validation of practical recommendations for improving learning processes, thereby addressing a critical gap in existing literature and practice.

This chapter amalgamates the findings from Chapters 4-6, reflecting on these results in the context of the existing literature and acknowledging the limitations of the research. It integrates the outcomes of all the research conducted in this thesis, addressing the research questions, presenting how these were answered by the findings of the studies, and identifying new questions or areas requiring further investigation. By summarising the most impactful insights, the chapter provides a comprehensive discussion that bridges the research findings with the broader academic discourse.

7.1 Reflecting on research questions

The analysis of how each research question is addressed by the studies is presented next according to the research design set out in Chapter 3, Table 28.

Table 28 *Research findings mapped to research questions*

Research Question	Key Findings	Research
1. What organisational practices of learning from cyber security incidents have researchers found?	Researchers have identified that organisational practices in learning from cyber security incidents are limited. Learning is often restricted to technical fixes and immediate responses without addressing underlying systemic causes. Structured analysis, such as double-loop learning, is recommended but not widely adopted. Broader incident learning is often confined to major incidents and does not include rigorous follow-up on actions.	• Systematic Literature review **Chapter 2**

Research Question	Key Findings	Research
2. How do organisations currently learn from cyber security incidents, and what challenges do they experience in the learning process?	Organisations often limit their learning to major incidents, conducting post-incident reviews but rarely using structured tools or methodologies. Learning tends to focus on single-loop processes, with limited follow-up on whether actions prevent future incidents. Thematic analysis revealed challenges such as hearing about all incidents, ensuring appropriate participation in incident reviews, and overcoming defensiveness in identifying underlying causes.	• Exploratory poll, practitioner interviews and thematic analysis **Chapter 4** • Development of preliminary recommendations **Chapter 5**
3. What new approaches to improve learning from cyber security incidents can be recommended?	Preliminary recommendations developed based on the practitioner interviews which were validated through a Delphi study and refined into six final recommendations. The study highlighted the need for greater collaboration, better causal analysis, and a focus on addressing systemic causes. While the importance of learning is recognised, time and resource constraints limit organisations' ability to fully implement changes.	• Delphi study **Chapter 6**

7.1.1 RQ1: What organisational practices of learning from cyber security incidents have researchers found?

This question was addressed through a systematic literature review (Chapter 2) of cyber security research. The existing literature indicates that learning from cyber security incidents is limited. Researchers have recommended that organisations implement more structured analysis of causes (He et al., 2015; He, Johnson, Lu, et al., 2014; He, Johnson, Renaud, et al., 2014), use double-loop learning (Ahmad et al., 2012a, 2015, 2020; Jaatun et al., 2009b; Line et al., 2006; Shedden et al., 2010), and expand their learning to include a broader range of incidents. The studies noted that learning from incidents is often restricted to major incidents (Ahmad et al., 2012a, 2015; Line, 2013; Line et al., 2016; Line & Albrechtsen, 2016) and there is insufficient follow-up on actions (Grispos et al., 2017). Organisations tended to focus on technical causes (Shedden et al., 2010) and use simple classifications such as "human error" (Evans et al.(2019). The existing literature provides no evidence that organisations assess whether their learning practices effectively enhance their cyber security response capabilities or improve their overall security posture.

Comparisons with other domains, such as safety, highlight the opportunity for more extensive studies on learning from cyber security incidents to fully understand organisational practices. While some cyber security researchers have adopted models from other fields—such as Bernsmed and Tøndel's use of REWI (2013), Evans et al.'s use of HEART (2019), He and Johnson's, use of GSN (2015), Jaatun et al.'s use of STEP (2009) (see Section 2.2.3)—the full learning processes developed in safety research, which include incident reporting, confirming actions are implemented, and continuous improvement of the learning process, have not been thoroughly studied in cyber security. Collaboration across

disciplines could significantly enrich the understanding of organisational practices for learning from cyber security incidents.

7.1.2 RQ2: How do organisations currently learn from cyber security incidents and what challenges do they experience in the learning process?

To answer this research question, an initial exploratory poll with 25 participants was followed by an interview study conducted with 34 practitioners from organisations across industry sectors, as described in Chapter 4. This study examined the practices these organisations follow and aimed to uncover the challenges they face in learning from incidents. The findings revealed that all organisations in the study engaged in some form of learning from incidents, with notable similarities across the organisations. A thematic analysis of the interviews identified three key challenges.

Firstly, there was the challenge of uncovering all incidents, particularly those within their supply chain. Organisations recognised the importance of employees reporting incidents and had implemented mandatory security awareness training to support this. However, they also highlighted the difficulty of fostering a culture where individuals feel safe enough to report incidents, especially those resulting from mistakes. An unexpected finding was the extent to which organisations were cautious in sharing lessons learned due to fear of negative consequences. This concern warrants further research to fully understand its justification and the potential detrimental impact it may have on learning.

Secondly, there was the challenge of identifying the causes of incidents, beyond the obvious technical breach. Organisations in this research held post-incident review meetings for major incidents to investigate the causes, yet the majority did not use any specific tools or methodologies for these reviews. As a result, the actions taken were often limited to single-loop learning. While post-incident reports with lessons learned were typically produced and shared with senior leaders and sometimes regulators, participation in the reviews was generally restricted to those directly involved in the incident response. Although participants acknowledged the value of broader participation, they had to weigh this against the time commitment required. Moreover, since none of the organisations had assessed the value derived from learning from incidents, they had not evaluated the potential return on investment from wider participation.

Lastly, there was the challenge of implementing the lessons learned. Organisations in more regulated industries, such as the energy and financial sectors, had more structured processes for tracking actions, often logging them in risk and compliance tools with progress reported to formal governance teams. In contrast, other organisations adopted a less formal approach, where tracking progress was left to the accountability of the action owner. While this formal approach in regulated industries is effective in ensuring actions are implemented, it also carries the risk that individuals, knowing they will be held accountable, might be reluctant to take ownership. This can lead to actions being scoped only to those that can be quickly and easily achieved, potentially limiting the depth and impact of the learning process. Even in organisations where action completion was tracked, the focus was on whether the action was completed rather than on whether it effectively reduced the likelihood of similar incidents in the future.

7.1.3 RQ3: What new approaches to improve learning from cyber security incidents can be recommended?

Chapter 5 developed recommendations based on the interviews to improve learning from incidents, which were subsequently validated in Chapter 6 through a Delphi study with practitioners. This study involved two rounds of feedback, with 31 practitioners participating in the first round and 21 in the second round.

The feedback from the Delphi study revealed a complex dynamic among practitioners; while there was a persistent fear regarding the sharing of information, there was also a strong emphasis on understanding the underlying causes of incidents. This suggests that, while practitioners are keen to enhance their learning processes, they are simultaneously wary of the potential risks associated with greater transparency. However, recommendations focused on driving the implementation of changes were ranked with lower importance, indicating a disconnect between the desire for deeper understanding and the commitment to taking concrete action to implement those changes. A recurring theme in participants' comments was the concern over the time investment required for some recommendations. This concern may have contributed to the lower ranking of recommendations such as “Ensure effective participation in post-incident reviews” as participants feared the time commitment involved. This also ties into the observation that the severity of incidents often drives the level of investment in learning, with organisations lacking the resources to investigate all incidents with the same rigour.

The study also found that organisations rarely assess the effectiveness of their learning practices. Recommendations that called for more rigorous evaluation and continuous improvement might have been ranked lower in the first round because organisations are not yet accustomed to—or do not immediately see the value in—such practices. The lack of established metrics or evidence linking learning practices to improved outcomes could contribute to this reluctance. Additionally, participants may have anticipated challenges in implementation due to internal resistance, as these recommendations were seen as requiring not just a cultural shift but also a significant investment of time.

The recommendation to “Foster strategic trusted relationships and prioritise effective collaboration with peers and suppliers” received the lowest ranking in the second round, with many participants expressing concerns over potential legal and regulatory repercussions. Recommendations that involved greater transparency or the sharing of information were often ranked lower due to fears of negative consequences, such as reputational damage or legal liability.

Despite these challenges, the recommendations received strong overall support, with an average score of 70% of participants strongly agreeing with the recommendation, endorsing the round of the Delphi study. The scores, feedback, and rankings were instrumental in refining the recommendations into six validated and prioritised actions that organisations can adopt to enhance their learning from incidents. These recommendations reflect a consensus among practitioners on the most effective strategies for improving incident learning practices. For the finalised list of recommendations, see Table 29.

Table 29 *The finalised list of prioritised recommendations*

Prioritised list of final recommendations
1. **Delve into underlying causes and trends.**
2. **Champion addressing structural causes.**
3. **Demonstrate an openness to hearing about incidents.**
4. **Ensure effective participation in post-incident reviews.**
5. **Drive the implementation and testing of lessons learned.**
6. **Foster strategic trusted relationships and prioritise effective collaboration with peers and suppliers.**

7.2 Comparison with industry standards and guidance

While many of the recommendations developed in this study reflect elements found in existing standards (e.g., ISO/IEC 27035-2, NIST SP 800-61r2), the research also identifies areas where current guidance falls short. Notably, these standards often assume that organisations will implement lessons learned from incidents as a matter of course, without adequately addressing the organisational, cultural, and resourcing barriers that may prevent this. In contrast, this study highlights the real-world challenges practitioners face in translating review findings into sustained improvements, and it offers more actionable guidance to help overcome these barriers—particularly in fostering psychological safety and ensuring adequate support for learning processes.

Although CREST (Creasey, 2013) suggests techniques such as the Five Whys Approach and Fault Tree Analysis to aid in root cause analysis, only two of the organisations interviewed reported using any structured approach. Furthermore, these organisations relied on internally developed techniques rather than those recommended in the guidance. A particularly notable gap in the documents is the absence of guidance on overcoming defensiveness during post-incident reviews. The creation of a blame-free environment was seen as essential by participants in both the interviews and the Delphi study, yet this critical factor is not addressed in existing frameworks.

Another key shortcoming of the guidance documents is their lack of direction on ensuring that lessons from incidents are effectively implemented and assessed to confirm they have improved cyber security. The challenge of implementing lessons was a recurring theme in the interviews, and its significance was further reinforced in the Delphi study, where 96% of participants agreed with the recommendation to *drive the implementation and testing of lessons learned*. Additionally, the recommendation to *champion the addressing of structural causes* was ranked as the second most important, highlighting the necessity of systemic changes to enhance organisational resilience. Despite this, the industry documents reviewed provide little practical guidance on how organisations can successfully embed lessons into their processes and measure their effectiveness. Addressing this gap is crucial to strengthening organisational learning and improving incident response outcomes.

ISO 27035-2 (ISO, 2023), NIST Special Publication 800-61 Revision 2 (NIST, 2012), CREST (Creasey, 2013), and ISACA (2020) all recommend considering who should attend post-incident reviews. This study's findings support this emphasis, as participants in both the interviews and the Delphi survey recognised the importance of having the right people involved in these discussions. Participants highlighted the need to balance different perspectives and levels of seniority while also acknowledging the practical challenges of securing attendees' time and ensuring the right mix of individuals. Achieving a balance that enables open discussion, meaningful lesson identification, and clear ownership of actions was seen as critical but difficult to implement in practice.

Further research is needed to enhance existing industry guidance documents to better support organisations in learning from incidents. The gaps identified in this research highlight the need for clearer, more actionable recommendations on root cause analysis, fostering a blame-free learning environment, and ensuring the implementation and assessment of lessons. Addressing these deficiencies could contribute to improving organisational learning from cyber incidents.

7.3 Comparison with existing scholarly literature

This research contributes significantly to the existing body of knowledge by uncovering more advanced practices of learning from cyber security incidents than those identified in earlier studies. The inclusion of 34 large multinational organisations from various industries, combined with how up-to-date the research is, provides a broader and more nuanced understanding of these practices. This breadth and recency contrast with prior research, which often focused on individual case studies (Ahmad et al.,

2012, 2015; Grispos et al., 2017) or smaller, industry-specific samples (Bartnes et al., 2016; Jaatun et al., 2009). Additionally, this research was enriched by a Delphi study involving two rounds of feedback from practitioners, which allowed for the validation and refinement of the findings. This approach ensures the study is not only more comprehensive but also addresses the limited research conducted in this area in recent years, making it particularly relevant and up-to-date.

7.3.1 Organisational learning practices

In Chapter 2, the literature review identified a recurring theme of limited and often superficial learning from cyber security incidents. The findings from this thesis support these observations, particularly in the widespread reliance on single-loop learning. Organisations frequently focus on addressing immediate technical issues without examining the broader systemic factors contributing to recurring incidents. This aligns with the work of Argyris and Schön (1978) who emphasised that single-loop learning—where feedback is used to adjust actions without challenging underlying assumptions—restricts an organisation's capacity for deeper learning. As a result, organisations miss opportunities to strengthen their security and prevent similar incidents in the future.

This research also highlights the emergence of more advanced practices in organisations with higher maturity levels in incident response. Notably, some organisations are recognising the value of analysing low-severity incidents to identify patterns and trends that could pre-empt larger issues. This proactive approach reflects an understanding of how small, seemingly isolated events can expose systemic vulnerabilities. In addition, the principles of learning from near misses, as advocated by safety researchers such as Dekker and Pruchnicki (2014) and Line et al. (2014), are increasingly being applied to cyber security. These researchers stress the importance of leveraging near misses to uncover weaknesses that may not become evident during major incidents, ensuring organisations are better prepared for future challenges. Such practices were not found in earlier cyber security studies, indicating a potential shift in how mature organisations approach incident learning.

The Delphi study conducted in this research reinforced these findings through its iterative feedback process, which enabled practitioners to validate and refine recommendations. The prioritisation of recommendations further highlighted the importance of addressing underlying causes and systemic issues. Specifically, "Delve into underlying causes and trends" and "Champion addressing structural causes" were ranked as the top priorities (see Chapter 6), reflecting a growing recognition among practitioners of the need to go beyond surface-level solutions. These findings indicate further insights could be drawn from cross-disciplinary comparisons, particularly with safety science.

7.3.2 Cross-disciplinary insights

The findings from this research suggest significant value in drawing on insights from other disciplines, particularly safety science, to enhance learning from cyber security incidents. Safety research has long emphasised the importance of understanding incidents not just as linear sequences of events but as complex interactions within socio-technical systems (Larouzee & Le Coze, 2020; Le Coze, 2013). This perspective contrasts with the more reductionist approaches often seen in the cyber security literature, where causes are frequently viewed as straightforward and linear—a control failure, for instance, is often attributed as the primary cause without considering the broader context.

In this research, participants in the interview studies frequently attributed incidents to failures of specific controls, reflecting the linear cause-and-effect thinking that is prevalent in cyber security practices. This tendency aligns with previous studies, where the causes of incidents are often simplified to technical failures or human errors, overlooking the complex interplay of organisational, cultural, and social factors that also contribute to incidents.

Safety science offers a more nuanced and complex understanding of incident causation. Researchers in this field have demonstrated that the narrative of an incident's causes is not simply discovered but is socially constructed during the investigation process (Dekker, 2012; Le Coze, 2013). This means that what is identified as the "cause" of an incident is heavily influenced by the perspectives, biases, and interactions of those conducting the investigation. The work of Drupsteen and Guldenmund (2014) and others in safety research highlights that incidents should be viewed as an event emerging from a combination of factors across different layers of the socio-technical system, rather than as the result of a single point of failure.

This research also supports this more complex view, as some participants acknowledged that their organisations' incident reviews often overlooked underlying systemic issues, focusing instead on immediate, tangible failures. For example, while a control failure might be identified as the cause of a security breach, the underlying reasons for that control's inadequacy—such as organisational culture, inadequate resources, or communication breakdowns—are often left unexplored. This reductionist stance limits the effectiveness of learning from incidents, as it prevents organisations from addressing the deeper issues that contribute to their vulnerabilities.

While some studies have adapted safety cause analysis methods (He et al., 2015; He, Johnson, Lu, et al., 2014; He, Johnson, Renaud, et al., 2014; He & Johnson, 2015, 2017), further research is needed to explore how more sophisticated cause analysis methods from the safety domain could be applied to cyber security incidents. Additionally, it is important to investigate why these methods have not been widely adopted by organisations, as the participants in this research were not using them.

The current standards for cyber security incident management, such as ISO/IEC 27035-2 (2023) and NIST Special Publication 800-61 Revision 2 (2012), primarily focus on the operational aspects of incident response, offering limited guidance on how to investigate and learn from incidents in a way that captures their complexity. These standards could be significantly enhanced by incorporating approaches from safety science that emphasise a systemic understanding of incidents. Techniques such as HFACS, AcciMap, and STAMP—discussed in Chapters 2 and 5—highlight the importance of addressing multiple layers of causation within a socio-technical system.

Moreover, safety research stresses that the process of learning from incidents involves constructing a narrative that not only explains what happened but also how and why it happened within the specific context of the organisation. This narrative construction is inherently social, shaped by the interactions and perspectives of those involved in the investigation (Le Coze, 2013). In contrast, the cyber security literature often treats incident causation as a more objective process, overlooking the subjective elements that influence how causes are identified and understood. This mindset was reinforced by the interviewees who reported that post-incident reports are usually just accepted by senior executives without any questioning of the processes used to identify the causes.

Prior studies in the cyber security domain have attempted to improve cause analysis by adopting techniques from engineering and safety science (Ahmad et al., 2012, 2015; Evans et al., 2019; He, Johnson, Renaud, et al., 2014; He & Johnson, 2015). However, these efforts have often remained within a reductionist framework, focusing on technical solutions while neglecting the organisational and social dynamics at play. Edmondson (2023) pointed out that, although learning from incidents is logically appealing, the realities of workplace emotions and power dynamics can obstruct the objective analysis necessary for thorough investigations and effective corrective actions. The findings from this research also hint at these elements coming into play through the comments about who participates in the reviews and the need to recommend deeper dives into the underlying causes, yet further research into this in a cyber security context is required.

There is a clear need for further research to uncover not only effective tools and techniques for cause analysis but also best practices for conducting thorough investigations that consider both technical and social factors. By integrating these cross-disciplinary insights, organisations can develop more robust learning practices that address immediate incident response needs and contribute to long-term resilience. Future research should continue to explore these intersections between safety science and cyber security, with an emphasis on enhancing the standards and practices used in cyber incident management to reflect a more holistic understanding of incident causation.

7.4 Comparison of findings with theoretical framework

This research used two theories to contextualise the collection and analysis of data: neo-institutional theory and organisational learning theory. Neo-institutional theory was employed to understand how external pressures may shape an organisation's learning practices from incidents, while organisational learning theory illuminated the internal influences impacting the learning process. Together, these theories provided a comprehensive framework for analysing the findings.

Neo-institutional theory explains how practices are shaped by isomorphic pressures of a coercive, normative, and mimetic nature, leading organisations to adopt similar practices without evaluating their effectiveness. Organisational learning theory provides insights into the challenges organisations face in the learning process, particularly the tendency to avoid questioning governing assumptions, which limits learning to superficial lessons.

The findings of this research largely support neo-institutional theory, as organisations reported adopting similar practices without evaluating their suitability or effectiveness. Notably, the recommendation to evaluate learning practices was the least supported in the first round of the Delphi study and was subsequently dropped as a standalone recommendation, although aspects of this recommendation were embedded in the revised version of the recommendations used in round 2, reflecting the suggestions from some respondents. The criticism of the preliminary recommendation on evaluating learning practices was that organisations did not have the time to invest in what was perceived as less essential than performing the practices (Fast et al., 2014)

The similarity of the processes reported in the interviews suggests that normative pressures shaped how organisations conducted mandatory training to encourage incident reporting and held post-incident reviews for high-severity incidents, resulting in reports with action items. However, there were differences in incident classification, participant involvement, and action tracking, reflecting minor adaptations to organisational needs. These findings support the proposition that practices are influenced by normative pressures, creating similarity across organisations.

Coercive pressures, in terms of regulation and legal factors, were surprisingly prevalent. For some interview participants, these pressures influenced how actions were written and reported in the course of sharing with regulators. As a result, they wanted to ensure they could complete the actions before agreeing to them as lessons. Many participants indicated that coercive pressures negatively affected their willingness to share lessons with peers or within their supply chain ecosystem. This reluctance is disappointing as it reduces the opportunity for organisations to learn from each other.

The Delphi study participants were concerned about the recommendation to share lessons; they recognised its importance and the benefit of learning from others but feared negative repercussions from sharing. Some suggested that regulators could play a role in facilitating this exchange. The UK's National Cyber Security Centre (NCSC) has created trust groups to encourage the sharing of lessons publicly (Ralph, 2024). Coercive pressures also influenced how practitioners used contracts to require suppliers to report incidents, although many lamented the ineffectiveness of these measures.

There were fewer strong examples of mimetic pressures in the findings. However, some practitioners did mention using incidents at peer organisations as a rationale to justify security investments within their own companies. Additionally, they noted that regulators and Audit Committees often expected post-incident reports because this was standard practice in other organisations. Despite this, there was no evidence provided to suggest that these post-incident reviews had effectively helped organisations prevent future incidents.

Interviewees recognised that defensiveness, as described in organisational learning theory, can hinder efforts to identify the underlying causes of incidents, ultimately limiting the lessons that can be learned. This aligns with the Delphi participants' ranking of "Delving into underlying causes and trends" as the most important recommendation.

The interview participants reported that team members tended to identify single-loop solutions, as these were within their control, and more senior leaders were needed in post-incident reviews to identify the deeper, systematic changes required. Interviewees also noted that reports produced were rarely critically scrutinised by senior executives, supporting organisational learning theory's description of organisations' reluctance to discuss deeper governing assumptions that might expose their inadequacies (Argyris, 1999).

In the interview study, participants suggested that actions agreed upon as lessons from incidents often reflected the CISO's preferences, or justified pre-planned investments, rather than being determined by rigorous investigation of causes and optimal actions. The limited evaluation of the effectiveness of lessons, beyond the action being completed, supports Meyer and Rowan's (1977) view that such practices are followed more to demonstrate an organisation's legitimacy rather than to challenge the organisation to question and refine its operations.

Many participants highlighted the importance of a no-blame culture, emphasising that incident reporting and post-incident reviews should be conducted without blaming individuals. This was the case right from the initial exploratory poll, where embracing a no-blame culture was seen as the most important factor for improving learning from incidents up to the Delphi study, where many comments referenced the need for a psychologically safe environment. This supports studies in the medical field by Edmondson (2023, 2004) that learning is hindered if individuals fear speaking out (Swuste et al., 2020). The studies in this research support the organisational learning theory that learning from incidents is challenging due to organisational defences and the need for a no-blame approach. Organisations need to consciously invest time and effort to create psychologically safe environments where leaders are willing to question their own choices and encourage employees to question deeply held assumptions.

7.5 Practical implications and implementations of findings

This research emphasises practical strategies for enhancing incident learning within organisations, particularly larger enterprises that frequently encounter security incidents. The recommendations provided are tailored to guide key decision-makers (such as CISOs, Heads of Incident Management, and senior business leaders) by proposing targeted actions aligned with their roles. Additionally, the Audit and Risk Committees play a crucial role in ensuring that improvements are consistently monitored and evaluated. These recommendations are grounded in rich data obtained from practitioner interviews, which explored the challenges organisations face and their impact on effective learning practices. The data provided insights into specific challenges encountered by organisations, and the initial recommendations were developed by integrating these insights with findings from the literature. These preliminary recommendations were refined and validated through two rounds of the Delphi study. The feedback collected was systematically evaluated and incorporated into the final recommendations, ensuring they are practical.

7.5.1 Assessing the effectiveness of learning practices

A key practical implication of this research is the need for organisations to explicitly assess the effectiveness of their current learning practices. By reflecting on what is working well and identifying areas for improvement, organisations can fine-tune their learning processes for greater efficacy. Senior business executives should take a proactive role in ensuring that the strengths and weaknesses of their learning practices are well understood across the organisation, enabling the practices to be improved. This reflection process should be built in as part of a continuous improvement strategy, fostering a culture that values learning and adaptation.

The wider literature consistently advocates for a continuous improvement approach to incident learning. However, feedback from Delphi participants suggested that many organisations are not yet in a position to robustly evaluate their learning processes. The recommendation to "Evaluate the effectiveness of the learning process" was the least supported in round one and was subsequently removed from round two, although some of its elements were embedded within other revised recommendations. Several participants indicated that while evaluation was theoretically important, it felt premature or impractical given their current levels of organisational maturity. Some viewed it as a lower priority compared to more immediate post-incident response activities, echoing earlier findings from the interviews that learning efforts often focus more on execution than reflection.

These insights suggest that meaningful evaluation may require a baseline of maturity in learning practices—something only now becoming feasible as organisations increasingly adopt structured and frequent post-incident reviews in cyber security contexts. As such, further research is needed to explore the barriers organisations face in evaluating their own learning from incidents. Understanding these obstacles—whether they relate to metrics, resourcing, leadership engagement, or organisational culture—will be critical to enabling a shift from reactive response to continuous improvement.

Furthermore, assessing the effectiveness of learning practices is crucial for determining how much effort organisations should invest in these activities. This includes evaluating the appropriate time spent on investigations, determining the number and roles of participants in post-incident reviews, and ensuring that the changes made as a result of lessons learned are actually effective in mitigating future incidents. Without such assessments, organisations risk adding additional controls or bureaucracy that may not reduce the prevalence of incidents, potentially diverting resources away from more impactful actions. The effectiveness of learning practices for cyber security incidents has not been extensively studied beyond the identification of causes, and more research in this area would provide valuable practical guidance.

As discussed in Chapter 2, it is challenging to robustly measure incidents, and much of the existing research operates on the implicit assumption that learning from incidents is beneficial, without explicitly confirming this through evidence. Measuring the efficacy of learning in reducing the number of future incidents is extremely difficult due to the lack of independent or reliable sources of incident data readily available to academic researchers (Salane & Jay, 2011). While measuring impact is challenging, organisations could explore whether investment in learning correlates with a reduction in significant incidents within an organisation, based on internal metrics such as incident frequency, impact, and time taken to restore. Additionally, examining repeat incidents or recurring causes—such as multiple incidents linked to insecure coding practices—could highlight areas where improvements in the learning process are needed. Moreover, those accountable for learning from incidents could elicit the perspectives from other stakeholders within the organisation to understand their views on the effectiveness of the learning.

Additionally, evaluation is necessary to understand if organisations are truly hearing about all the incidents they need to know about. Many interview participants expressed confidence that their organisations had an open culture where people felt comfortable reporting incidents; however, none had actually assessed whether this was the case. This gap highlights the need for further research to explore the effectiveness of organisational reporting cultures and whether they are successfully capturing all relevant incidents. Understanding this aspect of incident reporting is essential for ensuring that learning practices are comprehensive and that no critical incidents are overlooked.

7.5.2 Enhancing transparency and information sharing

The research highlighted significant concerns among organisations about incomplete information on incidents, particularly within their supply chains. This aligns with broader industry concerns reported in the World Economic Forum (in collaboration with Accenture) (2023), where 90% of 300 respondents expressed worries about the cyber resilience of their third-party partners. While challenges related to regulators and litigation remain complex and long-standing, there are clear opportunities to foster a culture of openness both within organisations and across industries. Participants identified the aviation industry as a model of best practice, where a deeply ingrained culture of openness and information sharing has enhanced safety and resilience. Adopting similar approaches in cyber security could improve collaboration and shared learning, ultimately strengthening collective defences.

Despite this potential, the research also uncovered a widespread reluctance to share information due to fears of reputational damage or legal repercussions. This hesitancy restricts the flow of critical information that could drive collective learning and bolster resilience. To overcome this, organisations need to cultivate forums and partnerships where information can be exchanged securely and with trust. Strengthening relationships within supply chains is essential for creating an environment where lessons can be shared openly and constructively, benefiting all parties involved.

Regulators and national security agencies could also play a more proactive role in facilitating information sharing. Initiatives such as the UK's National Cyber Security Centre (NCSC) industry trust groups provide a secure and trusted environment for sharing sensitive information and could serve as a model for other sectors and regions. By creating similar frameworks, agencies can help to break down barriers to collaboration and enable wider dissemination of valuable insights.

Additionally, organisations should critically examine whether guidance on information sharing given by their legal teams is overly cautious. The research indicates that perceived risks often outweigh evidence of actual negative consequences. By reassessing legal frameworks and adopting a more balanced approach, organisations can mitigate these concerns while still protecting their interests. Shifting to a mindset that prioritises the collective benefits of shared learning over individual fears is essential for fostering a more open and collaborative approach to cyber security.

7.5.3 Participation in the incident investigation

The research underscores the importance of carefully considering who participates in post-incident casual analysis. It is critical for organisations to involve individuals who can contribute the most to understanding the factors that led to the incident and identifying actions with the greatest potential to prevent similar issues in the future. Diverse teams, as noted by Elliott and Macpherson (2010), are essential for identifying comprehensive lessons, as individuals' prior experiences often constrain the actions they can envision. Depending on an organisation's culture, size, and nature, different causal analysis techniques may be appropriate. Leaders should encourage iterative learning and experimentation to address complex issues, ensuring that the chosen technique aligns with the organisation's specific needs and the nature of the incident. Structured discussions facilitated by these

techniques can help delve deeper into the underlying factors contributing to an incident, beyond its immediate cause.

7.5.4 Ensuring the implementation of lessons learned

It is critical to recognise that simply identifying a lesson does not protect an organisation—cyber resilience is only enhanced when concrete actions are taken to address the contributing factors. Organisations may have different governance structures and methods for tracking progress on these actions, but it is vital to ensure that follow-up is rigorous and that necessary actions are implemented effectively. Some lessons may require significant efforts to address structural causes, which can be challenging for organisations to implement. Leaders must create the necessary conditions, including the allocation of resources, prioritisation, and recognition, to enable progress on these demanding changes. Strong leadership is essential to ensure that lessons are not only learned but also acted upon in a way that enhances the organisation's security posture.

This study provides practical implications for organisations seeking to enhance their learning from cyber security incidents. The finalised list of prioritised recommendations, as presented in Table 30, offers a clear path forward. By assessing the effectiveness of current practices, fostering a culture of openness, employing appropriate causal analysis techniques, and ensuring the implementation of actions, organisations can strengthen their cyber resilience and improve their overall security posture. These practical steps, supported by committed leadership and a focus on continuous improvement, will contribute to a more robust and proactive approach to cyber security.

Table 30 *Summary of responsible parties mapped to final recommendations*

Recommendation	CISO	Heads of Incident Management	Senior Business Leaders	Audit and Risk Committees
1. Delve into underlying causes and trends	Create an effective learning environment and encourage systemic reflection on causes and reviews of trends.	Provide the data needed to identify underlying causes and conduct trend analysis of lower-level severity incidents.	Create an effective learning environment and encourage systemic reflection on causes.	Probe post-incident reports to ensure systemic factors are reviewed and themes identified.
2. Champion addressing structural causes	Advocate for long-term fixes and shape business cases to secure funding.	Support the analysis of structural causes and provide data needed for business cases.	Allocate resources and support for structural changes.	Oversee resource allocation and follow-up assessments.
3. Demonstrate an openness to hearing about incidents	Advocate blame-free reporting of incidents, positively acknowledging when incidents are reported.	Provide channels to enable the reporting of incidents, ensure these are investigated and updates given to those who report.	Create an environment where employees feel safe reporting incidents.	Encourage openness in reporting incidents to the committee and querying low levels of incident reporting.
4. Ensure effective participation in post-incident reviews	Lead coordination, ensure appropriate participants in the review.	Provide the details of the incident and suggest improvements to the response.	Encourage participation from cross-functional teams.	Monitor governance and ensure key participants are involved.

Recommendation	CISO	Heads of Incident Management	Senior Business Leaders	Audit and Risk Committees
5. Drive the implementation and testing of lessons learned	Ensure actions from reviews are tracked, reported and implementation challenges escalated.	Implement actions to support incident response improvements and support testing of other actions where applicable.	Ensure actions from reviews are tracked, reported and implementation challenges escalated.	Provide governance to monitor and where applicable test that lessons are implemented.
6. Foster strategic trusted relationships and prioritise effective collaboration with peers and suppliers	Build peer and supplier relationships at the CISO level for shared learning.	Build peer and supplier relationships at the Incident Response team level for sharing lessons.	Oversee collaboration in industry forums.	Enable sharing between organisations where applicable.

7.6 Limitations

This research has primarily focused on practitioners from UK-based companies, specifically targeting senior personnel within security functions. While these individuals provided a broad and strategic view of organisational practices, the perspectives of more junior team members—who may be closer to the operational details—were not explored. Additionally, insights from other stakeholders within the organisation, such as those in non-security roles, were not captured. For instance, as He and Johnson (2015, 2017) demonstrated by interviewing doctors and nurses in a hospital setting, different organisational roles can offer diverse and valuable perspectives. Future research could expand on this by including a wider range of participants across various roles and levels within organisations.

The recommendations presented in this study are derived from the insights provided by the interviewed practitioners and from existing studies related to learning from incidents. Given the broad nature of learning as a general topic, this research was necessarily selective, focusing on studies and theories that appeared most relevant to cyber security incident learning. Consequently, the scope of this work did not encompass every potential study that could inform the improvement of learning practices. A more exhaustive exploration of the broader literature could potentially yield additional insights.

This research addressed RQ2 by examining the learning practices employed by UK-based organisations, drawing data from 34 large companies. While these findings provide valuable insights, the limited geographic and organisational scope restricts the generalisability of the results. To determine whether these findings are representative of a broader cross-section of businesses, further studies involving a more diverse range of organisations in different locations, of varying sizes, and with a larger number of participants are necessary.

As with any qualitative research, the findings of this study are shaped by the interpretive lens of the researcher (Pilgrim, 2014). The interviews and subsequent thematic analysis were conducted with rigour and reviewed with the supervisory team, yet it is acknowledged that another researcher might arrive at different themes. In answer to RQ3, the corroboration of preliminary recommendations through a Delphi study, which included participants who were not involved in the initial interviews, provided an additional layer of validation. However, it is important to recognise that this Delphi study does not represent a statistically significant sample of the broader population of practitioners.

The theoretical frameworks employed in this study—neo-institutional theory and organisational learning theory—were selected for their applicability and usefulness to the research questions. However, it is possible that the use of different theoretical frameworks could have led to alternative interpretations or findings. For instance, while this study supported the influence of isomorphic

pressures as described by neo-institutional theory, it did not attempt to quantify the relative impact of these pressures. Future research could delve deeper into quantifying these influences to provide a more nuanced understanding.

The fieldwork for this research was conducted at a specific point in time, capturing a snapshot of organisational learning practices. The findings indicate that organisations today may be more advanced in their learning practices compared to previous studies, many of which were conducted over a decade ago. This evolution could reflect broader changes in cyber security practices. To understand these trends more comprehensively, longitudinal studies would be beneficial, offering insights into how cyber security practices evolve over time.

It is important to acknowledge that the participants in this study were volunteers, which may suggest a pre-existing interest in learning from incidents. This self-selection bias could mean that the findings are not fully representative of organisations that do not prioritise incident learning. Future research that includes a broader range of organisations—especially those with less emphasis on learning—might produce different results. It would be valuable to compare whether organisations that place less importance on learning experience a higher frequency of incidents. However, such comparisons are challenging due to the subjective nature of classifying and counting incidents. Researchers might explore conducting experiments to enhance learning practices in these organisations and assess the perceived benefits, particularly in those that had previously undervalued learning from incidents.

Additionally, this study covered a limited range of industries due to practical constraints. Research focused on particular sectors—such as charities, critical national infrastructure, or government departments—could uncover sector-specific differences in learning practices. Insights from industries with more mature learning practices could provide valuable guidance for sectors that are less advanced in this area. Alternatively, identifying differences across sectors could shed light on industry-specific challenges to learning, helping organisations address and remove barriers more effectively.

Finally, while this study sought feedback on the proposed recommendations, it did not involve the implementation or testing of these recommendations. The research relied on practitioners' views regarding their feasibility and effectiveness. Future studies could undertake controlled experiments across different companies or divisions to empirically test the recommendations. Such empirical validation would strengthen the practical applicability of the recommendations and provide more robust evidence of their effectiveness.

7.7 Chapter conclusion

This chapter provided a comprehensive synopsis of the findings from the research conducted in this thesis, comparing them with existing literature and theoretical frameworks, and discussing their practical implications and the limitations of this research. The findings extend the current understanding of organisational learning from cyber security incidents, highlighting both advancements in practice and areas that remain a challenge for organisations.

The findings reveal that, while some organisations are adopting more sophisticated practices for learning from incidents, there remains a significant reliance on single-loop learning and a tendency to address only the immediate, technical causes of incidents. The study's insights into the challenges of time constraints, limited participation in post-incident reviews, and the cautious approach to sharing information underscore the complexities organisations face in fully realising the benefits of learning from incidents. The prioritisation of recommendations, validated through the Delphi study, reflects a growing recognition among practitioners of the need to dig deeper into underlying causes and to champion systemic changes within their organisations.

This research also underscores the importance of assessing the effectiveness of learning practices. Without such assessments, organisations may struggle to justify the investment of resources in deeper investigations or in broadening participation in learning activities. The reluctance to share lessons, driven by fears of negative consequences, further limits the learning across supply chains, highlighting the need for trusted forums and stronger national or industry forums to facilitate more open exchanges of lessons.

From a theoretical perspective, the findings support the applicability of neo-institutional theory and organisational learning theory in understanding the factors that shape learning practices within organisations. These frameworks have provided valuable insights into how external pressures and internal dynamics influence organisational behaviour in the context of cyber security incidents. However, the complex nature of cyber security learning practices suggests that there may be value in exploring alternative or complementary theories in future research. By considering other theoretical perspectives, researchers can deepen the understanding of the diverse factors that impact learning from incidents and potentially uncover new strategies for enhancing organisational resilience.

The practical implications of this research are clear: organisations must critically evaluate their learning practices, foster a culture of openness, involve the right participants in post-incident reviews, and ensure that identified lessons are implemented effectively. By doing so, they can enhance their cyber resilience and improve their overall security posture. However, the limitations of this study—such as its focus on UK-based organisations, the potential for self-selection bias, and the reliance on qualitative data—must be acknowledged. Future research should seek to address these limitations, providing a broader, more representative understanding of organisational learning from cyber security incidents.

This thesis contributes to the ongoing discourse on cyber security incidents by offering actionable insights and recommendations for improving organisational learning practices. It also highlights the need for further research to explore the evolving nature of these practices, the impact of external pressures, and the role of organisational culture in shaping how incidents are understood and addressed. By building on the findings presented here, future studies can continue to advance the field, ultimately helping organisations to better protect themselves in an increasingly complex and threatening cyber landscape.

8 Conclusion and future work

This concluding chapter summarises the research presented in this thesis in the context of aims underpinning the research questions that were presented in, Section 1.5. Section 8.2 presents the contributions of this work to the body of knowledge and outlines its significance. Section 8.3 reflects on the research design and results to critically assess the validity and generalisability of the findings. Concludes this chapter, Section 8.4 suggests potential avenues for future research to build upon the findings of this thesis concludes this chapter.

8.1 Addressing the research questions

This thesis set out to investigate how organisations can improve their learning from cyber security incidents. The research was driven by three core research questions, see
Table **28**. Adopting a mixed methods approach grounded in a pragmatist research philosophy, the study combined qualitative methods (34 interviews) with quantitative methods (a poll and a two-round Delphi study with 31 and 21 responses, respectively). This approach leveraged the strengths of both methodologies to provide a comprehensive understanding of the research topic. Through a systematic literature review, practitioner insights, and expert feedback, the research examined current practices, identified key challenges, and proposed validated recommendations for improvement.

Unlike many other cyber security studies discussed in Chapter 2, these findings are drawn from a diverse group of participants at the CISO or senior level in large organisations. This research is broader in scope, encompassing more organisations and focusing specifically on the learning process. It offers valuable insights from senior practitioners on how to enhance organisational learning from incidents. Furthermore, unlike the predominantly technology-centric and engineering approaches often seen in the cyber security field, this study adopts a socio-organisational perspective. By employing Neo-Institutional Theory and Organisational Learning frameworks, it examines the practices and challenges organisations face in leveraging incidents to derive meaningful lessons.

The findings presented in Chapters 4 to 6 offer a comprehensive view of how large organisations currently learn from cyber security incidents and how these practices might be improved. Chapters 4 and 5 analysed practitioner interviews and relevant literature to identify common challenges and learning behaviours, while Chapter 6 validated a set of recommendations through a Delphi study. Chapter 7 provides a critical discussion of the study's findings in relation to the research questions, highlighting their theoretical and practical significance. It includes a mapping of the findings to the research questions (
Table **28**), offering a structured synthesis of how the evidence from interviews and the Delphi study addresses the aims of the thesis.

This thesis applied neo-institutional theory and organisational learning theory to contextualise the findings. Neo-institutional theory helped explain how coercive, normative, and mimetic pressures influence the adoption of incident learning practices—often without a critical assessment of their effectiveness. In particular, coercive pressures such as legal liability and regulatory scrutiny were found to discourage open reporting and information sharing. In contrast, organisational learning theory highlighted the importance of psychological safety and a blame-free culture in supporting more meaningful, double-loop learning. Organisations that fostered open discussion and treated incidents as opportunities for learning, rather than failure, were more likely to address systemic issues and improve resilience.

8.2 Contributions to knowledge

This research makes several important contributions to the field of incident learning within the cyber security domain. Table 31 summarises these contributions, which are detailed further in the subsequent text.

Table 31 *Summary of contributions*

No.	Contribution	Description
1	New synopsis of research on incident learning	The systematic literature review provided a comprehensive synthesis of existing research, identifying core elements and gaps in incident learning practices.
2	Breadth and recency of findings	The study included a larger, more varied sample across multiple industries, providing updated perspectives on incident learning.
3	A greater understanding of the challenges in incident learning	The findings provided detailed insights into practical challenges, such as hearing about incidents and ensuring diverse participation in post-incident reviews, were uncovered.
4	Practical recommendations	Six recommendations were developed and validated, giving organisations guidance on how to improve their learning practices.
5	Insights from other disciplines	The study highlighted the value of applying investigative techniques from safety science and other established fields.
6	Theoretical application	The analysis of findings applied neo-institutional and organisational learning theories to reveal the socio-technical and regulatory pressures shaping incident learning.

Contribution 1: A new synopsis of research on learning from cyber security incidents: The systematic literature review (Chapter 2) provided a new synthesis of the existing research on learning from cyber security incidents. The review identified the essential elements of an effective incident learning process, offering a foundation for future researchers to build upon. By consolidating findings from across the literature, this synthesis highlighted not only the gaps in current research but also the core practices that are necessary for organisations to effectively learn from incidents. The review also pinpointed future research opportunities, particularly in areas such as the evaluation of learning effectiveness, cross-industry comparisons, and the role of organisational culture in shaping learning processes. This synopsis enables researchers to refine their focus on key aspects of incident learning and serves as a valuable resource for both academic study and practical application in the field of cyber security.

Contribution 2: Breadth and recency of findings: This study explored a larger sample size and more varied industries than many previous studies, bringing a more up-to-date perspective on incident learning practices (Chapter 4). The inclusion of multinational organisations across multiple sectors allowed the findings to extend beyond industry-specific or case-study-based insights (as found in the literature review). Given the current prevalence of cyber security incidents, these contributions are even more critical, as they provide timely and broadly applicable insights that can enhance organisational preparedness and resilience across industries.

Contribution 3: A greater understanding of the challenges in incident learning: A key contribution of this research is its provision of a deeper understanding of the multifaceted challenges that organisations face in learning from cyber security incidents (Chapter 4). While industry standards such as NIST Special Publication 800-61 Revision 2 (2012) and ISO/IEC 270035-2 (2023) recommend learning from incidents, this study highlights the gap between these recommendations and the practical difficulties in executing effective learning processes. The research identified four main challenges across the entire learning practice.

First, organisations struggle to hear about all the incidents that occur—particularly minor ones or those within their supply chains—which limits their ability to gain a comprehensive view of risks and trends. Second, ensuring that the right people participate in post-incident investigations is challenging, with many organisations failing to engage a diverse group of stakeholders who could provide broader perspectives. Instead, they often limit participation to those directly involved, missing out on valuable insights. Third, this study revealed the difficulty of overcoming organisational defensiveness, which inhibits the exploration of underlying causes, particularly when addressing systemic issues that could implicate broader processes or leadership decisions. Lastly, the challenge of implementing lessons learned is significant, with organisations often failing to follow through on actions or assess whether changes effectively mitigate future incidents.

This research not only confirms the limitations of single-loop learning—where organisations focus on addressing immediate technical fixes—but also reveals some more advanced practices in organisations with higher levels of maturity. These organisations are beginning to address the deeper challenges and adopt more structured, holistic approaches to incident learning. Thus, this research provides a greater understanding of the obstacles to effective learning and highlights where organisations can make meaningful improvements to enhance their learning practices.

Contribution 4: Practical recommendations: The research developed a set of six recommendations, validated through the Delphi study (Chapter 7), aimed at improving organisational learning from cyber security incidents. These recommendations provide guidance that large organisations can implement to enhance their learning practices, including fostering greater participation, addressing structural causes, and improving the rigour of post-incident reviews.

Contribution 5: Insights from other disciplines: This study highlighted the value of drawing from more established fields such as safety science, aviation, and healthcare, which have a longer history of research into incident learning (Chapters 2 and 5). Safety science, in particular, has developed over several decades and offers well-documented investigative methods and frameworks that are highly relevant to cyber security. The safety field has evolved to incorporate both technical and organisational factors in its incident investigations, with an emphasis on learning from not just major incidents but also near misses and smaller-scale events. By adopting investigative techniques from these disciplines—such as more comprehensive incident reporting systems and detailed post-incident analysis—cyber security organisations can enhance their learning processes. The historical depth and breadth of research in these fields provide a valuable foundation from which cyber security can learn, accelerating the development of effective incident learning practices in a shorter time frame.

Contribution 6: Theoretical application: The application of neo-institutional and organisational learning theories to the domain of cyber security demonstrated their relevance in understanding the pressures that shape incident learning practices (Chapter 3). Neo-Institutional Theory, in particular, highlighted how coercive pressures, such as regulatory requirements and legal concerns, are shaping the sharing of lessons learned between organisations. This is an important finding for governments and regulators aiming to foster greater collaboration and lesson-sharing across industries to improve overall security and bolster national resilience. Organisational Learning Theory, on the other hand,

helps shift the focus in cyber security from a traditionally engineering-based perspective—where incidents are often viewed as caused by the failure of a specific component—towards a systems-thinking approach. This approach recognises that incidents result from complex socio-technical relationships and organisational choices. Moreover, it underscores the critical point that causes and lessons are not simply objective facts waiting to be uncovered; they are socially constructed through the investigation process. Understanding that causes and lessons are shaped by social interactions, rather than existing independently, highlights the need for organisations to critically engage in their learning processes, recognising the subjective nature of these insights.

8.3 Reflective critique of the research

Beyond the methodological challenges outlined in Chapter 3, this research acknowledges the inherent limitations of its empirical work. While the study sample was broad, it focused on large, UK-based organisations, which may limit the generalisability of the findings. Moreover, the self-selection of participants could suggest a bias towards organisations already interested in improving their incident learning practices, potentially skewing the results toward more mature approaches. A study with greater diversity across industries may yield different outcomes. Additionally, this research concentrated on UK-based businesses with between 400 to 200,000 employees. Different findings may emerge from studying non-UK businesses, smaller companies, or non-commercial organisations such as charities. Although many of the organisations were international, with participants from multinational backgrounds, the predominantly Western and Global Northern perspectives likely influenced the findings. Therefore, similar studies conducted in different geographies may produce different results.

The data collected in this research was extensive, including over 20 hours of interview transcriptions, which provided a rich basis for identifying key themes. As is typical in qualitative research, the interpretive nature of interviews and thematic analysis means the findings inevitably reflect the researcher's perspective. It is recognised that another researcher might have emphasised different themes, given the broad scope of the discussions. However, the Delphi study played a critical role in validating the recommendations, ensuring they were robust and reflective of expert consensus. While this research provides significant insights into organisational learning from incidents, further quantitative studies could complement these findings by evaluating the practical impact of the recommendations when implemented.

Although neo-institutional theory and organisational learning theory were used effectively in this study, these frameworks may not fully encapsulate the complexities of cyber security incident learning. Other analytical lenses—such as cultural theory[25] or cognitive psychology[26]—could have been employed, potentially leading to different insights. The literature review and theoretical choices were explicitly discussed throughout, ensuring transparency around the research decisions and their influence on the recommendations. Future research could explore additional theoretical perspectives to broaden our understanding of the factors influencing learning from incidents.

By restricting the scope of this thesis to organisational learning post-incident, it intentionally excludes the lessons learned by individuals and the informal, real-time learning that may occur during an incident as the organisation responds. These areas offer opportunities for future research and could provide further insights into the dynamics of learning within organisations.

[25] **Cultural Theory**: Examines how an organisation's shared values and norms influence behaviour, decision-making, and openness to incident reporting and learning.

[26] **Cognitive Psychology**: Studies mental processes such as perception and decision-making, offering insights into how individuals and teams process and retain information during and after incidents.

While these limitations provide avenues for further research, they do not detract from the significant contributions made by this thesis. Instead, they highlight the complexities of studying incident learning within organisations and emphasise the need for further exploration in this evolving field. By addressing these challenges head-on, this research has made meaningful contributions to both theory and practice, offering a solid foundation for future work.

8.4 Future research directions

The findings from this thesis open several avenues for future research that can build on and extend the insights generated by this work—see Appendix G for a list of potential future research questions.

8.4.1 Evaluation of learning practices

This research, grounded in neo-institutional theory, revealed that learning practices in organisations are often shaped by isomorphic pressures and conducted without evaluating their effectiveness. Practitioners highlighted the impact of time pressures on the practices they followed yet had not assessed the value of their learning efforts to determine whether they were investing too much or too little time. Many recognised the potential value of analysing trends from minor incidents or near misses but lacked data to justify such investments. Future research should explore whether the lessons implemented actually reduce the frequency and impact of incidents. Such studies could investigate how organisations can better evaluate their learning practices and balance the need for incident response with long-term learning. Additionally, future studies could adopt a design science approach (Hevner et al., 2004) to explore the practical challenges organisations face in determining how much effort should be invested in learning activities, how many people should participate, and whether learning efforts lead to a reduction in incidents. Observing post-incident reviews and gathering data from a wider set of stakeholders, including those outside the security team, would also provide valuable insights into organisational learning challenges.

8.4.2 Cross-sector comparisons

A deeper investigation into how different industries approach incident learning could offer valuable insights. High Reliability Organisations (HROs), such as those in aviation and healthcare, have long-established practices for learning from incidents (La Porte, 1996). Research into cyber security practices within HROs could help inform organisations on how to implement effective learning processes. The findings from this research suggest that more regulated industries, such as finance and energy, often have formal processes for tracking actions, but the study did not explicitly investigate sector-specific differences in depth. Expanding research across different industries, organisational sizes, and countries could illuminate broader patterns. Additionally, a longitudinal study could examine how learning practices evolve over time and whether advanced practices in some sectors spread to others.

8.4.3 Cultural and Governance Factors

This research found that a blame-free culture was crucial in encouraging incident reporting and effective investigations. organisational learning theory suggests that defensiveness can limit the identification of underlying causes. The study revealed concerns among participants about attributing causes to areas that might be difficult to address, as they did not want to be held accountable for fixing them. Future research could explore how organisational culture and governance structures influence incident learning. For example, investigating the impact of psychologically safe environments on reporting and post-incident review participation, and understanding what governance structures enable accountability for implementing lessons learned, would be valuable areas for further inquiry.

8.4.4 Tools and Techniques

This research found that organisations rarely used structured tools or methodologies for analysing incident causes, even though previous cyber security research has focused on techniques to identify causes. There is broad agreement that addressing underlying causes is important, as reflected in the prioritisation of "Delve into underlying causes and trends." Further research is needed to evaluate which tools are most effective in identifying lessons, particularly tools from the safety domain, such as those recommended by CREST (Creasey, 2013) or tools like AcciMap.[27] For example, Franco et al. (2019) applied the AcciMap tool to analyse a Denial of Service attack on a telecoms operator and found it enabled more lessons to be identified. Studies could also explore how techniques from other disciplines, such as sociology or safety science, could be adapted to cyber security to offer deeper insights into causes. Research could, for example, replicate studies like Vaughan's analysis of the Challenger shuttle disaster (Vaughan, 2016) to understand how risks and incidents are socially constructed within organisations.

8.4.5 The role of external pressures

This study highlighted the significant role of external pressures, such as regulatory frameworks, in shaping learning practices. More research is needed to explore how these pressures can be leveraged to encourage greater transparency and learning across industries, rather than fostering fear and reluctance to share lessons. Woods et al. (2023) explored the influence of cyber insurance and data breach attorneys on sharing practices, but more research is needed to fully understand the impact of litigation on incident learning. While some national security agencies and industry groups have created forums for peer sharing, the effectiveness of these forums in reducing incident prevalence remains underexplored. The increasing reliance on supplier ecosystems also demands further research into how organisations collaborate with suppliers on incident learning, including contractual obligations, participation in post-incident reviews, and the sharing of near-miss data.

To conclude, this thesis takes its title from a quote provided by one of the most experienced CISOs interviewed:

"I don't think we're there yet."

Despite the maturity of some organisations' incident learning practices, even the most advanced practitioners recognise that there is always room for improvement. As cyber threats evolve, so too must the practices used to mitigate them. This research provides recommendations for improving organisational learning practices and offers new insights into how organisations can learn more effectively from cyber security incidents. Ultimately, the continuous enhancement of learning practices is essential for building resilience in the face of an ever-changing threat landscape. This thesis contributes to this evolving field by offering a comprehensive roadmap for organisations aiming to improve their learning from incidents and enhance their overall security posture.

[27] The AcciMap tool was developed by Rasmussen for accident analysis for more details see (Waterson et al., 2017).

9 References

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, *71*(8), 939–953. https://doi.org/10.1002/asi.24311

Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams - Challenges in supporting the organisational security function. *Computers & Security*, *31*(5), 643–652. https://doi.org/10.1016/j.cose.2012.04.001

Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A case analysis of information systems and security incident responses. *International Journal of Information Management*, *35*(6), 717–723. https://doi.org/10.1016/j.ijinfomgt.2015.08.001

Akinrolabu, O. (2019). *Cyber Supply Chain Risks in Cloud Computing-The Effect of Transparency on the Risk Assessment of SaaS Applications* [Doctoral thesis]. University of Oxford.

Al Sabbagh, B., Kowalski, Stewart., Yngström, Louise., Ekstedt, Mathias., & Stockholms universitet Samhällsvetenskapliga fakulteten. (2019). *Cybersecurity Incident Response A Socio-Technical Approach.* [PhD dissertation, Stockholm University]. http://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-167873

Albakri, A., Boiten, E., & De Lemos, R. (2018, August 27). Risks of sharing cyber incident information. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3230833.3233284

Al-ma'aitah, M. A. (2022). Investigating the drivers of cybersecurity enhancement in public organizations: The case of Jordan. *Electronic Journal of Information Systems in Developing Countries*, *88*(5). https://doi.org/10.1002/isd2.12223

Alotaibi, M. J., Furnell, S., & Clarke, N. (2019). A framework for reporting and dealing with end-user security policy compliance. *Information and Computer Security*, *27*(1), 2-25. https://doi.org/10.1108/ics-12-2017-0097

Alvesson, M. (2003). Beyond Neopositivists, Romantics, and Localists: A Reflexive Approach to Interviews in Organisational Research. *Academy of Management Review*, *28*(1), 13–33.

Alvesson, M., & Spicer, A. (2019). Neo-Institutional Theory and Organization Studies: A Mid-Life Crisis? *Organization Studies*, *40*(2), 199–218. https://doi.org/10.1177/0170840618772610

Alvesson, Mats, Sveningsson, & Stefan. (2016). *Changing Organizational Culture* (2nd ed.). Routledge.

Amundrud, Ø., Aven, T., & Flage, R. (2017). How the definition of security risk can be made compatible with safety definitions. *J Risk and Reliability*, *231*(3), 286–294. https://doi.org/10.1177/1748006X17699145

Anderson, D. R., Sweeney, D. J., Williams, T. A., Camm, J. D., Cochran, J. J., & Shoesmith, E. (2020). *Statistics for Business and Economics* (5th ed.). Cengage Learning, EMEA.

Andrade, R., Torres, J., & Cadena, S. (2019). *Cognitive Security for Incident Management Process*.

Arce, D., Woods, D. W., & Böhme, R. (2024). Economics of incident response panels in cyber insurance. *Computers & Security*, *140*, 103742. https://doi.org/10.1016/j.cose.2024.103742 https://doi.org/https://doi.org/10.1016/j.cose.2024.103742

Argote, L. (2013). *Organizational Learning* (2nd ed.). Springer US. https://doi.org/10.1007/978-1-4614-5251-5

Argote, L., & Levine, J. M. (2017). The Oxford Handbook of Group and Organizational Learning. In *The Oxford Handbook of Group and Organizational Learning*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780190263362.001.0001

Argote, L., & Ophir, R. (2017). Intraorganizational Learning. In *The Blackwell Companion to Organizations* (pp. 181–207). Blackwell Publishing Ltd. https://doi.org/10.1002/9781405164061.ch8

Argyris. (1990). *Overcoming Organisational Defenses: Facilitating Organisational Learning*. Allyn and Bacon.

Argyris. (1999). *On Organizational Learning* (2nd ed.). Blackwell Publishing.

Argyris, C. (1976). Single-Loop and Double-Loop Models in Research on Decision Making. *Administrative Science Quarterly*, *21*(3), 363–375. https://doi.org/https://doi.org/10.2307/2391848

Argyris, C. (1994). Good Communication that Blocks Learning. *Harvard Business Review*, *72*(4), 77–85.

Argyris, C., & Schön, D. A. (1978). *Organizational Learning II: Theory, Method, and Practice*. Addison-Wesley Publishing Company.

Argyris, C., & Schon, D. A. (1996). *Organizational Learning II: Theory, Method, and Practice*. Addison-Wesley.

Arlington Research Commissioned by egress. (2020). *The 2020 Outbound Email Security Report*.

Ashraf, M., Jiang, J. (Xuefeng), & Wang, I. Y. (2022). Are there trade-offs with mandating timely disclosure of cybersecurity incidents? Evidence from state-level data breach disclosure laws. *Journal of Finance and Data Science*, *8*, 202–213. https://doi.org/10.1016/j.jfds.2022.08.001

Association of Information Systems. (2015). AIS Code of Research Conduct. In *AIS Administrative Bulletin: Vol. 2014.0224.01*.

Azadegan, A., Srinivasan, R., Blome, C., & Tajeddini, K. (2019). Learning from near-miss events: An organizational learning perspective on supply chain disruption response. *International Journal of Production Economics*, *216*, 215–226. https://doi.org/10.1016/j.ijpe.2019.04.021

Ballreich, F. L., Volkamer, M., Müllmann, D., Berens, B. M., Häußler, E. M., & Renaud, K. V. (2023). Encouraging Organisational Information Security Incident Reporting. *Proceedings of the 2023 European Symposium on Usable Security*, 224–236. https://doi.org/10.1145/3617072.3617098

Baram, M., & Schoebel, M. (2007). Safety culture and behavioral change at the workplace. *Safety Science*, *45*(6), 631–636. https://doi.org/10.1016/j.ssci.2007.04.001

Bartnes Line, M., Anne Tøndel, I., & Jaatun, M. G. (2016). Current practices and challenges in industrial control organizations regarding information security incident management – Does size matter? Information security incident management in large and small industrial control organizations. *International Journal of Critical Infrastructure Protection*, *12*, 12–26. https://doi.org/https://doi.org/10.1016/j.ijcip.2015.12.003

Bartnes, M., Moe, N. B., & Heegaard, P. E. (2016). The future of information security incident management training: A case study of electrical power companies. *Computers & Security*, *61*, 32–45. https://doi.org/10.1016/j.cose.2016.05.004

Barton, K. A., Tejay, G., Lane, M., & Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. *Computers and Security*, *59*, 9–25. https://doi.org/10.1016/j.cose.2016.02.007

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information and Management*, *51*(1), 138–151. https://doi.org/10.1016/j.im.2013.11.004

Baze, A. (2021). *Improving Incident Response Through Simplified Lessons Learned Data Capture*.

BBC. (2021, May 19). *Colonial Pipeline boss confirms $4.4m ransom payment*. https://www.bbc.com/news/business-57178503?

Beck, K., Beedle, M., van Bennekum, A., Cockburn, A., Cunningham, W., Fowler, M., Grenning, J., Highsmith, J., Hunt, A., Jeffries, R., Kern, J., Marick, B., Martin, R. C., Mellor, S., Schwaber, K., Sutherland, J., & Thomas, D. (2001). *Manifesto for Agile Software Development*. https://agilemanifesto.org/

Beiderbeck, D., Frevel, N., von der Gracht, H. A., Schmidt, S. L., & Schweitzer, V. M. (2021). Preparing, conducting, and analyzing Delphi surveys: Cross-disciplinary practices, new directions, and advancements. *MethodsX*, *8*, 101401. https://doi.org/10.1016/J.MEX.2021.101401

Bergen, N., & Labonté, R. (2020). "Everything Is Perfect, and We Have No Problems": Detecting and Limiting Social Desirability Bias in Qualitative Research. *Qualitative Health Research*, *30*(5), 783–792. https://doi.org/10.1177/1049732319889354

Bernsmed, K., & Tøndel, I. A. (2013). Forewarned is forearmed: Indicators for evaluating information security incident management. *Proceedings - 7th International Conference on IT Security Incident Management and IT Forensics, IMF 2013*, 3–14. https://doi.org/10.1109/IMF.2013.14

Bishop, P. G. . (2003). *Learning from incidents involving E/E/PE systems : part 2 : recommended scheme*. Health and Safety Executive.

Boakes, E. (2022). *Security Convergence: Building an evidence-based roadmap* [Doctoral thesis]. University of Portsmouth.

Boell, S., the, D. C.-K.-C. of, & 2014, undefined. (2014). A hermeneutic approach for conducting literature reviews and literature searches. *Aisel.Aisnet.Org*, *34*, 257–286. https://aisel.aisnet.org/cais/vol34/iss1/12/

Boin, A., & Hart, P. T. (2003). Public Leadership in Times of Crisis: Mission Impossible? *Public Administration Review*, *63*(5), 544–553. https://doi.org/10.1111/1540-6210.00318

Boin, A., McConnell, A., & Hart, P. T. (2008). *Governing after crisis: The politics of investigation, accountability and learning*. Cambridge University Press.

Brantly, A., & Smeets, M. (2020). Military Operations in Cyberspace. In *Handbook of Military Sciences* (pp. 1–16). Springer International Publishing. https://doi.org/10.1007/978-3-030-02866-4_19-1

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Braun, V., & Clarke, V. (2022). *Thematic Analysis: A Practical Guide* (A. Maher & E. Carter, Eds.; Kinle). SAGE Publications Asia-Pacific Pte Ltd.

Briggs, P., Jeske, D., & Coventry, L. (2017). The design of messages to improve cybersecurity incident reporting. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10292 LNCS*, 3–13. https://doi.org/10.1007/978-3-319-58460-7_1

Brinsfield, C. T. (2013). Employee silence motives: Investigation of dimensionality and development of measures. *Journal of Organizational Behavior*, *34*(5), 671–697. https://doi.org/10.1002/job.1829

Britton, M. (2024, March 7). *Key Takeaways from the 2023 FBI IC3 Report: Business Email Compromise Losses Jump to Nearly $3 Billion*. Abnormal Security. https://abnormalsecurity.com/blog/2023-fbi-ic3-report-takeaways

Brostoff, S., & Sasse, M. A. (2001). Safe and Sound: A Safety-Critical Approach to Security. *Proceedings of the 2001 Workshop on New Security Paradigms*.

Bulgurcu, B., & Mashatan, A. (2024). Environmental Factors that Hinder an Organization's Ability to Learn from Cyber Incidents: A Case Study on SolarWinds. *Proceedings of the 57th Hawaii International Conference on System Science*. https://hdl.handle.net/10125/107274

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). Purposive sampling: complex or simple? Research case examples. *Journal of Research in Nursing*, *8*, 652–661. https://doi.org/10.1177/1744987120927206

Cannon, M. D., & Edmondson, A. C. (2005). Failing to learn and learning to fail (intelligently): How great organizations put failure to work to innovate and improve. *Long Range Planning*, *38*(3 SPEC. ISS.), 299–319. https://doi.org/10.1016/j.lrp.2005.04.005

Cappelli, D., Moor, A., & Trzeciak, R. (2012). *The CERT guide to insider threats: How to Ppevent, detect, and respond to information technology crimes*. Addison-Wesley.

Catino, M. (2008). A Review of Literature: Individual Blame vs. Organizational Function Logics in Accident Analysis. *Journal of Contingencies and Crisis Management*, *16*(1).

Cavusoglu, H., Cavusoglu, H., Son, J. Y., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information and Management*, *52*(4), 385–400. https://doi.org/10.1016/j.im.2014.12.004

Chaudhary, S. (2024). Driving behaviour change with cybersecurity awareness. *Computers and Security*, *142*. https://doi.org/10.1016/j.cose.2024.103858

Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, *5*. https://doi.org/10.1016/j.chbr.2022.100167

Chyung, S. Y. Y., Roberts, K., Swanson, I., & Hankinson, A. (2017). Evidence-Based Survey Design: The Use of a Midpoint on the Likert Scale. *Performance Improvement*, *56*(10), 15–23. https://doi.org/10.1002/pfi.21727

Clare, J., & Kourousis, K. I. (2021). Learning from incidents: A qualitative study in the continuing airworthiness sector. *Aerospace*, *8*(2), 1–20. https://doi.org/10.3390/aerospace8020027

Clayton, M. J. (1997). Delphi: A technique to harness expert opinion for critical decision-making tasks in education. *Educational Psychology*, *17*(4), 373–386. https://doi.org/10.1080/0144341970170401

Cobb, S. (2015). *SIZING CYBERCRIME: INCIDENTS AND ACCIDENTS, HINTS AND ALLEGATIONS*.

Cockram, T. J., & Lautieri, S. R. (2007). *Combining security and safety principles in practice*.

Cohen, F. (1997). Information system attacks: A preliminary classification scheme. *Computers & Security*, *16*(1), 29–46. https://doi.org/10.1016/S0167-4048(97)85785-9

Conboy, K., Fitzgerald, G., & Mathiassen, L. (2012). Qualitative methods research in information systems: motivations, themes, and contributions. *European Journal of Information Systems 2012 21:2*, *21*(2), 113–118. https://doi.org/10.1057/EJIS.2011.57

Conklin, T. (2016). *Pre-Accident Investigations: Better questions - An Applied Approach to Operational Learning*. CRC Press.

Connolly, L. Y., & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *Computers & Security*, *87*. https://doi.org/10.1016/j.cose.2019.101568

Cook, R. I. (1998). *How Complex Systems Fail*. University of Chicago.

Cooke, D. L. (2003). Learning from Incidents. *21st System Dynamics Conference*, *22.3*, 1–30.

Cornejo, G. A. (2021). *Human Errors in Data Breaches: An Exploratory Configurational Analysis*. Nova Southeastern University.

Creasey, J. (2013). *Cyber Security Incident Response Guide Version 1*. https://www.crest-approved.org/wp-content/uploads/2022/04/CSIR-Procurement-Guide-1.pdf

Cresswell, J. (2008). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. SAGE Publications.

Creswell, J. D., & Creswell, D. J. (2023). *Research Design - Qualitative, Quantitative, and Mixed Methods Approaches* (sixth). Sage.

Creswell, J. W., & Creswell, J. D. (2023). *Research Design - Qualitative, Quantitative, and Mixed Methods Approaches* (6th ed.). SAGE Publications.

Creswell, J. W., & Miller, D. L. (2000). Determining Validity in Qualitative Inquiry. *Theory Into Practice*, *39*(3), 124-130. https://doi.org/10.1207/s15430421tip3903_2

Crossan, M. M., Lane, H. W., & White, R. E. (1999). An Organizational Learning Framework: From Intuition to Institution. *Academy of Management Review*, *24*(3), 522–537. https://doi.org/http://dx.doi.org/10.2307/259140

CrowdStrike. (2023). *2023 Global Threat Report*. https://www.crowdstrike.com/en-us/resources/reports/crowdstrike-2023-global-threat-report/

Curado, C. (2006). Organisational learning and organisational design. *Learning Organization*, *13*(1), 25–48. https://doi.org/10.1108/09696470610639112/FULL/HTML

Cybereason. (2022). *Ransomware - the true cost to business*. https://www.cybereason.com/ebook-ransomware-the-true-cost-to-business

Cybersecurity and Infrastructure Security Agency. (2023). *Securing the software supply chain for customers* (Version 1.0). U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/2023-01/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_CUSTOMER.PDF

Cyert, R. M., & March, J. G. (1963). *A behavioral theory of the firm.* (2nd ed.). Englewood Cliffs.

Da Silva, J. (2023). Protection, expertise and domination: Cyber masculinity in practice. *Computers and Security*, *133*. https://doi.org/10.1016/j.cose.2023.103408

de Loë, R. C., Melnychuk, N., Murray, D., & Plummer, R. (2016). Advancing the State of Policy Delphi Practice: A Systematic Review Evaluating Methodological Evolution, Innovation, and Opportunities. *Technological Forecasting and Social Change*, *104*, 78–88. https://doi.org/10.1016/j.techfore.2015.12.009

Dekker, S. (2012). Just culture: Balancing safety and accountability, 2nd edition. In *Just Culture: Balancing Safety and Accountability, 2nd Edition*.

Dekker, S. (2016). *Drift into failure: From hunting broken components to understanding complex systems*. CRC Press.

Dekker, S. (2019). *Foundations of safety science: A century of understanding accidents and disasters*. https://books.google.com/books?hl=en&lr=&id=dwWSDwAAQBAJ&oi=fnd&pg=PP1&dq=Dekker,+Sidney.+Foundations+of+safety+science:+A+century+of+understanding+accidents+and+disasters.+Routledge,+2019&ots=-Rfolu7zm4&sig=TYzvhg_H-TUhkTpwgcZl2lpzTro

Dekker, S., & Pruchnicki, S. (2014). Drifting into failure: theorising the dynamics of disaster incubation. *Theoretical Issues in Ergonomics Science*, *15*(6), 534–544. https://doi.org/10.1080/1463922X.2013.856495

Demjaha, A., Caulfield, T., Sasse, M. A., & Pym, D. (2019). 2 Fast 2 Secure: A Case Study of Post-Breach Security Changes. *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW),* 192–201. https://publications.parliament.uk/pa/cm201617/cmselect/cmcumeds/148/

Department for Science Innovation and Technology. (2024). *Cyber security skills in the UK labour market 2024*. https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2024/cyber-security-skills-in-the-uk-labour-market-2024

DiMaggio, P. J., & Powell, W. W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review*, *48*(April), 147–160. https://doi.org/http://dx.doi.org/10.2307/j.ctv1f886rp.7

DiNardi, G. (n.d.). *80+ of the Worst Hacked Celebrities From the Last Decade*. Retrieved July 5, 2023, from https://www.aura.com/learn/hacked-celebrities

Dobra-Kiel, A. (2023, November 12). *Unwrapping Psychological Safety In The Workplace - Behave web page*. https://behave.co.uk/unwrapping-psychlogical-safety-in-the-workplace/

Drupsteen, L. (2014). *Improving organisational safety through better learning from incidents and accidents ESReDA project group on Dynamic learning from accident investigation View project Social entrepreneurs-business models View project*. https://www.researchgate.net/publication/269098708

Drupsteen, L., Bos, E., Groeneweg, J., & Zwetsloot, G. I. J. M. (2013). Increasing the learning potential from events: Case studies. *Chemical Engineering Transactions*, *31*, 433–438. https://doi.org/10.3303/CET1331073

Drupsteen, L., Groeneweg, J., & Zwetsloot, G. I. J. M. (2013). Critical steps in learning from incidents: Using learning potential in the process from reporting an incident to accident prevention. *International Journal of Occupational Safety and Ergonomics*, *19*(1), 63–77. https://doi.org/10.1080/10803548.2013.11076966

Drupsteen, L., & Guldenmund, F. W. (2014). What Is Learning? A Review of the Safety Literature to Define Learning from Incidents, Accidents and Disasters. *Journal of Contingencies and Crisis Management*, *22*(2), 81–96. https://doi.org/10.1111/1468-5973.12039

Drupsteen, L., & Hasle, P. (2014). Why do organizations not learn from incidents? Bottlenecks, causes and conditions for a failure to effectively learn. *Accident Analysis and Prevention*, *72*, 351–358. https://doi.org/10.1016/j.aap.2014.07.027

Duchek, S., Raetze, S., & Scheuch, I. (2020). The role of diversity in organizational resilience: a theoretical framework. *Business Research*, *13*(2), 387–423. https://doi.org/10.1007/s40685-019-0084-8

Easterby-Smith, M., & Lyles, M. A. (2012). *Handbook of Organizational Learning and Knowledge Management* (2nd ed.). John Wiley & Sons Ltd. https://doi.org/10.1002/9781119207245

Ebert, N., Schaltegger, T., Ambuehl, B., Schöni, L., Zimmermann, V., & Knieps, M. (2023). Learning from safety science: A way forward for studying cybersecurity incidents in organizations. In *Computers and Security* (Vol. 134). Elsevier Ltd. https://doi.org/10.1016/j.cose.2023.103435

Edmondson, A. C. (2023). *Right Kind of Wrong: Why Learning to Fail can Teach us to Thrive* (Kindle Edition). Cornerstone.

Edmondson, A. C. (2002). The local and variegated nature of learning in organizations: A group-level perspective. *Organization Science*, *13*(2), 128–146. https://doi.org/10.1287/orsc.13.2.128.530

el perspective. *Organization Science*, *13*(2), 128–146. https://doi.org/10.1287/orsc.13.2.128.530

Edmondson, A. C. (2004). Learning from Mistakes is Easier Said than Done: Group and Organizational Influences on the Detection and Correction of Human Error. *The Journal of Applied Behavioral Science*, *40*(1), 66–90. https://doi.org/10.1177/0021886304263849

Edmondson, A. C. (2018). *The fearless organization: Creating psychological safety in the workplace for learning, innovation, and growth*. John Wiley & Sons.

El-Gazzar, R., Hustad, E., & Olsen, D. H. (2016). Understanding cloud computing adoption issues: A Delphi study approach. *Journal of Systems and Software*, *118*, 64–84. https://doi.org/10.1016/j.jss.2016.04.061

Elliott, D., & Macpherson, A. (2010). Policy and practice: Recursive learning from crisis. *Group and Organization Management*, *35*(5), 572–605. https://doi.org/10.1177/1059601110383406

Elliott, R., Fischer, C. T., & Rennie, D. L. (1999). Evolving guidelines for publication of qualitative research studies in psychology and related ®elds. *British Journal of Clinical Psychology*, *38*, 215–229.

ESReDA. (2015). *Guidelines for Preparing a Training Toolkit in Event Investigation and Dynamic Learning*. www.esreda.org

Evans, M. G., He, Y., Yevseyeva, I., & Janicke, H. (2019). Published incidents and their proportions of human error. *Information and Computer Security*, *27*(3), 343–357. https://doi.org/10.1108/ICS-12-2018-0147

Evans, M., He, Y., Maglaras, L., & Janicke, H. (2019). HEART-IS: A novel technique for evaluating human error-related information security incidents. *Computers & Security*, *80*, 74–89. https://doi.org/10.1016/j.cose.2018.09.002

Evenseth, L. L., Sydnes, M., & Gausdal, A. H. (2022). Building Organizational Resilience Through Organizational Learning: A Systematic Review. In *Frontiers in Communication* (Vol. 7). Frontiers Media S.A. https://doi.org/10.3389/fcomm.2022.837386

Fabiano, B., & Currò, F. (2012). From a survey on accidents in the downstream oil industry to the development of a detailed near-miss reporting system. *Process Safety and Environmental Protection*, *90*(5), 357–367. https://doi.org/10.1016/j.psep.2012.06.005

Farrell, P., & Scherer, K. (1983). The Delphi technique as a method for selecting criteria to evaluate nursing care. *Canadian Journal of Nursing Research Archive*, 51–60.

Fast, N. J., Burris, E. R., & Bartel, C. A. (2014). Managing to stay in the dark: Managerial self-efficacy, ego defensiveness, and the aversion to employee voice. *Academy of Management Journal*, *57*(4), 1013–1034. https://doi.org/10.5465/amj.2012.0393

Federal Bureau of Investigation Internet Crime Complaint Center. (2024). *Internet crime report 2023*. https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf

Fiol, C. M., & Lyles, M. A. (1985). Organizational Learning. *Source: The Academy of Management Review*, *10*(4), 803–813. https://www.jstor.org/stable/258048?seq=1&cid=pdf-

FireEye Mandiant Services. (2021). *M-TRENDS ®*. https://vision.fireeye.com/editions/11/11-m-trends.html#

Florêncio, D., Florêncio, F., & Herley, C. (2013). Sex, Lies and Cyber-crime Surveys. *Economics of Information Security and Privacy III. Springer, New York, NY,* 35–53. https://doi.org/10.1007/978-1-4614-1981-5_3

Franc, J. M., Hung, K. K. C., Pirisi, A., & Weinstein, E. S. (2023). Analysis of Delphi study 7-point linear scale data by parametric methods: Use of the mean and standard deviation. *Methodological Innovations*, *16*(2), 226–233. https://doi.org/10.1177/20597991231179393

Franco, Z., González, J. J., Canós, J. H., Wienen, H. C. A., Nl Faiza, H. C. A. W., Bukhsh, A., Vriezekolk, E., & Wieringa, R. J. (2019). Applying Generic AcciMap to a DDOS Attack on a Western-European Telecom Operator. *Proceedings of the 16th ISCRAM Conference*, 528–535.

Friday, D., Savage, D. A., Melnyk, S. A., Harrison, N., Ryan, S., & Wechtler, H. (2021). A collaborative approach to maintaining optimal inventory and mitigating stockout risks during a pandemic: capabilities for enabling health-care supply chain resilience. *Journal of Humanitarian Logistics and Supply Chain Management*, *11*(2), 248–271. https://doi.org/10.1108/JHLSCM-07-2020-0061

Fujs, D., Mihelič, A., & Vrhovec, S. L. (2019, August). The power of interpretation: Qualitative methods in cybersecurity research. In *Proceedings of the 14th International Conference on Availability, Reliability and Security* (pp. 1-10). https://doi.org/10.1145/3339252.3341479

Furnell, S. (2008). *Securing information and communications systems: Principles, technologies, and applications*. Artech House.

Gale, M., Bongiovanni, I., & Slapnicar, S. (2022). Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead. *Computers & Security*, *121*, 102840. https://doi.org/10.1016/j.cose.2022.102840

Gartner. (2023, September 28). *Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024*. https://doi.org/10.6188114.8

Garvin, D. A., Edmondson, A. C., & Gino, F. (2008). Is Yours a Learning Organization? *Harvard Business Review*. www.hbr.org

Gattuso, J. L. (2003, October 6). *Air Travel: A Hundred Years of Safety*. Mackinac Centre for Public Policy. https://www.mackinac.org/V2003-30

Gibbs, L., Kealy, M., Willis, K., Green, J., Welch, N., & Daly, J. (2007). What have sampling and data collection got to do with good qualitative research? *Australian and New Zealand Journal of Public Health*, *31*(6), 540–544. https://doi.org/10.1111/j.1753-6405.2007.00140.x

Gikas, C. (2010). A general comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards. *Information Security Journal*, *19*(3), 132–141. https://doi.org/10.1080/19393551003657019

Giulio, C. Di, Sprabery, R., Kamhoua, C., Kwiat, K., Campbell, R., & Bashir, M. N. (2017). IT Security and Privacy Standards in Comparison: Improving FedRAMP Authorization for Cloud Service Providers. *Proceedings - 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, CCGRID 2017*, 1090–1099. https://doi.org/10.1109/CCGRID.2017.137

Glesne, C. (2016). *Becoming Qualitative Researchers: An Introduction*. Pearson.

Gnoni, M. G., Tornese, F., Guglielmi, A., Pellicci, M., Campo, G., & De Merich, D. (2022). Near miss management systems in the industrial sector: A literature review. In *Safety Science* (Vol. 150). Elsevier B.V. https://doi.org/10.1016/j.ssci.2022.105704

Goffman, E. (2003). The Presentation of Self in Everyday Life. In *Social theory re-wired* (pp. 450–459). Routledge.

Goldkuhl, G. (2012). Pragmatism vs interpretivism in qualitative information systems research. *European Journal of Information Systems*, *21*(2), 135–146. https://doi.org/10.1057/EJIS.2011.54/TABLES/1

Gonzalez, J. J. (2005). Towards a Cyber Security Reporting System-A Quality Improvement Process. In *Lecture Notes in Computer Science* (Vol. 3688, pp. 368–380). https://doi.org/https://doi.org/10.1007/11563228_28

Goode, J., Levy, Y., Hovav, A., & Smith, J. (2018). Expert assessment of organizational cybersecurity programs and development of vignettes to measure cybersecurity countermeasures awareness. *Online Journal of Applied Knowledge Management* (Vol. 6, Issue 1). https://doi.org/10.36965/ojakm.2018.6(1)67-80

Grispos, G. (2016). *On The Enhancement of Data Quality in Security Incident Response Investigations* [Doctoral thesis]. University of Glasgow.

Grispos, G., Glisson, W. B., & Storer, T. (2014). Rethinking Security Incident Response: The Integration of Agile Principles. *20th Americas Conference on Information Systems*.

Grispos, G., Glisson, W. B., & Storer, T. (2015). Security Incident Response Criteria: A Practitioner's Perspective. *In 21st Americas Conference on Information Systems*. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1449&context=amcis2015

Grispos, G., Glisson, W. B., & Storer, T. (2017). Enhancing security incident response follow-up efforts with lightweight agile retrospectives. *Digital Investigation*, *22*, 62–73. https://doi.org/https://doi.org/10.1016/j.diin.2017.07.006

Grispos, G., Glisson, W. B., & Storer, T. (2019). *How Good is Your Data? Investigating the Quality of Data Generated During Security Incident Response Investigations*. https://doi.org/https://doi.org/10.24251/hicss.2019.859

Große, C., Nyman, M., & Sundberg, L. (2020). Information Technology Consulting Firms' Readiness for Managing Information Security Incidents. In *Communications in Computer and Information Science: Vol. 1221 CCIS* (pp. 48–73). Springer. https://doi.org/10.1007/978-3-030-49443-8_3

Gusenbauer, M., & Haddaway, N. R. (2020). Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of Google Scholar, PubMed, and 26 other resources. *Research Synthesis Methods*, *11*(2), 181–217. https://doi.org/10.1002/jrsm.1378

Hamdani, S. W. A., Abbas, H., Janjua, A. R., Shahid, W. Bin, Amjad, M. F., Malik, J., Murtaza, M. H., Atiquzzaman, M., & Khan, A. W. (2021). Cybersecurity Standards in the Context of Operating System. In *ACM Computing Surveys* (Vol. 54, Issue 3). Association for Computing Machinery. https://doi.org/10.1145/3442480

Hanafin, S. (2004). *Review of literature on the Delphi Technique*.

Hardy, D. J., O'Brien, A. P., Gaskin, C. J., O'Brien, A. J., Morrison-Ngatai, E., Skews, G. R., Ryan, T., & McNulty, N. B. (2004). Practical application of the Delphi technique in a bicultural mental health nursing study in New Zealand. *Journal of Advanced Nursing*, *46*(1), 95–109.

Harpe, S. E. (2015). How to analyze Likert and other rating scale data. *Currents in Pharmacy Teaching and Learning*, *7*(6), 836–850. https://doi.org/10.1016/j.cptl.2015.08.001

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*. https://doi.org/10.1016/j.jisa.2020.102726

Hausman, D. M. (1998). *Causal Asymmetries*. Cambridge University Press.

He, Y., & Johnson, C. (2015). Improving the redistribution of the security lessons in healthcare: An evaluation of the Generic Security Template. *International Journal of Medical Informatics*, *84*(11), 941–949. https://doi.org/https://doi.org/10.1016/j.ijmedinf.2015.08.010

He, Y., & Johnson, C. (2017). Challenges of information security incident learning: An industrial case study in a Chinese healthcare organization. *Informatics for Health and Social Care*, *42*(4), 393–408. https://doi.org/10.1080/17538157.2016.1255629

He, Y., Johnson, C., & Lu, Y. (2015). Improving the exchange of lessons learned in security incident reports: case studies in the privacy of electronic patient records. *Journal of Trust Management*, *2*(1). https://doi.org/10.1186/s40493-015-0016-2

He, Y., Johnson, C., Lu, Y., & Lin, Y. (2014). Improving the information security management: An industrial study in the privacy of electronic patient records. *Proceedings - IEEE Symposium on Computer-Based Medical Systems*, 525–526. https://doi.org/10.1109/CBMS.2014.121

He, Y., Johnson, C., Renaud, K., Lu, Y., & Jebriel, S. (2014). An empirical study on the use of the Generic Security Template for structuring the lessons from information security incidents. *2014 6th International Conference on Computer Science and Information Technology, CSIT 2014 - Proceedings*, 178–188. https://doi.org/10.1109/CSIT.2014.6805998

He, Y., Zamani, E. D., Lloyd, S., & Luo, C. (2022). Agile incident response (AIR): Improving the incident response process in healthcare. *International Journal of Information Management*, *62*. https://doi.org/10.1016/j.ijinfomgt.2021.102435

Heinrich, H. W. (1928). The Origin of Accidents - The Apparent Cause Is Not Always the Basic Cause. *The National Safety Council*, *18*.

Hekneby, T., & Olsen, T. H. (2024). The role of leadership in organizational learning in multinational companies. *Learning Organization*, *31*(2), 141–162. https://doi.org/10.1108/TLO-09-2022-0101

Help Net Security. (2024, May 24). *Worried about job security, cyber teams hide security incidents*. https://www.helpnetsecurity.com/2024/05/24/cyber-teams-major-challenges/

Heraghty, D., Dekker, S., & Rae, A. (2018). Accident report interpretation. *Safety*, *4*(4). https://doi.org/10.3390/safety4040046

Herrmann, D., & Pridöhl, H. (2020). Basic concepts and models of cybersecurity. In *The ethics of cybersecurity* (pp. 11–44). https://doi.org/https://doi.org/10.1007/978-3-030-29053-5

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105.

Hewitt, T. A., & Chreim, S. (2015). Fix and forget or fix and report: A qualitative study of tensions at the front line of incident reporting. *BMJ Quality and Safety*, *24*(5), 303–310. https://doi.org/10.1136/bmjqs-2014-003279

Hielscher, J., Menges, U., Parkin, S., Delft, T. U., Kluge, A., & Sasse, M. A. (2023). "Employees Who Don't Accept the Time Security Takes Are Not Aware Enough": The CISO View of Human-Centred Security. *32st USENIX Security Symposium*. https://www.forbes.com/sites/bobzukis/2022/04/18/the-sec-

Ho, H., Ko, R., & Mazerolle, L. (2022). Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review. *Computers & Security*, *115*. https://doi.org/10.1016/j.cose.2022.102611

Hollnagel, E., Woods, D. D., & Leveson, N. (2006). *Resilience engineering: Concepts and precepts* (D. D. Woods & N. Leveson, Eds.). Ashgate Publishing, Ltd.

Horne, C. A., Maynard, S. B., & Ahmad, A. (2020, December 12). *Towards Governance of Information Security Incident Response*. https://aisnet.org/general/custom.asp?page=SeniorScholarBasket

Howard, J. D., & Longstaff, T. A. (1998). *SANDIA REPORT A Common Language for Computer , Security Incidents Energy under Contract DE-ACj4-94AL85000. .s*.

Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security - a neo-institutional perspective. *Journal of Strategic Information Systems*, *16*(2), 153–172. https://doi.org/10.1016/j.jsis.2007.05.004

Huber, G. P. (1991). Organizational Learning: The Contributing Processes and the Literatures. *Organization Science*, *2*(1), 88–115. https://www.jstor.org/stable/2634941

Humayun, M., Niazi, M., Jhanjhi, · Nz, Alshayeb, · Mohammad, & Mahmood, · Sajjad. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arabian Journal for Science and Engineering*, *45*(3), 3171–3189. https://doi.org/10.1007/s13369-019-04319-2

Humphrey-Murto, S., Varpio, L., Gonsalves, C., & Wood, T. J. (2017). Using consensus group methods such as Delphi and Nominal Group in medical education research*. *Medical Teacher*, *39*(1), 14–19. https://doi.org/10.1080/0142159X.2017.1245856

Husák, M., Sokol, P., Žádník, M., Bartoš, V., & Horák, M. (2023). Lessons Learned from Automated Sharing of Intrusion Detection Alerts: The Case of the SABU Platform. *Digital Threats: Research and Practice*. https://doi.org/10.1145/3611391

Ibrishimova, M. D. (2018). Cyber incident classification: issues and challenges. *Lecture International Conference on P2P, Parallel, Grid, Cloud and Internet Computing. Springer, Cham* , *24*. *https://doi.org/10.1007/978-3-030-02607-3_43*

Information Systems Audit and Control Association (ISACA). (2020). *Security Incident Management Audit Program*. https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KoDPEA0

International Organization for Standardization. (2023). *ISO/IEC 27035-2:2023: Information security, cybersecurity and privacy protection — Information security incident management — Part 2: Guidelines to plan and prepare for incident response*. https://www.iso.org/standard/75843.html

IT Governance. (2024, January 5). *List of Data Breaches and Cyber Attacks in 2023 – 8,214,886,660 records breached*. Blog. https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023?utm_source

ITIL 4 continual improvement model & VUCA | Axelos. (n.d.). Retrieved February 1, 2022, from https://www.axelos.com/resource-hub/white-paper/itil4-continual-improvement-model-vuca-environment-white-paper

Jaatun, M. G., Albrechtsen, E., Line, M. B., Johnsen, S., Waerø, I., Longva, O., & Tøndel, I. (2008). *A Study of Information Security Practice in a Critical Infrastructure Application*. Springer.

Jaatun, M. G., Albrechtsen, E., Line, M. B., Tøndel, I. A., & Longva, O. H. (2009). A framework for incident response management in the petroleum industry. *International Journal of Critical Infrastructure Protection*, *2*(1–2), 26–37. https://doi.org/10.1016/j.ijcip.2009.02.004

Jaatun, M. G., Bartnes, M., & Tøndel, I. A. (2016). Zebras and Lions: Better incident handling through improved cooperation. *Communications in Computer and Information Science*, *648*, 129–139. https://doi.org/10.1007/978-3-319-49466-1_9

Jaatun, M. G., Johnsen, S. O., Bartnes, M., Longva, O. H., Tøndel, I. A., Albrechtsen, E., & Wærø, I. (2007). *Incident Response Management in the oil and gas industry*.

Jaatun, M. G., & Tøndel, I. A. (2015). How much cloud can you handle? *Proceedings - 10th International Conference on Availability, Reliability and Security, ARES 2015*, 467–473. https://doi.org/10.1109/ARES.2015.38

Jacobsson, A., Ek, Å., & Akselsson, R. (2012). Learning from incidents - A method for assessing the effectiveness of the learning cycle. *Journal of Loss Prevention in the Process Industries*, *25*(3), 561–570. https://doi.org/10.1016/j.jlp.2011.12.013

Jeyaraj, A., & Zadeh, A. (2020). Institutional Isomorphism in Organizational Cybersecurity: A Text Analytics Approach. *Journal of Organizational Computing and Electronic Commerce*, *30*(4), 361–380. https://doi.org/10.1080/10919392.2020.1776033

Johnson, C. W. (2002). Reasons for the Failure of Incident Reporting in the Healthcare and Rail Industries. *Proceedings of the Tenth Safety-Critical Systems Symposium, Southampton, UK 2002*, 31–57. http://130.209.240.1/~johnson/papers/incident_problems.pdf

Johnson, C. W. (2003). *Failure in Safety-Critical Systems: A Handbook of Accident and Incident Reporting*. University of Glasgow Press.

Jore, S. H. (2019). The Conceptual and Scientific Demarcation of Security in Contrast to Safety. *European Journal for Security Research*, *4*(1), 157–174. https://doi.org/10.1007/S41125-017-0021-9

Kaspersky. (2017). *Banks Spend on IT Security is 3x Higher Than Non-Financial Organizations*. Corporate News. https://www.kaspersky.com/about/press-releases/2017_banks-spends

Kaur, M., van Eeten, M., Janssen, M., Borgolte, K., & Fiebig, T. (2021). *Human Factors in Security Research: Lessons Learned from 2008-2018*. http://arxiv.org/abs/2103.13287

Kävrestad, J., Birath, M., & Clarke, N. L. (2024). *Fundamentals of digital forensics: A guide to theory, research, and practice* (3rd ed.). Springer. https://doi.org/https://doi.org/10.1007/978-3-031-53649-6

Keeney, S., Hasson, F., & McKenna, H. (2006). Consulting the oracle: Ten lessons from using the Delphi technique in nursing research. *Journal of Advanced Nursing*, *53*(2), 205–212. https://doi.org/10.1111/j.1365-2648.2006.03716.x

Kelly, L. M., & Cordeiro, M. (2020). Three principles of pragmatism for research on organizational processes. *Methodological Innovations*, *13*(2). https://doi.org/10.1177/2059799120937242

Khan, N. F., Yaqoob, A., Khan, M. S., & Ikram, N. (2022). The cybersecurity behavioral research: A tertiary study. *Computers & Security*, *120*, 102826. https://doi.org/10.1016/j.cose.2022.102826

Khan, S., Kabanov, I., Hua, Y., & Madnick, S. (2022). A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned. *ACM Transactions on Privacy and Security*, *26*(1). https://doi.org/10.1145/3546068

Kirlappos, I., Parkin, S., & Sasse, M. A. (2014). *Learning from "Shadow Security": Why understanding non-compliant behaviors provides the basis for effective security*. https://doi.org/10.14722/usec.2014.23<007

Kitchenham, B., Brereton, P., Li, Z., Budgen, D., & Burn, A. (2010). *Repeatability of systematic literature reviews*. https://doi.org/https://doi.org/10.1049/ic.2011.0006

Klein, G. A. (2009). *Streetlights and shadows: Searching for the keys to adaptive decision making* (Kindle). Mit Press.

Knight, R., & Nurse, J. R. C. (2020). A framework for effective corporate communication after cyber security incidents. *Computers and Security*, *99*. https://doi.org/10.1016/j.cose.2020.102036

Knowles, C. (2024, October 4). *Cybercrime to cost $12 trillion by 2025, says Forrester*. https://securitybrief.co.nz/story/cybercrime-to-cost-12-trillion-by-2025-says-forrester

Kosseff, J. (2023). Upgrading Cybersecurity Law. *Hous. L. Rev*, *61*, 51. https://www.law.com/americanlawyer/2022/08/16/afirms-tec

Kral, P. (2012). *SANS Incident handler's handbook 2012*. https://www.sans.org/white-papers/33901/

Krausmann, E., & Necci, A. (2021). Thinking the unthinkable: A perspective on Natech risks and Black Swans. *Safety Science*, *139*. https://doi.org/10.1016/j.ssci.2021.105255

Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., & Halgand, Y. (2015). A survey of approaches combining safety and security for industrial control systems. In *Reliability Engineering and System Safety* (Vol. 139, pp. 156–178). Elsevier Ltd. https://doi.org/10.1016/j.ress.2015.02.008

Kumar, G., Banerjee, R. N., Meena, P. L., & Ganguly, K. (2016). Collaborative culture and relationship strength roles in collaborative relationships: a supply chain perspective. *Journal of Business and Industrial Marketing*, *31*(5), 587–599. https://doi.org/10.1108/JBIM-12-2014-0254

Kumar, R., & Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. In *Computer Science Review* (Vol. 33, pp. 1–48). Elsevier Ireland Ltd. https://doi.org/10.1016/j.cosrev.2019.05.002

Kuypers, M. A., Maillart, T., & Paté-Cornell, E. (2016). An Empirical Analysis of Cyber Security Incidents at a Large Organization. *Department of Management Science and Engineering, Stanford University, School of Information, UC Berkeley 30* .

Kvale, S. (1996). *InterViews: An introduction to qualitative research interviewing* (A. Virding, Ed.). SAGE Publications, Inc.

La Porte, T. (1996). High Reliability Organizations- Unlikely, Demanding and At Risk. *Journal of Contingencies and Crisis Management*, *4*(2), 60–71.

La Porte, T. R. (1996). High reliability organizations: Unlikely, demanding and at risk. *Journal of Contingencies and Crisis Management*, *4*(2), 60–71. https://doi.org/10.1111/J.1468-5973.1996.TB00078.X

Lakshmi, R., Naseer, H., Maynard, S., & Ahmad, A. (2021). Sensemaking in cybersecurity incident response- The interplay of organizations, technology and individuals. *ECIS 2021 Research-in-Progress Papers. 29*. https://aisel.aisnet.org/ecis2021_rip/29

Larouzee, J., & Le Coze, J. C. (2020). Good and bad reasons: The Swiss cheese model and its critics. In *Safety Science* (Vol. 126). Elsevier B.V. https://doi.org/10.1016/j.ssci.2020.104660

Le Coze, J. C. (2013). What have we learned about learning from accidents? Post-disasters reflections. *Elsevier*. https://doi.org/https://doi.org/10.1016/j.ssci.2012.07.007

Leroy, H., Dierynck, B., Anseel, F., Simons, T., Halbesleben, J. R. B., McCaughey, D., Savage, G. T., & Sels, L. (2012). Behavioral Integrity for Safety, Priority of Safety, Psychological Safety, and Patient Safety: A Team-Level Study. *Journal of Applied Psychology*, *97*(6), 1273. https://doi.org/10.1037/a0030076

Leveson, N. (2004). A new accident model for engineering safer systems. *Safety Science*, *42*(4), 237–270.

Leveson, N., Fleming, C., … M. S.-S. I., & 2012, undefined. (2012). Safety assessment of complex, software-intensive systems. *SAE International Journal of Aerospace*, *5.2012-01–2134*, 233–244. https://search.proquest.com/openview/0edd331a1b280b68e4383450bb727bcf/1?pq-origsite=gscholar&cbl=5013117

Leveson, N. G. (2011). Applying systems thinking to analyze and learn from events. *Safety Science*, *49*(1), 55–64. https://doi.org/10.1016/j.ssci.2009.12.021

Libicki, M. C. (2021). Cyberspace in peace and war. In E*uropean Journal on Criminal Policy and Research* (2nd ed., Issue 3). Naval Institute Press.

Likert. (1932). A Technique for the Measurement of Attitudes. *Archives of Psychology*, *22*, 5–55.

Lin, Y., Chen, A., Zhong, S., Giannikas, V., Lomas, C., & Worth, T. (2023). Service supply chain resilience: a social-ecological perspective on last-mile delivery operations. *International Journal of Operations and Production Management*, *43*(1), 140–165. https://doi.org/10.1108/IJOPM-03-2022-0180

Lindberg, A. K., Hansson, S. O., & Rollenhagen, C. (2010). Learning from accidents - What more do we need to know? *Safety Science*, *48*(6), 714–721. https://doi.org/10.1016/j.ssci.2010.02.004

Line, M. B. (2013). A case study: Preparing for the smart grids - Identifying current practice for information security incident management in the power industry. In *Proceedings - 7th International Conference on IT Security Incident Management and IT Forensics, IMF 2013* (pp. 26–32). https://doi.org/10.1109/IMF.2013.15

Line, M. B. (2015). *Understanding security management practices: A case study in the electric power industry* [Doctoral thesis]. Norwegian University of Science and Technology.

Line, M. B., & Albrechtsen, E. (2016). Examining the suitability of industrial safety management approaches for information security incident management. *Information and Computer Security*, *24*(1), 20–37. https://doi.org/10.1108/ICS-01-2015-0003

Line, M. B., Albrechtsen, E., Johnsen, S. O., Longva, O. H., & Hillen, S. (2006). Monitoring of Incident Response Management Performance. *International Conference on IT-Incident Management & IT-Forensics*. https://dblp.org/db/conf/imf/imf2006.html

Line, M. B., Tøndel, I. A., & Jaatun, M. G. (2016). Current practices and challenges in industrial control organizations regarding information security incident management - Does size matter? Information security incident management in large and small industrial control organizations. *International Journal of Critical Infrastructure Protection*, *12*, 12–26. https://doi.org/10.1016/j.ijcip.2015.12.003

Line, M. B., Zand, A., Stringhini, G., & Kemmerer, R. (2014). *Targeted Attacks against Industrial Control Systems: Is the Power Industry Prepared?* https://doi.org/10.1145/2667190.2667192

Linstone, H. A., Turoff, M., & Helmer, O. (1975). *The Delphi Method Techniques and Applications Edited by*. Addison-Wesley.

Lisova, E., Šljivo, I., & Čaušević, A. (2019). Safety and Security Co-Analyses: A Systematic Literature Review. In *IEEE Systems Journal* (Vol. 13, Issue 3, pp. 2189–2200). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/JSYST.2018.2881017

Littlejohn, A., Margaryan, A., & Lukic, D. (2010). How organisations learn from safety incidents: A multifaceted problem. *Journal of Workplace Learning*, *22*(7), 428–450. https://doi.org/10.1108/13665621011071109/FULL/HTML

Littlejohn, A., Margaryan, A., Vojt, G., & Lukic, D. (2017). Learning from Incidents Questionnaire (LFIQ): The validation of an instrument designed to measure the quality of learning from incidents in organisations. *Safety Science*, *99*, 80–93. https://doi.org/10.1016/J.SSCI.2017.02.005

Lukic, D., Littlejohn, A., & Margaryan, A. (2012). A framework for learning from incidents in the workplace. *Safety Science*, *50*(4), 950–957. https://doi.org/10.1016/j.ssci.2011.12.032

Lukic, D., Margaryan, A., & Littlejohn, A. (2010). How organisations learn from safety incidents: A multifaceted problem. *Journal of Workplace Learning*, *22*(7), 428–450. https://doi.org/10.1108/13665621011071109

Lund, C. (2014). Of What is This a Case?: Analytical Movements in Qualitative Social Science Research. *Human Organization*, *73*(3), 224-234. https://doi.org/10.17730/humo.73.3.e35q482014x033l4

Lundberg, J., Rollenhagen, C., & Hollnagel, E. (2009). What-You-Look-For-Is-What-You-Find - The consequences of underlying accident models in eight accident investigation manuals. *Safety Science*, *47*(10), 1297–1311. https://doi.org/10.1016/j.ssci.2009.01.004

Lundberg, J., Rollenhagen, C., & Hollnagel, E. (2010). What you find is not always what you fix—How other aspects than causes of accidents decide recommendations for remedial actions. *Accident Analysis & Prevention*, *42*(6), 2132–2139. https://doi.org/10.1016/J.AAP.2010.07.003

Mandiant. (2022). *M-Trends 2022 - Mandiant special report*. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.mandiant.com/sites/default/files/2022-04/M-Trends%25202022%2520Executive%2520Summary.pdf&ved=2ahUKEwim2ZON0deLAxXWaEEAHWIvMi0QFnoECA0QAQ&usg=AOvVaw2iAuciInxIaSNrnKxnXlwT

Manfield, R. C., & Newey, L. R. (2018). Resilience as an entrepreneurial capability: integrating insights from a cross-disciplinary comparison. *International Journal of Entrepreneurial Behaviour and Research*, *24*(7), 1155–1180. https://doi.org/10.1108/IJEBR-11-2016-0368

Margaryan, A., Littlejohn, A., & Lukic, D. (2018). *The development and evaluation of a Learning from Incidents toolkit*. http://www.tandfonline.com/

Margaryan, A., Littlejohn, A., & Stanton, N. A. (2017). Research and development agenda for Learning from Incidents. *Safety Science*, *99*, 5–13. https://doi.org/10.1016/J.SSCI.2016.09.004

McIntosh, T., Liu, T., Susnjak, T., Alavizadeh, H., Ng, A., Nowrozy, R., & Watters, P. (2023). Harnessing GPT-4 for generation of cybersecurity GRC policies: A focus on ransomware attack mitigation. *Computers & Security*, *134*, 103424. https://doi.org/10.1016/j.cose.2023.103424

McKenna, H. P. (1994). The Delphi technique: a worthwhile research approach for nursing? *Journal of Advanced Nursing*, *19*, 1221–1225.

Mehrizi, M. H.R., Nicolini, D., & Modol, J.R. (2022). How Do Organizations Learn from Information System Incidents? A Synthesis of the Past, Present, and Future. *MIS Quarterly*, *46*(1), 531–590. https://doi.org/10.25300/MISQ/2022/14305

Meyer, J. W., & Rowan, B. (1977). Institutionalized Organizations: Formal Structure as Myth and Ceremony. In *American Journal of Sociology* (Vol. 83, Issue 2). https://about.jstor.org/terms

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *BMJ (Online)*, *339*(7716), 332–336. https://doi.org/10.1136/BMJ.B2535

Moore, T., Dynes, S., & Chang, F. R. (2016). Identifying How Firms Manage Cybersecurity Investment. *Workshop on the Economics of Information Security (WEIS)*, 1–27. Dallas, TX, USA: Darwin Deason Institute for Cyber Security, Southern Methodist University.

Morrison, E. W., & Milliken, F. J. (2000). Organizational Silence: A Barrier to Change and Development in in a Pluralistic World. *The Academy of Management Review*, *25*(4), 706–725. http://about.jstor.org/terms

Mott, G., Turner, S., Nurse, J. R. C., MacColl, J., Sullivan, J., Cartwright, A., & Cartwright, E. (2023). Between a rock and a hard(ening) place: Cyber insurance in the ransomware era. *Computers and Security*, *128*. https://doi.org/10.1016/j.cose.2023.103162

Mukhopadhyay, A., & Jain, S. (2024). A framework for cyber-risk insurance against ransomware: A mixed-method approach. *International Journal of Information Management*, *74*. https://doi.org/10.1016/j.ijinfomgt.2023.102724

Murphy, V. L., Littlejohn, A., & Rienties, B. (2021). Learning from incidents: applying the 3-P model of workplace learning. *Journal of Workplace Learning*. https://doi.org/10.1108/JWL-04-2021-0050

Murphy, V. L., Littlejohn, A., Rienties, B., King, S., & Bryden, R. (2018). Where does information on incidents come from? *Society of Petroleum Engineers - SPE International Conference and*

Exhibition on Health, Safety, Security, Environment, and Social Responsibility 2018. https://doi.org/10.2118/190526-ms

National Cyber Security Centre (NCSC). (n.d.). *Categorising UK cyber incidents*. https://www.ncsc.gov.uk/information/categorising-uk-cyber-incidents

National Cyber Security Centre (NCSC). (2019). *NCSC CAF guidance - D.2 Lessons learned*. Version 3.0. https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/d-2-lessons-learned

National Cyber Security Centre (NCSC). (2021, May 11). *10 Steps to Cyber Security - Incident Management*. https://www.ncsc.gov.uk/collection/10-steps/incident-management

National Cyber Security Centre (NCSC). (2022). *Cyber Security Longitudinal Survey Wave 1*. https://www.gov.uk/government/publications/cyber-security-longitudinal-survey-wave-one/cyber-security-longitudinal-survey-wave-1

National Cyber Security Centre. (2024). *NCSC Annual Review 2024*. https://www.ncsc.gov.uk/collection/ncsc-annual-review-2024

National Institute of Standards and Technology (NIST) Computer Security Resource Center CSRC. (n.d.). *NIST Glossary*. Glossary. Retrieved February 25, 2022, from https://csrc.nist.gov/glossary/term/incident

National Institute of Standards and Technology (NIST). (2006). Guide to integrating forensic techniques into incident response (NIST Special Publication 800-86). In *U.S. Department of Commerce.* https://doi.org/https://doi.org/10.6028/NIST.SP.800-86

National Institute of Standards and Technology. (2012). *Computer security incident handling guide* (NIST Special Publication No. 800-61 Revision 2). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-61r2

Neto, N. N., Moraes De Paula, A. G., & Malara Borges, N. (2021). *Developing a Global Data Breach Database and the Challenges Encountered*. https://doi.org/10.1145/3439873

Nicolini, Davide. (2012). *Practice Theory, Work, and Organization: an Introduction*. Oxford University Press.

Niekerk, J. Van, & von Solms, R. (2004). Organisational learning models for information security. *The ISSA 2004 Enabling Tomorrow Conference*, *30*. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.106.4619&rep=rep1&type=pdf

Novak, J., Mcintire, D., Hueca, A., Manley, B., Mudd, S., & Bills, T. (2021). *The Sector CSIRT Framework: Developing Sector-Based Incident Response Capabilities CERT Division*. https://doi.org/10.1184/R

Nurse, J. R. C. (2019). Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit. In *The Oxford Handbook of Cyberpsychology* (pp. 662–690). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198812746.013.35

O'Connor, C., & Joffe, H. (2020). Intercoder Reliability in Qualitative Research: Debates and Practical Guidelines. *International Journal of Qualitative Methods*, *19*. https://doi.org/10.1177/1609406919899220

Onwuegbuzie, A. J., & Leech, N. L. (2003, November 5). On Becoming a Pragmatic Researcher: The Importance of Combining Quantitative and Qualitative Research Methodologies. *Mid-South Educational Research Association, Biloxi, MS*.

O'Reilly, M., & Parker, N. (2013). "Unsatisfactory Saturation": A critical exploration of the notion of saturated sample sizes in qualitative research. *Qualitative Research*, *13*(2), 190–197. https://doi.org/10.1177/1468794112446106

Papastergiou, S., Mouratidis, H., & Kalogeraki, E.-M. (2019). Cyber Security Incident Handling, Warning and Response System for the European Critical Information Infrastructures (CyberSANE). *International Conference on Engineering Applications of Neural Networks. Springer, Cham, 2019*.

Paulus, T. M., & Lester, J. N. (2021). *Doing qualitative research in a digital world*.

Perrow, C. (1984). *Normal accidents: living with high-risk technologies*. Princeton University Press. https://doi.org/10.1515/9781400828494

Petrie, D. A., & Swanson, R. C. (2018). The mental demands of leadership in complex adaptive systems. *Healthcare Management Forum*, *31*(5), 206–213. https://doi.org/10.1177/0840470418778051

Piazza, A., & Abrahamson, E. (2020). Fads and Fashions in Management Practices: Taking Stock and Looking Forward. *International Journal of Management Reviews*, *22*(3), 264–286. https://doi.org/10.1111/ijmr.12225

Pietre-Cambacedes, L., & Bouissou, M. (2013). Cross-fertilization between safety and security engineering. In *Reliability Engineering and System Safety* (Vol. 110, pp. 110–126). Elsevier Ltd. https://doi.org/10.1016/j.ress.2012.09.011

Pilgrim, D. (2014). Some implications of critical realism for mental health research. *Social Theory and Health*, *12*(1), 1–21. https://doi.org/10.1057/sth.2013.17

Pollock, T. (2017). *Reducing human error in cyber security using the Human Factors Analysis Classification System (HFACS).* (Issue 2). https://digitalcommons.kennesaw.edu/ccerphttps://digitalcommons.kennesaw.edu/ccerp/2017/research/2

Pols, P. (2017). *Designing a unified kill chain for analyzing, comparing, and defending against cyber attacks* [Masters thesis, Cyber Security Academy]. Leiden University Student Repository. https://studenttheses.universiteitleiden.nl/handle/1887/64569

PwC. (2021). *Conti cyber attack on the HSE Independent Post Incident Review-Executive Summary and Learnings for Other Organisations*. https://www.lenus.ie/handle/10147/631006

PWC. (2023, January 16). *PwC's 26th Annual Global CEO Survey*. The Leadership Agenda. https://www.pwc.com/gx/en/issues/c-suite-insights/ceo-survey-2023.html

Rae, A., & Provan, D. (2019). Safety work versus the safety of work. *Safety Science*, *111*, 119–127. https://doi.org/10.1016/j.ssci.2018.07.001

Rahman, N. H. A., & Choo, K. K. R. (2015). A survey of information security incident handling in the cloud. *Computers and Security*, *49*, 45–69. https://doi.org/10.1016/j.cose.2014.11.006

Ralph, B. (2024, July 24). *"If you have knowledge, let others light their candles in it." Why sharing lessons learned from cyber security incidents and 'near misses' will help everyone to improve*. https://www.ncsc.gov.uk/blog-post/let-others-light-candles

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science*, *27*(2/3), 183–213.

Rasmussen, J. (1998). Constructivism and phenomenology what do they have in common, and how can they be told apart? *Cybernetics and Systems*, *29*(6), 553–576.

Reed, J. P. (2020). Beyond the "fix-it" treadmill. *Communications of the ACM*, *63*(5), 58–63. https://doi.org/10.1145/3380322

Renaud, K. (2012). Blaming noncompliance is too convenient: What really causes information breaches? *IEEE Security and Privacy*, *10*(3), 57–63. https://doi.org/10.1109/MSP.2011.157

Renaud, K., & Goucher, W. (2012). Health service employees and information security policies: an uneasy partnership? *Information Management & Computer Security*, *20*(4), 296–311.

Rollenhagen, C., Westerlund, J., Lundberg, J., & Hollnagel, E. (2010). The context and habits of accident investigation practices: A study of 108 Swedish investigators. *Safety Science*, *48*(7), 859–867. https://doi.org/10.1016/J.SSCI.2010.04.001

Russell Vastveit, K., Boin, A., & Njå, O. (2015). Learning from incidents: Practices at a Scandinavian refinery. *Safety Science*, *79*, 80–87. https://doi.org/10.1016/j.ssci.2015.05.001

Russell Vastveit, K., & Njå, O. (2014). The roles of incident investigations in learning processes at a Scandinavian refinery. *Journal of Loss Prevention in the Process Industries*, *32*, 335–342. https://doi.org/10.1016/J.JLP.2014.09.015

Ryan, J. J. C. H., & Jefferson, T. I. (2003, May). The use, misuse, and abuse of statistics in information security research. *Proceedings of the 2003 ASEM National Conference*.

Ryciuk, U., & Nazarko, J. (2020). Model of trust-based cooperative relationships in a supply chain. *Journal of Business Economics and Management*, *21*(5), 1225–1247. https://doi.org/10.3846/jbem.2020.12829

Rządca, R., & Strumińska-Kutra, M. (2016). Local governance and learning: in search of a conceptual framework. *Local Government Studies*, *42*(6), 916–937. https://doi.org/10.1080/03003930.2016.1223632

Saarelainen, K., & Jäntti, M. (2015). Quality and Human Errors in IT Service Infrastructures - Human error based on root causes of incidents and their categorization. *11th International. Conference on Innovations in Information Technology (IIT)*. https://doi.org/https://doi.org/10.1109/innovations.2015.7381541

Salane, D. E., & Jay, J. (2011). Are Large Scale Data Breaches Inevitable? Center for Cybercrime Studies. *Cyber Infrastructure Protection*, *9*, 51–80.

Salmon, P. M., Cornelissen, M., & Trotter, M. J. (2012). Systems-based accident analysis methods: A comparison of Accimap, HFACS, and STAMP. *Safety Science*, *50*(4), 1158–1170. https://doi.org/10.1016/j.ssci.2011.11.009

Salviotti, G., Abbatemarco, N., De Rossi, L., & D'ignazio, C. (2024). Understanding the Role of Leadership Competencies in Cyber Crisis Management: A Case Study. *Proceedings of the 57th Hawaii International Conference on System Sciences*. https://hdl.handle.net/10125/106892

Sanne, J. M. (2008). Incident reporting or storytelling? Competing schemes in a safety-critical and hazardous work setting. *Safety Science*, *46*(8), 1205–1222. https://doi.org/10.1016/J.SSCI.2007.06.024

SANS Institute. (2021). *Incident handler's handbook* (6th ed.). https://www.sans.org/white-papers/incident-handlers-handbook/

Sarker, S., Xiao, X., Beaulieu, T., & Lee, A. S. (2018). Learning from first-generation qualitative approaches in the is discipline: An evolutionary view and some implications for authors and evaluators (part 1/2). *Journal of the Association for Information Systems*, *19*(8), 752–774. https://doi.org/10.17705/1jais.00508

Schein, E. H. (2017). *Organizational Culture and Leadership* (P. Schein, Ed.; 5th ed.). John Wiley & Sons inc.

Schilling, J., & Kluge, A. (2009). Barriers to organizational learning: An integration of theory and research. *International Journal of Management Reviews*, *11*(3), 337–360. https://doi.org/10.1111/J.1468-2370.2008.00242.X

Schneier, B. (1999). Attack Trees - Schneider, 1999. *Dr. Dobb's Journal*, *24*(12), 21–29.

Schneier, B. (2000). *Secrets and lies: Digital security in a networked world* (1st ed.). Wiley.

Security Magazine. (2023, April 11). *Over 40% of cybersecurity teams told to keep breaches confidential*. https://www.securitymagazine.com/articles/99192-over-40-of-cybersecurity-teams-told-to-keep-breaches-confidential

Senge, P., Kleiner, A., Roberts, C., Ross, R., Roth, G., Smith, B., & Gunman, E. C. (1999). *The dance of change: The challenges to sustaining momentum in learning organizations*.

Senge, P. M. (2010). *The Fifth Discipline: The art and practice of the learning organization (Century business)* (2nd, Kindle Edition ed.). Random House Business Books.

Shaikh, F. A., & Siponen, M. (2023). Organizational Learning from Cybersecurity Performance: Effects on Cybersecurity Investment Decisions. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-023-10404-7

Shappell, S., & Wiegmann, D. A. (2000). *The Human Factors Analysis and Classification System-HFACS*. https://www.researchgate.net/publication/247897525

Shaty, O. (2021). *Lessons learned from Lessons learned from analyzing 100 data analyzing 100 data breaches breaches*. https://www.imperva.com/resources/whitepapers/Lessons-learned-from-analyzing-100-data-breaches-Report-210603-v4.pdf

Shedden, P., Ahmad, A., & Ruighaver, A. B. (2010). Organisational Learning and Incident Response: Promoting Effective Learning Through The Incident Response Process. *Proceedings of the 8th*

Australian Information Security Management Conference . https://doi.org/10.4225/75/57b6771734788

Shedden, P., Ahmad, A., Ruighaver, A. B., Shedden, P. ;, & Ahmad, A. ; (2011). *Informal Learning in Security Incident Response Teams*. 1–1. http://aisel.aisnet.org/acis2011/37

Sillito, J., & Pope, M. (2024). Learning From Lessons Learned: Preliminary Findings From a Study of Learning From Failure. *Proceedings of the 2024 IEEE/ACM 17th International Conference on Cooperative and Human Aspects of Software Engineering*, 97–102. https://doi.org/10.1145/3641822.3641867

Silverman, D. (2017). How was it for you? The Interview Society and the irresistible rise of the (poorly analyzed) interview. *Qualitative Research*, *17*(2), 144–158. https://doi.org/10.1177/1468794116668231

Spiegelhalter, D. (2019). *The art of statistics: Learning from data*. Penguin UK.

Spranger, J., Homberg, A., Sonnberger, M., & Niederberger, M. (2022). Reporting guidelines for Delphi techniques in health sciences: A methodological review. *Zeitschrift Fur Evidenz, Fortbildung Und Qualitat Im Gesundheitswesen*, *172*, 1–11. https://doi.org/10.1016/j.zefq.2022.04.025

Stahl, J. V, Taylor, N. E., & Hill, C. E. (2012). Philosophical and historical background of consensual qualitative research. In *Consensual Qualitative Research: A Practical Resource for Investigating Social Science Phenomena*.

Statista. (2024, January). *Distribution of cyber incidents in organizations worldwide as of September 2023, by type*. Cyber Crime & Security. https://www.statista.com/statistics/1483769/global-cyber-incidents-by-type/

Staykova, M. P. (2019). Rediscovering the Delphi Technique: A Review of the Literature. *Advances in Social Sciences Research Journal*, *6*(1). https://doi.org/10.14738/assrj.61.5959

Stone, J. (2020, May 28). *Judge rules Capital One must hand over Mandiant's forensic data breach report*. https://cyberscoop.com/capital-one-breach-mandiant-report-judge-ruling/

Street, C., & Ward, K. W. (2019). Cognitive Bias in the Peer Review Process: Understanding a Source of Friction between Reviewers and Researchers. *The DATA BASE for Advances in Information System*, *50*(4).

Svedung, I., & Rasmussen, J. (2002). Graphic representation of accident scenarios: Mapping system structure and the causation of accidents. *Safety Science*, *40*(5), 397–417. https://doi.org/10.1016/S0925-7535(00)00036-9

Sveen, F. O., Rich, E., & Jager, M. (2007). Overcoming organizational challenges to secure knowledge management. *Information Systems Frontiers*, *9*(5), 481–492. https://doi.org/10.1007/s10796-007-9052-5

Sveen, F. O., Sarriegi, J. M., Rich, E., & Gonzalez, J. J. (2007). Toward viable information security reporting systems. *Information Management and Computer Security*, *15*(5), 408–419. https://doi.org/10.1108/09685220710831143

Swuste, P., van Gulijk, C., Groeneweg, J., Zwaard, W., Lemkowitz, S., & Guldenmund, F. (2020). From clapham junction to macondo, deepwater horizon: Risk and safety management in high-tech-high-hazard sectors: A review of English and Dutch literature: 1988–2010. In *Safety Science* (Vol. 121, pp. 249–282). Elsevier B.V. https://doi.org/10.1016/j.ssci.2019.08.031

Tamuz, M., Franchois, K. E., & Thomas, E. J. (2011). What's past is prologue: Organizational learning from a serious patient injury. *Safety Science*, *49*(1), 75–82. https://doi.org/10.1016/J.SSCI.2010.06.005

Tan, T., Ruighaver, T., & Ahmad, A. (2003, November 25). Incident Handling: Where the need for planning is often not recognised. *1st Australian Computer, Network & Information Forensics Conference 2003*.

Tatu, T., Ament, C., & Jaeger, L. (2018). Lessons Learned from an Information Security Incident: A Practical Recommendation to Involve Employees in Information Security. *Proceedings of the 51stHawaii International Conference on System Sciences*. https://doi.org/https://doi.org/10.24251/hicss.2018.471

Tavris, C., & Aronson, E. (2020). *Mistakes Were Made (but Not by Me): Why We Justify Foolish Beliefs, Bad Decisions and Hurtful Acts* (3rd Edition). Pinter & Martin Ltd.

Tejay, G. P. S., & Mohammed, Z. A. (2023). Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective. *Information and Management*, *60*(3). https://doi.org/10.1016/j.im.2022.103751

Terry, G., Hayfield, N., Clarke, V., & Braun, V. (2017). Thematic Analysis. In *The SAGE handbook of qualitative research in psychology* (Vol. 2, pp. 17–37). SAGE Publications Inc.

Tetrick, L., Zaccaro, S., Dalal, S. J., Repchick, J. A., Hargrove, K. M., Winslow, A. K., Chen, C. J., Fletcher, T. C., Schrader, Z., Gorab, S. W., Niu, A. K., & Wang, Q. &. (2016). *Improving Social Maturity of Cybersecurity Incident Response Teams*. http://calctraining2015.weebly.com/the-handbook.html

The Assurance Case Working Group, (ACWG). (2021). *Goal Structuring Notation Community Standard Version 3 The Assurance Case Working Group (ACWG)* (SCSC-141C). https://scsc.uk/scsc-141C

Thiebes, S., Scheidt, D., Schmidt-Kraepelin, M., & Benlian, A. (2018). Paving the Way for Real-Time Delphi in Information Systems Research: A Synthesis of Survey Instrument Designs and Feedback Mechanisms. *Research Papers*, *89*. https://aisel.aisnet.org/ecis2018_rp/89

Tøndel, I. A., Line, M. B., & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. *Computers & Security*, *45*, 42–57. https://doi.org/10.1016/J.COSE.2014.05.003

Torraco, R. J. (2016). Writing Integrative Literature Reviews: Using the Past and Present to Explore the Future. In *Human Resource Development Review* (Vol. 15, Issue 4, pp. 404–428). SAGE Publications Ltd. https://doi.org/10.1177/1534484316671606

Tripathi, C. R. (2022). *The Role of Imitation in Technological Learning and Catch-up: Evidence from the Indian Automobile Industry* [PhD dissertation, The University of Manchester]. https://research.manchester.ac.uk/files/248798443/FULL_TEXT.PDF

Trussler, S. (2020). *A Construction Industries View on Accountability in a No-Blame Culture* [Lund University]. http://www.risk.lth.se

Tytler, J., & Copson, L. (2024, February 9). *Incident response in 2023 – a view from the data*. S-RM Article. https://www.s-rminform.com/latest-thinking/incident-response-in-2023-a-view-from-the-data?utm_source

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*. https://doi.org/https://doi.org/10.1016/j.cose.2021.102387

UK Government. (2024). *Cyber security longitudinal survey-wave three*. https://www.gov.uk/government/publications/cyber-security-longitudinal-survey-wave-three-results/cyber-security-longitudinal-survey-wave-three

UK Government Official Statistics. (2023). *Cyber security breaches survey 2023*. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023

7 (2002). *Sarbanes–Oxley Act of 2002*, Pub. L. No. 107-204, 116 Stat. 745. https://www.govinfo.gov/content/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf

U.S. Department of Justice. (2019, March 20). *Lithuanian Man Pleads Guilty To Wire Fraud For Theft Of Over $100 Million In Fraudulent Business Email Compromise Scheme*. https://www.justice.gov/usao-sdny/pr/lithuanian-man-pleads-guilty-wire-fraud-theft-over-100-million-fraudulent-business

Vakola, M., & Bouradas, D. (2005). Antecedents and consequences of organisational silence: An empirical investigation. *Employee Relations*, *27*(5), 441–458. https://doi.org/10.1108/01425450510611997

Van Court Hare. (1967). *System Analysis: A Diagnostic Approach*. Harcourt.

Van der Kleij, R., Kleinhuis, G., & Young, H. (2017). Computer security incident response team effectiveness: A needs assessment. *Frontiers in Psychology*, *8*(DEC). https://doi.org/10.3389/fpsyg.2017.02179

van der Wagen, W. (2018). The Cyborgian Deviant- An Assessment of the Hacker through Actor-Network Theory - vanderWagen, 2018. *Journal of Qualitative Criminal Justice and Criminology*, *6*(2), 157–178.

Van Gogh, M., Beato, F., & Rohland, L. (2024, June 20). *Why transport and supply chain ecosystems need to be cyber secured*. https://www.weforum.org/stories/2024/06/transport-supply-chain-ecosystems-cyber-resilience/

Vastveit, K. R., Boin, A., & Njå, O. (2015). Learning from incidents: Practices at a Scandinavian refinery. *Safety Science*, *79*, 80–87. https://doi.org/10.1016/J.SSCI.2015.05.001

Vaughan, D. (2005). Organizational rituals of risk and error. In *Organizational encounters with risk* (pp. 33–66).

Vaughan, D. (2016). *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA* (Enlarged Edition). The University of Chicago Press, Ltd.

Venkatesh, V., Brown, S. A., & Sullivan, Y. W. (2016). Guidelines for conducting mixed-methods research: An extension and illustration. *Journal of the Association for Information Systems*, *17*(7), 435–495. https://doi.org/10.17705/1jais.00433

Vicente, K. J., & Rasmussen, J. (1990). The Ecology of Human-Machine Systems II: Mediating "Direct Perception" in Complex Work Domains. *Ecological Psychology*, *2*(3), 207–249. https://doi.org/10.1207/s15326969eco0203_2

Vuko, T., Slapničar, S., & Čular, M. (2021). *Key drivers of cybersecurity audit effectiveness: the neo-institutional perspective*. https://ssrn.com/abstract=3932177

Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. *Computers and Security*, *87*. https://doi.org/10.1016/j.cose.2019.101589

Waterson, P., Jenkins, D. P., Salmon, P. M., & Underwood, P. (2017). 'Remixing Rasmussen': The evolution of Accimaps within systemic accident analysis. *Applied Ergonomics*, *59*, 483–503. https://doi.org/10.1016/j.apergo.2016.09.004

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. In *Source: MIS Quarterly* (Vol. 26, Issue 2).

Weick, K. E. (1995). *Sensemaking in organizations* (Vol. 3). Sage Publications.

Westphal Marc-David L Seidel, J. D., Stewart, K. J., Dacin, T., Davis, G., Greve, A., Greve, H., Haunschild, P., Hay-ward, M., Henderson, A., Huber, G., Shah, N., & Zajac, E. (1997). Second-order Imitation: Uncovering Latent Effects of Board Network Ties We appreciate the helpful comments and suggestions of Gautam Ahuja. In *Administrative Science Quarterly* (Vol. 717).

Wienen, H. C. A., Bukhsh, F. A., Vriezekolk, E., & Wieringa, R. J. (2017). *Accident Analysis Methods and Models-a Systematic Literature Review*. (Technical Report No. TR-CTIT-17-04). Centre for Telematics and Information Technology, University of Twente. https://research.utwente.nl/en/publications/accident-analysis-methods-and-models-a-systematic-literature-revi

Willig, C. (2022). *Introducing qualitative research in psychology: adventures in theory and method* (4e ed.). Open University Press. https://www.mheducation.co.uk/professionals/open-university-press/olc/willig-qualitative-research

Woods, D. D. (2018). The theory of graceful extensibility: basic rules that govern adaptive systems. *Environment Systems and Decisions*, *38*(4), 433–457. https://doi.org/10.1007/s10669-018-9708-3

Woods, D. W., Wolff, J., Böhme, R., & Schwarcz, D. (2023). Lessons Lost: Incident Response in the Age of Cyber Insurance and Breach Attorneys. *Open Access to the Proceedings of the 32nd USENIX Security Symposium Is Sponsored by USENIX.*, 2259–2273. https://www.usenix.org/conference/usenixsecurity23/presentation/woods

World Economic Forum. (2022). *The Global Risks Report 2022 17th Edition* (17th ed.). https://www.weforum.org/reports/global-risks-report-2022

World Economic Forum. (2023). *Chief Risk Officers Outlook*. https://www.weforum.org/publications/chief-risk-officers-outlook-july-2023/#:~:text=A%20survey%20of%20the%20World,over%20the%20next%20six%20months.

World Economic Forum. (2024, January 10). *2023 was a big year for cybercrime – here's how we can make our systems safer*. Forum Institutional. https://www.weforum.org/stories/2024/01/cybersecurity-cybercrime-system-safety/

World Economic Forum (in collaboration with Accenture). (2023). *Global Cybersecurity Outlook 2023*. https://www.weforum.org/publications/global-cybersecurity-outlook-2023/

Wrigstad, J., Bergström, J., & Gustafson, P. (2017). One event, three investigations: The reproduction of a safety norm. *Safety Science*, *96*, 75–83. https://doi.org/10.1016/j.ssci.2017.03.009

Yin, R. (2018). *Case study research and applications: design and methods* (6th ed.). SAGE Publications, Inc.

Zhang, H., Babar, M. A., & Tell, P. (2011). Identifying relevant studies in software engineering. *Information and Software Technology*, *53*(6), 625–637. https://doi.org/10.1016/j.infsof.2010.12.010

Zibak, A., & Simpson, A. (2019, August 26). Cyber threat information sharing: Perceived benefits and barriers. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3339252.3340528

Zietsma, C., Ziet, C., & Branzei, O. (2002). The War of the Woods: Facilitators and Impediments of Organizational Learning Processes. *British Journal of Management*, *13*(S2), S61–S74. https://doi.org/https://doi.org/10.1111/1467-8551.13.s2.6

Zwetsloot, G. I. J. M., Kines, P., Ruotsala, R., Drupsteen, L., Merivirta, M. L., & Bezemer, R. A. (2017). The importance of commitment, communication, culture and learning for the implementation of the Zero Accident Vision in 27 companies in Europe. *Safety Science*, *96*, 22–32. https://doi.org/10.1016/j.ssci.2017.03.001

10 Appendices

Appendix A – Literature search queries

Table A1 lists the search engine queries for the literature search. All databases were queried most recently in December 2024.

Table A1 *Sources and search queries*

Source	Search query
The ACM Guide to Computing Literature https://dl.acm.org/	AllField:("security incident" OR "security incidents" OR "incident response" OR "CSIRT") AND AllField:("organisational learning" OR "organizational learning" OR "lessons learned" OR "lessons learnt")
IEEE Xplore https://ieeexplore.ieee.org/	("security incident" OR "security incidents" OR "incident response" OR "CSIRT") AND ("organisational learning" OR "organizational learning" OR "lessons learned" OR "lessons learnt")
ScienceDirect https://www.sciencedirect.com/	("security incident" OR "security incidents" OR "incident response" OR "CSIRT") AND ("organisational learning" OR "organizational learning" OR "lessons learned" OR "lessons learnt")
SpringerLink https://link.springer.com/	("security incident" OR "security incidents" OR "incident response" OR "CSIRT") AND ("organisational learning" OR "organizational learning" OR "lessons learned" OR "lessons learnt")
ProQuest One Literature https://www.proquest.com/literature	("security incident" OR "security incidents" OR "incident response" OR "CSIRT") AND ("organisational learning" OR "organizational learning" OR "lessons learned" OR "lessons learnt")
Scopus https://www.scopus.com/	("security incident" OR "security incidents" OR "incident response" OR "CSIRT") AND ("organisational learning" OR "organizational learning" OR "lessons learned" OR "lessons learnt")
Wiley Online Library https://onlinelibrary.wiley.com/	("security incident" OR "security incidents" OR "incident response" OR "CSIRT") AND ("organisational learning" OR "organizational learning" OR "lessons learned" OR "lessons learnt")
Web of Science Core Collection https://www.webofscience.com/	("security incident" OR "security incidents" OR "incident response" OR "CSIRT") AND ("organisational learning" OR "organizational learning" OR "lessons learned" OR "lessons learnt")

Appendix B - Exploratory poll

Table B1 lists the companies of the registered attendees who were invited to participate in the poll. The responses were anonymous so from those listed it is not known who participated in which questions. There was an average response rate of 38%, 25 people across the five questions asked in the poll:

1. What type of learning happens in your organisation following a cyber security incident?
2. When investigating the causes of incidents we consider (tick all that apply)?
3. Who in your organisation do you share lessons with (select one option)?
4. How are lessons acted upon (tick all that usually apply)?
5. Which would help your organisation to learn more from incidents (tick all that apply)?

Table B1 *The registered attendees for the session in which the exploratory poll was conducted*

Industry sector	**Example participating companies**	**Example roles**
Finance and insurance	Allianz, AXA, Banco Santander, Deutsche Bank, ING Group, Mastercard, NatWest Group, ITAU BBA Europe, Standard Bank Group	CISO, Deputy CISO, Director of Cyber Protect, EVP Cyber Security Products, Chief Security Architect
Industrial, energy, transport and logistics	Anglo American, Babcock International, DP World, Epiroc, MOL Group, Galp Energia, Fiege Logistik, Menzies Distribution, Motor Oil Hellas, SIG plc, Zehnder Group	CISO, Head of IT, Global CTO, Group Director IT Security
Government, public bodies and non-for-profits	BSI Group, FINOS	Head of Security Operations, Director of Community
Services, retail, tourism and entertainment	Carrefour, Tesco, The Estée Lauder Companies, The Very Group, IHG, Compass Group, News UK, Skyscanner, Sony, Metropolitan Gaming	CISO, Head of Information Security, Director of Group Resilience

Appendix C - Interview participants

Table C1 *The interview participants' organisation size and industry, their job role and years of experience in security*

#	Industry	Size	Role	Years of experience in security
P1	Industrial, energy, transport and logistics	Huge	CISO	30
P2	Finance and insurance	Large	Other	25
P3	Industrial, energy, transport and logistics	Large	Other	10
P4	Government, public bodies and non-for-profits	Huge	CISO	14
P5	Finance and insurance	Huge	Other	4
P6	Finance and insurance	Huge	Other	16
P7	Finance and insurance	Large	Other	15
P8	Industrial, energy, transport and logistics	Huge	Other	24
P9	Government, public bodies and non-for-profits	Large	Other	10
P10	Services, retail, tourism and entertainment	Huge	CISO	25
P11	Finance and insurance	Huge	Other	18
P12	Industrial, energy, transport and logistics	Huge	CISO	15
P13	Industrial, energy, transport and logistics	Medium	Other	19
P14	Services, retail, tourism and entertainment	Medium	CISO	25
P15	Finance and insurance	Huge	Other	12
P16	Finance and insurance	Huge	Other	15
P17	Services, retail, tourism and entertainment	Huge	Other	4
P18	Industrial, energy, transport and logistics	Huge	CISO	10
P19	Industrial, energy, transport and logistics	Large	CISO	10
P20	Services, retail, tourism and entertainment	Medium	CISO	3
P21	Services, retail, tourism and entertainment	Large	CISO	8
P22	Services, retail, tourism and entertainment	Large	Other	13
P23	Finance and insurance	Large	Other	10
P24	Finance and insurance	Large	CISO	25
P25	Industrial, energy, transport and logistics	Large	CISO	18
P26	Industrial, energy, transport and logistics	Medium	CIO	4
P27	Industrial, energy, transport and logistics	Medium	CIO	10
P28	Industrial, energy, transport and logistics	Large	CISO	25
P29	Industrial, energy, transport and logistics	Medium	CISO	18
P30	Government, public bodies and non-for-profits	Medium	CIO	10
P31	Services, retail, tourism and entertainment	Large	CISO	11
P32	Finance and insurance	Medium	CISO	25
P33	Finance and insurance	Large	CISO	25
P34	Industrial, energy, transport and logistics	Large	CISO	13

Notes:

The organisations were categorised into four main groups: 1) Finance and insurance, 2) Government, public bodies and non-for-profits, 3) Industrial, energy, transport and logistics, and 4) Services, retail, tourism and entertainment. These categories were used as the financial industry is heavily regulated, with mature cyber security functions which are well resourced (Kaspersky, 2017)*, government and public bodies often have less available funds, and services and retail often have digital products and personal consumer data. Industrial, energy, transport and logistics often have a lot of IOT systems as well as corporate IT (medical would also fit in this category but no such organisations were interviewed in this study).*

Organisations were categorised by size into Medium for those with 250 to 999 employees, Large for 1,000 to 50,000 and Huge for those with over 50,000.

The "other" category included roles such as three CIOs, four Heads of Incident Response, two Information Security Managers and other roles such as Cyber Advice & Strategy or Head of Enterprise Application Security etc. all participants were asked about their knowledge and experience of how their organisation learns from incidents at the start of the interview to confirm they were able to contribute to the study. 21 participants identified as male and 13 identified as female.

Appendix D - Practitioner interview protocol

Table D1 *The practitioner interview protocol questions and prompts*

INTERVIEW PROTOCOL		
STUDY: **ORGANISATIONAL LEARNING FROM CYBER SECURITY INCIDENTS**		
Date:	*Time:*	*Location:*
Interview type (virtual / F2F):		
Researcher:		
Interviewee:		
Name (pseudonym):	*Organisation (pseudonym):*	*Role:*
Introduction:	☐ ☐ ☐ ☐ ☐ ☐	1. The researcher introduces themself. 2. Explains the interview process and it will last for approximately an hour. 3. Examples are encouraged but do not say the name of people or organisations 4. Confirms Participant Information Sheet has been provided. 5. Explains interview will be recorded. 6. Questions?
INTERVIEW		
Type of question	**Questions**	**Prompts**
Background	**Tell me about your role and experience of incidents**	• Number of employees in your organisation? • Your organisation's industry or industries? • Your current role? • Length of service at your organisation? • The approximate number of years working in the field of security? • The approximate number of incidents your organisation typically experiences in a year? • Involvement in incident management?

Type of question	Questions	Prompts
Current practices reporting	**What are your organisation's incident reporting practices?**	• How do people report security incidents? • How is the importance of reporting highlighted in the organisation? • How do you think your security culture impacts reporting? • How do you think psychological safety/blame culture impacts reporting? • Who decides which events are classified as incidents? • Who decides whether you would or would not report to different organisations (Police, NCSC, regulators etc.)? • Who would handle the response to a major incident (internal team, managed service provider, specialist IR firm – and particularly in the latter, whether there is any differentiation between members of the NCSC CIR scheme vs other companies)?
Current practices for investigate	**How does your organisation investigate incidents?**	• What is your opinion on efforts to investigate the cause of an incident? • Does your organisation use any incident causation models or templates from the safety discipline to investigate incidents? • Is the same approach applied to all incidents? • What about several incidents with the same theme? • Who decides on the approach to use? • Is this approach always effective? • What situations have you experienced where incident causes can be numerous and complex? • How deep does your investigation go into underlying causes? • What types of causes do you consider (technology design, physical conditions, operating procedures, policies, organisation structure, governance, staffing, training, suppliers, industry factors, laws and regulations, political and social factors)? • Typically who participates in the investigation? • What outputs does the investigation generate? • Who defines and who needs to agree on any lessons learned? • Who are these outputs shared with (internally and externally)?
Current practice intervention	**How does your organisation plan interventions based on what is learned from incidents?**	• Who defines and who needs to agree with actions based on learning from incidents? • Who decides the prioritisation? • How are resources secured to complete the interventions? • Who is the action plan shared with?

Type of question	Questions	Prompts
Current practice intervention	**How are these interventions actioned?**	• How is progress against the actions tracked and reported? • Who is accountable for ensuring they are completed? • What types of actions have happened in your organisation based on incidents experienced (e.g. CSIRT improvements, policies updated, risk assessments changed, training material changed etc)? linked to the incident?
Current practice learning and challenges	**How does your organisation evaluate its learning from incidents (learning to learn)?**	• How do you evaluate if the actions have been effective? • What obstacles to learning from incidents have you experienced in your position? • How well do you believe your organisation learns from incidents? • In your opinion, what conditions or developments could improve learning from incidents/occurrences in your organisation?

Appendix E - Interview codebook and themes

Table E1 *The themes and the associated codes from the practitioner interviews*

Themes	Codes
ISOMORPHIC PRESSURES	***Coercive***
	Complexity of global jurisdictions
	Fear of litigation and the regulator
	Reporting to the regulator, police or security agencies
	Suppliers contracted to report incidents
	Threat intelligence notifications of incidents affecting supply chain
	Use of insurance
	How orgs are evaluating if the lessons are effective
	Mimetic
	Learning from others in the industry
	Sharing the lessons outside the org
	Use of third parties
	Normative
	Allocation of resources to implement lessons
	Causal analysis practices
	Classifying incidents practices
	Cyber incident processes as other IT incidents
	Encouraging reporting
	Example lessons implemented
	Incident reporting practices
	Learning feeds into risk management
	Learning from low level incidents
	Learning from simulation exercises
	Learning to improve incident response
	Linking to strategic transformation plans
	Output of post-incident review
	Repeat incidents
	Reporting the trends of incidents
	Seeing causes as control failures
	Sharing the lessons intra-org
	Technology tools need to support learning
	Tracking actions practices
	Who assigns owners & approves actions
	Who decides this is the cause
	Who participates in identifying the lessons
CHALLENGES OF UNCOVERING INCIDENTS	Challenges of reaching non-wired workers
	Chronic unease
	Consequence management is needed sometimes
	Culture
	Litigation & regulation impact on learning
	Psychological safety & blame
	Security linked to safety culture
	Suppliers may not share all incidents
	Using real people to bring campaigns to life
	Challenges of reporting from OT environments

Themes	Codes
CHALLENGE OF IDENTIFYING THE CAUSES	Defensiveness & politics
	Desire to return to normal and put the incident behind you
	Difficulty of finding time
	People participating in investigating the cause
	Regulators can encourage deeper investigations
	Understanding the true causes
CHALLENGES OF IMPLEMENTING LESSONS	Accountability & governance is important
	Business ownership
	Challenge of securing the fringes
	Constant need to improve security
	Dependency on third parties
	Drift back into failure
	Global jurisdictions
	Justifying spend on cyber and quantifying the risk
	Leadership's understanding of cyber risks
	Management balancing competing priorities
	Maturity of the organisation
	Need agility as things are constantly changing
	Need to build a resilient organisation
	Not tracking implementing lessons
	Organisational barriers
	Pervasiveness of technology expanding the attack surface
	Reporting line of the CISO or security function
	Secure by Design
	Structural changes are hard to implement

Appendix F - Delphi survey participants

A table F listing the participants' organisation size and industry, their job role and years of experience in security (their answers were anonymous).

Table F1 *Delphi survey participants round 1*

Industry sector	Size	Role		Years of experience in cyber security
Industrial, energy, transport and logistics	Less than 1,000	CIO or Head of IT		10
Industrial, energy, transport and logistics	1,000 to 50,000	CISO or Head of Security		10
Services, retail, tourism and entertainment	1,000 to 50,000	CISO or Head of Security		17
Industrial, energy, transport and logistics	Less than 1,000	CIO or Head of IT		20
Industrial, energy, transport and logistics	1,000 to 50,000	CISO or Head of Security		25
Government, public bodies and non-for-profits	1,000 to 50,000	CISO or Head of Security		18
Services, retail, tourism and entertainment	1,000 to 50,000	CISO or Head of Security		10
Finance and insurance	1,000 to 50,000	CISO or Head of Security		23
Finance and insurance	1,000 to 50,000	CISO or Head of Security		17
Government, public bodies and non-for-profits	1,000 to 50,000	CISO or Head of Security		15
Services, retail, tourism and entertainment	More than 50,000	Other	Cyber and Advisory Leader	5
Finance and insurance	Less than 1,000	CISO or Head of Security		11
Finance and insurance	Less than 1,000	CISO or Head of Security		30
Industrial, energy, transport and logistics	1,000 to 50,000	CISO or Head of Security		17
Services, retail, tourism and entertainment	1,000 to 50,000	Other	Head of Security Architecture	20
Finance and insurance	More than 50,000	CISO or Head of Security		6
Finance and insurance	1,000 to 50,000	CISO or Head of Security		24
Services, retail, tourism and entertainment	1,000 to 50,000	Other	Head of Cloud Security Engineering	14
Government, public bodies and non-for-profits	1,000 to 50,000	Other	Head of IT Infrastructure	30
Industrial, energy, transport and logistics	More than 50,000	CISO or Head of Security		25

Industry sector	Size	Role		Years of experience in cyber security
Finance and insurance	1,000 to 50,000	Other	Senior Group Incident and Disaster Recovery Manager	6
Services, retail, tourism and entertainment	Less than 1,000	CIO or Head of IT		4
Government, public bodies and non-for-profits	1,000 to 50,000	Other	Information Security Manager	12
Industrial, energy, transport and logistics	More than 50,000	CISO or Head of Security		25
Finance and insurance	More than 50,000	Other	Cyber Risk and Analysis Senior Manager	15
Finance and insurance	Less than 1,000	CISO or Head of Security		16
Finance and insurance	1,000 to 50,000	Other	Cyber and Information Security Risk Office	18
Industrial, energy, transport and logistics	More than 50,000	CISO or Head of Security		20
Industrial, energy, transport and logistics	1,000 to 50,000	Other	Leader for Cyber Security Services	27
Services, retail, tourism and entertainment	More than 50,000	Other	Cyber security Consultant	12
Industrial, energy, transport and logistics	1,000 to 50,000	CISO or Head of Security		30

Table F2 *Delphi survey participants round 2*

Industry sector	Size	Role		Years of experience in cyber security
Government, public bodies and non-for-profits	More than 50,000	CISO or Head of Security		17
Government, public bodies and non-for-profits	1,000 to 50,000	Other	Information Security Manager	23
Finance and insurance	1,000 to 50,000	CISO or Head of Security		25
Government, public bodies and non-for-profits	1,000 to 50,000	CISO or Head of Security		18
Services, retail, tourism and entertainment	1,000 to 50,000	CISO or Head of Security		10
Services, retail, tourism and entertainment	1,000 to 50,000	CISO or Head of Security		25
Services, retail, tourism and entertainment	1,000 to 50,000	Other	Head of Cyber Security Architecture	25
Services, retail, tourism and entertainment	1,000 to 50,000	Other	Head of Cloud Security Engineering	14
Industrial, energy, transport and logistics	1,000 to 50,000	CISO or Head of Security		15
Industrial, energy, transport and logistics	More than 50,000	CISO or Head of Security		25
Industrial, energy, transport and logistics	Less than 1,000	CIO or Head of IT		15

Industry sector	Size	Role		Years of experience in cyber security
Industrial, energy, transport and logistics	1,000 to 50,000	CISO or Head of Security		25
Services, retail, tourism and entertainment	More than 50,000	Other	Advisory and Cyber Leader	6
Finance and insurance	Less than 1,000	CISO or Head of Security		15
Services, retail, tourism and entertainment	Less than 1,000	CIO or Head of IT		4
Finance and insurance	More than 50,000	Other	Cyber Risk and Analysis Senior Manager	17
Services, retail, tourism and entertainment	1,000 to 50,000	CISO or Head of Security		15
Industrial, energy, transport and logistics	1,000 to 50,000	CISO or Head of Security		30
Finance and insurance	1,000 to 50,000	CISO or Head of Security		23
Finance and insurance	More than 50,000	Other	Cyber Risk	15
	More than 50,000	Other	Consultancy	25

Appendix G - Potential future research questions

Future research questions:

- What learning from incident practices are the most commonly used?
- How do organisations in specific sectors such as the public sector, technology sector and critical national infrastructure sectors learn from incidents?
- How do the learning from incident practices compare between different geographical regions?
- Does the size of an organisation's cyber security team or the years experience of their CISO impact the learning practices adopted?
- When compared, what enables some organisations / some industries to be more effective at learning from incidents than others?
- How do organisations examine how effective they are at learning from incidents?
- How effective is learning from incidents in reducing the prevalence of future incidents?
- What are the perspectives of stakeholders outside cyber security incident response teams on the effectiveness of learning from incidents?
- What is the optimal investment of time and resources in learning from incident activities and how is this determined?
- How does organisational culture and governance structures influence incident learning?
- What is the value of participants from different functions and levels of seniority in investigating the causes of incidents?
- Which strategies are effective in working with suppliers on learning from incidents?
- What are the most effective mechanisms and tools to identify lessons from incidents?
- In what ways do organisations allow the underlying causes to exist and incidents to occur?
- What are the optimal governance structures to enable decision-making and accountability for implementing lessons learned?
- How does culture impact the ability of an organisation to learn from incidents?
- What are the barriers that prevent organisations learning from incidents and how might these be overcome?
- How effective are the recommendations in this research at improving learning from incidents, as assessed by the organisations implementing them?