Computers & Security 139 (2024) 103699

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

"I don't think we're there yet": The practices and challenges of organisational learning from cyber security incidents

Clare M. Patterson *, Jason R.C. Nurse, Virginia N.L. Franqueira

Institute of Cyber Security for Society (iCSS), School of Computing, University of Kent, Canterbury, UK

ARTICLE INFO

Keywords:
Cyber security incidents
Organisational learning
Post-incident review
Cyber resilience
Learning practices
Lessons learned
Neo-institutional theory
Isomorphic pressures

ABSTRACT

Learning from cyber incidents is crucial for organisations to enhance their cyber resilience and effectively respond to evolving threats. This study employs neo-institutional and organisational learning theories to examine how organisations learn from incidents and gain insights into the challenges they face. Drawing on qualitative research methods, interviews were conducted with 34 security practitioners from organisations operating in the UK spanning a range of industries. The findings highlight the importance of consciously evaluating learning practices and creating a culture of openness to hear about incidents from employees, customers and suppliers. Deciding which incidents to learn from, as well as who should participate in the learning process, emerged as critical considerations. Overcoming defensiveness and addressing systemic causes were recognised as barriers to effective learning. The study emphasises the need to assess the value and impact of identified lessons and to avoid superficial reviews that treat symptoms rather than underlying causes to improve resilience. While progress has been made in learning from incidents, further enhancements are needed. Practical recommendations have been proposed to suggest how organisations may gain valuable insights for maximising the benefits derived from incident learning. This research contributes to the existing knowledge on organisational learning and informs future studies exploring the social and political influences on the learning process. By considering the suggested recommendations, organisations may strengthen their cyber security, foster a culture of continuous improvement, and respond effectively to the dynamic cyber security landscape.

1. Introduction

The rapid advancements in digital technologies, devices, and interconnectivity have revolutionised operational efficiency and cost reduction within organisations (De Reuver et al., 2017). However, these transformative benefits come hand in hand with the persistent and ever-evolving risk of cyber threats (NCSC, 2022b). The traditional notion of defending organisational perimeters has become obsolete as organisations now exist within a dynamic ecosystem characterised by fluid boundaries and intricate interdependencies with suppliers. The integration of new digital technologies into legacy IT infrastructures introduces increased complexity, consequently heightening cyber security risks (WEF Global Cybersecurity Outlook, 2023). In addition, as business operations become increasingly automated, the attack surface for cyber adversaries expands, underscoring the paramount importance of continuously enhancing an organisation's cyber security capabilities (Akinrolabu, 2019).

Globally, the number of cyber-attacks continues to grow in scale and complexity, with new attacks being innovated daily (CrowdStrike, 2023). The costs and impacts of such attacks are substantial, with cyber-attacks projected to cost the world over USD 8 trillion in 2023 (Morgan, 2023). Industry reports indicate a 50% increase in the number of cyber-attacks globally in 2021 compared to the previous year (Check Point Research Team, 2022). Furthermore, cybercrime-related costs in the US have grown from nearly USD 7 billion to more than USD 10 billion between 2021 and 2022 (FBI's Internet Crime Complaint Center (IC3), 2022). These costs include revenue and reputation losses, as well as leaks of sensitive information. It is important to note that the actual costs of cyber-attacks may be even higher due to underreporting by businesses concerned about reputational damage or incidents which remain undetected.

These escalating numbers highlight the severity of the situation and the urgent need for robust cyber security measures. Cyber risks are considered one of the top five threats to companies by over four thousand CEOs from over one hundred countries surveyed by PwC (2023) and nearly half of them were consequently planning to increase their

* Corresponding author.
E-mail address: cmp54@kent.ac.uk (C.M. Patterson).

https://doi.org/10.1016/j.cose.2023.103699
Received 18 August 2023; Received in revised form 21 November 2023; Accepted 31 December 2023
Available online 5 January 2024

investments in cyber security. The shortage of skilled cyber security professionals (Hüsch and Sullivan, 2023) means organisations need to find better ways to reduce the prevalence of incidents. By enhancing their cyber security capabilities, organisations can try to better protect their assets and mitigate the risks posed by cyber security incidents.

Cyber security incidents serve as a wake-up call for organisations, highlighting weaknesses in their security posture and providing an opportunity to learn and enhance resilience (Baskerville et al., 2014). By examining the lessons learned from such incidents, organisations can bolster their defences and protect themselves against future threats (Van der Kleij et al., 2017). However, it remains unclear if organisations are effectively harnessing these incidents as learning opportunities. This article investigates the current practices employed by organisations in learning from cyber security incidents and explores the challenges they encounter in this process.

Organisational learning, as understood in this article, refers to the collective learning that occurs within an organisation, emphasising changes made at the organisational level rather than individual learning (Crossan et al., 1999). In accordance with the National Institute of Standards and Technology (NIST) definition, a cyber security incident is defined as *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.). The NIST 800-61 R2 guide (Cichonski, 2012) and other industry guidance include a post-incident review phase in their recommended practices, suggesting organisations can learn from incidents to improve their cyber security measures (see Appendix D for further details on the industry guidance).

While previous research suggests that organisations can benefit from improving their learning practices in the aftermath of incidents, there is currently no consensus on what constitutes good practice in this domain (Patterson et al., 2023). Furthermore, limited research has been conducted in recent years to assess whether earlier recommendations by researchers are being implemented by organisations. This article aims to bridge this gap by examining the current practices employed by organisations in learning from cyber security incidents and the challenges they face in this process.

To analyse the forces that shape organisational learning practices, we utilise two theoretical lenses: neo-institutional theory and organisational learning theory. Neo-institutional theory offers valuable insights into the external pressures, norms, and institutional influences that contribute to an organisation's learning behaviour (Hasan et al., 2021). In parallel, organisational learning theory allows us to assess the quality of learning processes within organisations (Miranda, 2020; Rządca and Strumińska-Kutra, 2016; Shortell, 2016). This study aims to gather insights from security practitioners across various organisations regarding their current learning practices in the context of cyber security incidents and the associated challenges. Our primary research question is:

> How do organisations currently learn from cyber incidents, and what challenges do they encounter in the learning process?

The subsequent sections of this article are structured as follows. Section 2 provides an overview of existing research on organisational learning from cyber security incidents and introduces the neo-institutional and organisational learning theoretical frameworks and their application in the realm of cyber security. Section 3 describes the research methods employed in this study. Section 4 presents the themes identified through interviews conducted for this research. This is followed by a discussion of the findings, the limitations of the study, and practical implications in Section 5. Finally, Section 6 concludes the paper by summarising the key findings and suggesting avenues for future research.

2. Background and related work

2.1. Organisationational learning theory and its application to cyber security

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 and Lyles, 2012; Fiol and Lyles, 1985; Huber, 1991). Argote and Ophir (2017) describe organisational learning as a process that changes the organisation as a result of experiences. Fiol and Lyles (1985) view organisational learning as the acquisition of knowledge from experiences and the translation of that knowledge into actions taken by the organisation. By studying learning from cyber security incidents, our aim is to understand both the practices organisations employ to extract lessons from incidents and the changes they make because of them.

The concept of organisational learning was first introduced by Cyert and March (1963). Argyris and Schön (1978) later solidified the idea and introduced the crucial concepts of single and double-loop learning. Learning is triggered by either aligned outcomes with planned expectations, i.e. a 'match', or not aligned, i.e. a 'mismatch', as is the case when an incident occurs and organisations want to learn how to avoid that outcome in the future, see Fig. 1. Single-loop learning represents straightforward adjustments, such as recognising an unmonitored server and including it in the Security Operations Centre's monitoring. Double-loop learning delves deeper into the processes, organisational structures, and decisions that lead to the omission of a server from monitoring. Their work sparked subsequent research, including Senge's contributions (Senge, 2010), which not only defined the characteristics of a learning organisation but also incorporated elements of systems thinking, building upon Argyris and Schön's theories. Cyber security researchers have also applied the models of double-loop learning in the study of how organisations learn from incidents, as evidenced by studies conducted by Ahmad et al. (2012, 2020) and Shedden et al. (2010, 2011). Nonetheless, further research is essential to explore this topic in greater depth (He et al., 2014; Hove et al., 2014; Line and Albrechtsen, 2016; Shedden et al., 2010; Tøndel et al., 2014).

Early research by Niekerk and von Solms (2004) introduced the concept of double-loop learning but suggested the need for further investigation. Shedden et al. (2010) provided a valuable introduction to learning from incidents, with a review of organisational learning literature that emphasises the application of double-loop learning principles to strengthen incident response and organisational security. Double-loop learning involves delving deeper into understanding the factors that contributed to the occurrence of an incident, going beyond identifying the immediate cause. Wiik and Kossakowski (2005) identified a capability trap in incident handling, where organisations become overwhelmed with incidents and struggle to allocate time for improvements. Gonzalez (2005) similarly highlighted the challenge of diverting resources from incident handling to invest in learning from incidents.

Research specific to learning from security incidents has primarily focused on four main clusters: the Norwegian petroleum industry (Jaatun et al., 2009; Line et al., 2009), the Australian financial sector (Ahmad et al., 2012, 2015; Shedden et al., 2011), the Chinese healthcare sector (He et al., 2014; He and Johnson, 2017), and the UK financial sector (Grispos, 2016; Grispos et al., 2017, 2019). For example, within the energy industry, the Incident Response Management method (Jaatun et al., 2007) incorporates safety processes that are founded on the double-loop learning processes originally introduced by Argyris (1976). Studies by Jaatun et al. (2008; 2007) and Line et al. (2006) examined the end-to-end incident management process, highlighting cultural hesitancy to report incidents and the significance of the learning phase (Jaatun et al., 2009). Bartnes et al. (2016) also emphasised the value of exploring double-loop learning from incidents, even minor ones.

These findings align with earlier research by Ahmad et al. (2012) which also found reviews for high-impact incidents, but potentially

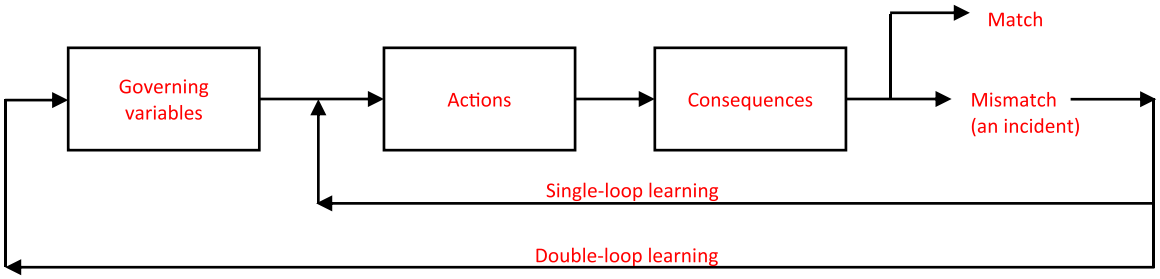

Fig. 1. Single-loop and double-loop learning adapted from Argyris (1999).

missing learning opportunities from lower-impact incidents. Ahmad et al. (2015) observed similar limitations in participation and knowledge sharing in post-incident reviews in another Australian financial business. Grispos (2016) studied a financial organisation in the UK, highlighting the need for a cultural shift to enable effective root cause analysis and the challenges of time constraints. He also suggested that, due to the absence of a common definition of the analysis process, it was not clear to members of the incident response team conducting the analysis if the steps they took were adequate. Grispos et al. (2017) introduced retrospectives to evaluate incident response effectiveness and the implementation of lessons learned, finding that, despite the availability of additional information, it was not always effectively used to improve security.

He et al. (2015, 2014a, 2014b) and He and Johnson (2015, 2017) explored the use of Goal Structuring Notations (GSN) to understand the causes of cyber security incidents. GSN effectively demonstrated incident causes in terms of control or policy failures but had limitations in capturing underlying socio-technical causes (He et al., 2015, 2014b; He and Johnson, 2017, 2012). Additionally, Nese (2018) conducted research on learning lessons from incident intrusion data and recommended integrating data from intrusions with threat intelligence to improve the detection of incidents in the future. Van der Kleij et al. (2017) in their study of incident response teams concluded that learning from incidents at an organisational level needs to be improved by implementing a systematic lessons learned procedure.

While previous research has leveraged organisational learning to enhance the analysis of incident causes, limited attention has been given to data collection during causal investigations or the implementation of identified lessons, and their subsequent impact on reducing future incidents. These gaps in the literature underscore the potential for organisations to refine their incident learning processes. This study employs organisational learning theory to scrutinise whether the practices employed by organisations for learning from incidents effectively contribute to enhancing cyber security.

2.2. Neo-institutional theory and its application to cyber security

The practices of organisational learning from incidents in cyber security are influenced by various factors, including IT processes, standards, regulatory requirements, military and safety approaches, organisational culture, and established norms. Institutional theory has been frequently used in research on information systems to explain organisational practices in the context of wider pressures (Cavusoglu et al., 2015). The neo-institutional theory was chosen as a framework for this study because it considers both internal and external factors in explaining the evolution of organisational practices (Hasan et al., 2021; Hu et al., 2007). It is currently one of the most used in organisation studies (Alvesson and Spicer, 2019). The theory proposed by Dimaggio and Powell (1983) provides a valuable lens for examining the influences that shape these practices. It highlights how isomorphic pressures, i.e., coercive, normative and mimetic, can unconsciously drive organisations to conform to common practices without adequately evaluating their effectiveness, see Fig. 2.

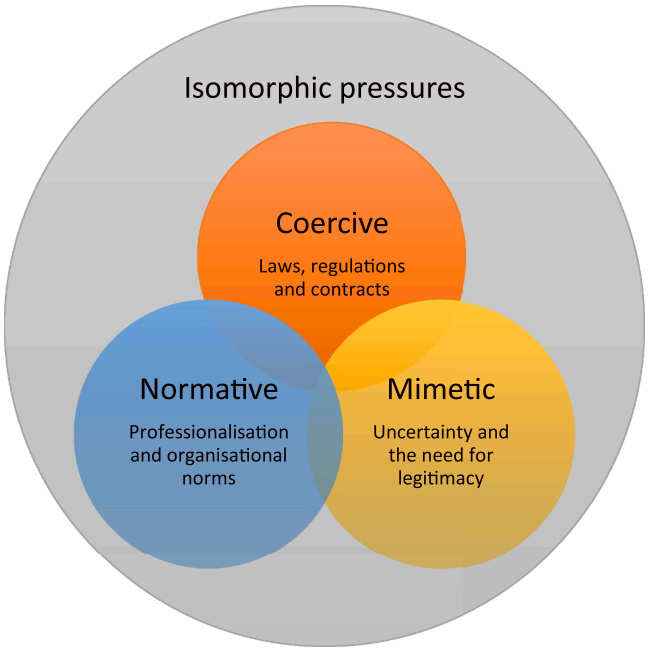

Fig. 2. Attributes of isomorphic pressures in neo-institutional theory. Adapted from Dimaggio and Powell, (1983).

Coercive pressures encompass regulations, laws, legal contracts, and market structures that organisations are obliged to comply with. The standards and guidance available to organisations emphasise the importance of learning from incidents for improving overall cyber resilience (for further details see Appendix D). For example, the ISO/IEC 27035 outlines enhancements to security control implementation, policies, risk assessments, threat intelligence, security databases, and incident management plans. It also suggests that organisations should go beyond individual incidents to identify trends and take preventive actions to reduce the likelihood of future incidents.

While these standards and guidance acknowledge the need to identify systemic weaknesses, they do not provide specific guidance on how to effectively identify and implement lessons to reduce the likelihood and impact of future incidents (Ahmad et al., 2020). These documents often assume a positivist epistemological perspective, treating lessons as ready-to-be-harvested crops. However, the process of uncovering lessons is a collaborative effort between different stakeholders (Lundberg et al., 2009, 2010). The quality and effectiveness of lessons learned from incidents are heavily reliant on the thorough identification of underlying causes (Boin et al., 2008).

Normative pressures emerge from the professionalism of the cyber security field and the sharing of practices by service providers, such as consultants, as well as the utilisation of standard tools and templates. For instance, organisations may 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). The level of cyber security expertise among board members can shape leadership's expectations for organisational security practices (Gale et al., 2022).

The uncertainty resulting from rapid technological innovation and the unpredictability of cyber-attacks create **mimetic pressures**. Organisations strive to imitate practices seen as successful to gain legitimacy for their own approaches. Cross-industry groups and conferences play a role in disseminating similar practices. Organisations may adopt practices simply because more mature organisations have implemented them, without considering whether those practices are truly the best fit for their own context (Jeyaraj and Zadeh, 2020).

In recent years, the neo-institutional theory has been applied in several studies to investigate the impact of **isomorphic pressures** on cyber security practices. For instance, Cavusoglu et al. (2015) examined the influence of institutional pressures on organisations' adoption of cyber security measures. Their study revealed that coercive and normative pressures played a significant role in compelling organisations to enhance their security capabilities. However, the study did not find a similar effect for mimetic pressures.

Vuko et al. (2021) conducted a study on the effectiveness of internal audit assurance in managing cyber security risks. Their analysis also identified the influence of mimetic pressures, assessed by the level of outsourcing, but found that normative and coercive pressures had a stronger impact. Specifically, the presence of normative pressures was associated with higher cyber security audit effectiveness, as indicated by the security qualifications of internal auditors.

In contrast, earlier research by Barton et al. (2016) found that only mimetic influences were correlated with senior management belief in the importance of information system security, while normative and coercive pressures had an insignificant impact. Similarly, Al-ma'aitah (2022) found that mimetic and coercive pressures had the most significant impact on enhancing cyber security in organisations based on a study of Jordanian governmental organisations. Interestingly, their findings contradicted those of Jeyaraj and Zadeh (2020), which could be attributed to a potential lack of understanding of the concept of normative pressures among the survey respondents in the study by Al-ma'aitah (2022).

Moreover, in their study on the isomorphic nature of cyber security practices, Jeyaraj and Zadeh (2020) explored how organisations adopt similar approaches over time. They discovered that mimetic pressures played a substantial role in shaping organisations' behaviour, as they sought to emulate the security strategies and technologies employed by market leaders to enhance their resilience against cyber threats. Notably, their research emphasised the evolution of the pressures over time. Although coercive pressures demonstrated a more substantial impact in the immediate timeframe, over the long term, as the security practices an organisation put in place in response to new regulations became firmly established, normative pressures were stronger in shaping these practices.

Similarly, Hu et al. (2007) investigated the impact of institutional pressures on organisations' cyber security capabilities, focusing on regulations such as the Sarbanes-Oxley Act of 2002 (2020). Their findings indicated that coercive forces significantly influenced organisations' security practices while distinguishing the effects of normative pressures from mimetic influences was more challenging in the specific organisation they studied.

In a recent study by Gale et al. (2022), neo-institutional theory was employed to examine directors' engagement with cyber security at the board level. Their study concluded that coercive and normative pressures had the strongest impact, but mimetic pressures also influenced board members' engagement with cyber security.

By employing neo-institutional theory as our analytical framework, this study focuses on gathering insights from security practitioners across organisations regarding their existing learning practices in the context of cyber security incidents and the associated challenges. Through an exploration of coercive, normative, and mimetic pressures, we aim to deepen our understanding of the factors that influence organisational learning practices in the cyber security domain. This research builds upon the existing body of knowledge, enriching our comprehension of how security practitioners navigate these pressures and adapt their cyber security learning practices to enhance resilience against evolving cyber threats.

3. Research methods

To explore how organisations experience, understand, and practice learning from incidents, a qualitative approach was chosen, as this allows an in-depth understanding of the phenomenon (Paulus, 2021). Recognising both the merits of positivist and constructivist theoretical frameworks, this research tries to be pragmatic and takes a position between these two extremes. This study seeks to understand and analyse the practices organisations adopt to learn from incidents. Whilst, at the same time, it acknowledges how individuals describe their experience, reflects the context of their organisation, as well as the wider industry or social environment. This research only studies the "lived experience" of the security practitioners and recognises there will be multiple constructed perceptions by other stakeholders of how an organisation learns (Willig, 2022).

This study received ethical approval from the University of Kent's ethics review board before conducting interviews with participants. Given the sensitive nature of the topic stringent measures were taken to ensure confidentiality and anonymity of participants. However, it is important to note that, details pertaining to specific organisational incident learning processes are presented in a generalised and anonymised manner. The procedures and results discussed in this study represent aggregated insights from multiple sources and are intended to contribute to the broader understanding of cyber security incident learning practices rather than provide a detailed account of specific organisational procedures. Every effort has been made to protect the identities of the participants and the organisations involved.

A semi-structured approach was selected to address all key question areas (see Appendix B) with each participant. This approach allows variations in question wording in individual interviews to allow interviewees to share their personal experiences and interpretations. This enables a more nuanced understanding of the complex process of learning from incidents. Senior security practitioners were identified across a range of industries from organisations in the private and public sectors, who met the criteria of having operations in the UK and more than 250 employees (as these are more likely to have experienced an incident and to have made changes as a result of it (NCSC, 2022a). The 34 practioners were interviewed between October 2022 and April 2023 and their organisations ranged in size from 450 employees to over 200, 000. These organisations represent a cross-section of industries, which were for convenience grouped into four main categories; see Table 1 and further details in Appendix A.

The interviewees were chosen based on their role to ensure they have sufficient knowledge of how their organisation learns from incidents. There was no incentive offered for participating in the study. A purposive sampling method was adopted as this allows the sample selected to match the research aims (Campbell et al., 2020). This was supplemented with further participants added through snowball sampling to ensure a

Table 1
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**

broad range of industries was covered. This is based on the assumption that different industries may have differing practices and, by intentionally selecting participants from a range of industries, a more complete answer to our research questions can be gathered. Tetrick et al. (2016) adopted a similar approach in their study of improving the skills and team effectiveness of cyber security incident response teams across 17 organisations. The number of security practitioners interviewed is small compared to the total population. However, this number of interviews was considered sufficient to answer the research question. As O'Reilly and Parker (2013) claimed, it is not only the number of participants but also the appropriateness of the data they can provide. Half of the participants were Chief Information Security Officers (CISO) or had a leadership-level role reporting directly to the CISO (e.g. four Heads of Incident Response, two Information Security Managers, two Cyber Security Risk Managers). Overall, the participants had spent an average of 15 years of working in cyber security providing a wide source of experience to draw upon and lends credibility to their insights.

Pilot interviews were held to test the questions and an interview protocol was used to ensure all topics were covered with every participant, but detailed questions varied according to the interviewees' personal experiences and interpretations. Questions were always asked about the learning practices of the organisation including reporting, investigating the causes of incidents, identifying lessons and implementing them. All participants were also asked for their views on what enabled organisations to learn and what they saw as the obstacles to successfully learning from incidents. For the interview protocol, see Appendix B.

The interviews were conducted, virtually (28) or face-to-face (6) depending on the preference and the availability of participants and lasted an average of 39 mins. All interviews were audio recorded and transcribed. Due to the confidential nature of the topic, any elements identifying the individual or organisation were removed. Following a similar approach to that adopted by Clare and Kourousis (2021) in their study of learning from incidents in aviation maintenance. The interview transcripts were analysed after each interview and coded by the first researcher, supported by the NVivo software. The transcripts underwent multiple rounds of analysis, with codes being iteratively refined throughout the study. These refinements were achieved through discussions with the research team and a thorough review of relevant literature. The coding process aimed to identify predominant patterns and significant insights expressed by interview participants, which were then fine-tuned through several iterations involving all authors. Key themes were rigorously developed and collectively agreed upon by the authors, ensuring they were well-grounded in the data and provided valuable perspectives on the research question. Our approach was influenced by the Braun and Clarke's methodology (2006); refer to Appendix C for the codebook and themes.

The interviews were conducted to gain insights into the perspectives of security practitioners regarding their organisations' learning practices and the challenges they confront in this process. Consequently, quantifying the frequency of topics mentioned by participants was not deemed suitable due to variations in depth and emphasis. Adopting an approach suggested by Braun and Clarke (2022) to offer an idea of the significance of the finding, terms such as 'many' were employed when at least 20 practitioners referred to a specific topic. Throughout this study, quotations from the data are included to exemplify these themes and provide a deeper understanding of our analysis.

4. Findings

4.1. Isomorphic pressures on organisational learning practices

The analysis of the interview data led to the identification of four overarching themes that emerged across the interviews, see Fig. 3. In response to the initial aspect of the research question on how organisations currently learn from cyber incidents, the first theme – "Isomorphic pressures on organisational learning practices" – highlights how the current practices of learning from incidents have developed under the influence of isomorphic pressures, aligned with neo-institutional theory. It became evident that organisations engage in these practices without explicitly assessing their effectiveness. When participants were asked how they evaluated the effectiveness of their practices of learning from incidents, none reported their organisations had deliberately assessed them although many cited the absence of a repeat of the same incidents as evidence lessons had been learnt.

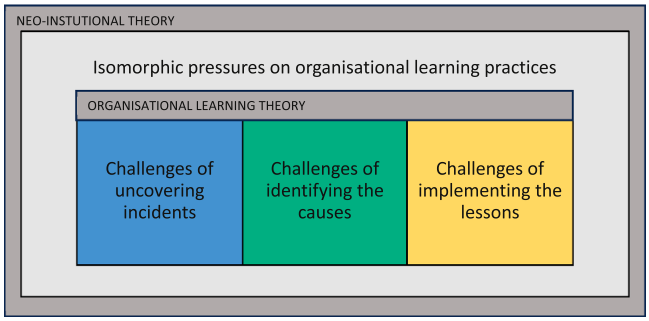

Fig. 3. Themes developed in this study.

To address the second aspect of the research question concerning the challenges encountered in the learning process, three themes were developed, drawing upon organisational learning theory. They reflect the participants' accounts of what impeded maximising their learning from incidents. These three themes cover challenges faced at different stages of the learning process; challenges of uncovering incidents, challenges of identifying the causes, challenges of implementing the lessons.

4.1.1. Coercive pressures

Coercive pressures such as regulatory reporting requirements played a significant role in shaping incident communication practices and in the involvement of legal and communications teams in incident response. Participants frequently described the challenges of being part of a global organisation, as determining jurisdiction can become complex due to factors such as the impacted subject, the location of the breach, or the identity of the attacker [P6]. The involvement of multiple offices and the need to communicate with different regulators and government organisations further exacerbated the complexity of incident communication [P16].

Also, market structure coercive pressures resulted in all organisations implementing contractual obligations for their suppliers to report cyber security incidents to them. The IT services of organisations are now frequently inextricably dependent on a web of suppliers. Yet, participants expressed frustration with the lack of transparency from suppliers, "*sometimes we see it in the press quite honestly and so even though we have contractual requirements, you know it's quite complicated*" [P33]. Others commented that information about incidents is often limited to public relations messages or website publications [P20]. This limited transparency created a need for assumptions and delayed the organisations' ability to assess the impact of incidents, as one participant explained: "*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 acknowledged the challenges, they also recognised their role in shaping the relationship with suppliers encouraging them to be more forthcoming. Creating a culture of open communication with suppliers was seen as vital to enable proactive action and collaboration:

> *"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]

However, participants also expressed concerns about their own organisations' fear of litigation or regulatory actions, which limited their willingness to share incident information with other organisations. While some participants shared sanitised lessons with regulators beyond legal requirements to benefit others in the industry, this practice was not widespread. There was a recognition among participants that a mechanism should be established to allow organisations to share incident lessons without negative consequences for the sharing organisation.

More than half of the participants acknowledged that fear of legal or regulatory consequences had a significant impact on the depth of investigations and the actions taken following incidents; *"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."* [P24]. As another participant described, the fear of regulation and litigation created a sense "*of nervousness about writing down root causes and learnings … that sort of stops people from being as candid as they could about what happened."* [P10].

While some participants shared sanitised lessons with regulators beyond legal requirements to support others in the industry, this practice was not broadly observed. Participants recognised the societal benefit of sharing incident lessons, allowing others to learn and receive support. However, uncertainty remained about the appropriate mechanisms for enabling incident sharing without it causing issues for the sharing organisation. There was a call for the industry as a whole to mature towards the "*ability to share freely while knowing that it's not going to backfire in many ways."* [P7].

4.1.2. Normative pressures

Normative pressures influenced the practices of incident reporting and classification within organisations. While there was a standard approach to mandatory training on the need to report cyber security incidents, there was no explicit assessment of its effectiveness. However, many organisations supplemented the mandatory training with additional encouragement, fostering a blame-free culture where individuals felt safe to report incidents.

All organisations had some method of classifying incidents based on their impact. However, each organisation had a slightly different approach. Some used classifications such as Gold, Silver, and Bronze, while others employed a scale of 1–4 or 1–5. Participants also reported following the general IT incident management process their organisations had for prioritising any IT incidents, "*I try and use as much of the IT process as I can and not reinvent the wheel.*" [P28]. Whilst participants were not explicitly asked about industry frameworks several voluntarily mentioned either the ITIL (IT Infrastructure Library) IBM, (2022) (P12, P20, P24, P25, P28, P30) or NIST (NIST, 2018) (P5, P10, P14, P15, P19) frameworks. Although some organisations attempted to align their incident classification with their IT incident classification, others used a dedicated cyber security classification. Different organisations employed different approaches to categorise incidents, with some distinguishing data breaches from cyber-attacks while others used a single security incident classification. The uniqueness of each cyber incident was cited as a challenge to standardising incident classifications.

Despite having defined incident classifications, participants mentioned their organisations did not always adhere to their own definitions of incident classification due to organisational politics and the desire to assign certain people or prioritise specific incidents. Moreover, the classification of an incident could change during its lifecycle as more information about the impact and nature of the incident became available. This led to incidents being reclassified or, in some cases, never officially classified as incidents at all. As one participant explained *"We do have some that we will classify as a P2 because it could be and then it dies down and is re-classified as a P3, and then it won't go into the post-incident process"* [P18]. How incidents are classified is important as it determines the level of post-incident investigation conducted.

Practitioners relied on their judgement to assign incident classifications, driven by the required incident response rather than a consideration of the level of post-incident learning. The classification of an incident often determined the involvement of senior management in post-incident review investigations, as well as which teams participated in the review process based on the areas impacted. The nature of the incident determines which teams are involved:

"It depends on what the incident is. So, if it's an incident related to, say, HR systems then HR would need to be part of that conversation all the way through because they own the application or they own the service, so it depends on the area impacted." [P22].

The classification of an incident determined the effort an organisation made to learn from it, the participants involved in post-incident reviews, and with whom the results were shared. However, the process of classifying incidents remained subjective. There was no consistency across organisations as one participant admitted "… *as cyber practitioners that is a deficiency worldwide, currently we don't classify incidents the same way anywhere and frameworks are just now beginning to come out."* [P33]. This lack of uniformity makes it difficult to obtain reliable statistics on the number of cyber security incidents, further emphasising the challenges associated with studying incidents in the field of cyber security.

4.1.3. Mimetic pressures

Mimetic pressures played a significant role in the participants' perspectives on learning from incidents. While they expressed an urgent desire for more information sharing and learning from peers, they acknowledged that individuals often prioritise learning from incidents that directly affect them. Moreover, they found it challenging to share detailed incident information with others due to concerns about litigation, regulatory implications, and contractual obligations.

In the face of uncertainty, organisations tend to imitate the practices of others. Participants discussed the difficulties of implementing lessons learned due to leadership's limited understanding of cyber risk and the constant evolution of the field, making it challenging to quantify and address incidents effectively. Although participants recognised the importance of learning from incidents impacting other organisations particularly peers, they often perceived less motivation and urgency to learn when an incident occurred in a different organisation or industry. The distance between the incident and their own organisation affected their level of engagement with the incident and the perceived relevance of the lessons learned *"If you're in Germany, an incident happens in Spain, you don't experience it in the same way."* [P10]. However, participants acknowledged that the types of incidents happening in other organisations informed their perception of threats to their own organisation. Many believed that increased sharing of incidents by other organisations would facilitate learning within their own organisations. Conscious efforts were made to share incident information with regulators, security agencies, and peers to assist others, although participants acknowledged "*you spread the knowledge that you get from the incidents. But this often doesn't happen because of the high workload"* [P19].

4.2. Challenges of uncovering incidents

The participants emphasised the challenges associated with gaining comprehensive awareness of incidents within their organisational environment. They expressed a sense of perpetual concern, acknowledging that it was only a matter of time before a major incident occurred if they had not experienced one recently [P18, P25]. This awareness motivated them to actively seek out potential problems, recognising the

proactive identification of incidents as crucial. Several participants articulated their desire for improved visibility into incidents, believing that more incidents were happening than they were currently aware.

As organisations increasingly recognise the importance of encouraging incident reporting by employees, customers, and suppliers, they are shifting away from a culture of individual blame. Instead, incidents are viewed as opportunities for the whole organisation to learn not just that one person [P23]. The focus has shifted from punishing individuals to treating them as victims of a crime, with their consent to share their stories to encourage others to come forward [P18]. Reflecting on this cultural shift, one participant stated, "*We've taken a step away from that culturally*" [P5]. The practitioners emphasised the value of fostering a culture of openness within their organisations, as one participant memorably described it: *"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."* [P29]

Most interviewees expressed the need for a work environment that embraces incidents as opportunities for growth and improvement, rather than as occasions for personal advancement or the detriment of others. This shift in mindset was observed industry-wide, not only in how employees were treated but also in the hiring and termination of Chief Information Security Officers (CISOs). Participants noted a reversal in hiring practices, with organisations now seeking candidates who possess incident experience [P5, P17]. However, they acknowledged that creating a culture of speaking up and promoting transparency presented significant challenges. They recognised that overnight cultural change was not feasible but were committed to working towards it [P5, P6, P9]. Summarising the challenge, one participant stated, "*The biggest single challenge so far has been to encourage a culture of openness and transparency amongst our people to admit failure*" [P12].

4.3. Challenges of identifying the causes

In the study, participants highlighted several challenges encountered when attempting to identify the true causes of incidents within their organisations. While many participants expressed satisfaction with the thoroughness of their investigations, none of the organisations had deliberately assessed how well they were investigating causes. Some participants described finding a root cause and articulating it as the failure of one component of the system, often overlooking less obvious causes such as culture or funding models. As one participant mentioned, "*We'd look at the control failure and we'd articulate it in the context of the control failure*" [P5].

Participants acknowledged the opportunity to improve the depth of incident causal analysis, "*that second level of really digging, is certainly an improvement area we could make."* [P31]. Practical constraints, such as limited time and resources, hindered their ability to explore more systemic causes. For example, one participant highlighted the need to take a step back and review the end-to-end process to understand why certain vulnerabilities existed in their managed IT infrastructure:

> *"We've identified a significant number of vulnerabilities in our managed estate that says the patching process isn't working right. This doesn't mean you need to thrash the patching people harder because they're doing their best. What this says is you need to take a step back and review the end-to-end process to say why? Why is this not working? What's gone wrong? And the trouble doing that is that it takes time." [P18].*

Motivating people to prioritise investigations into underlying causes posed an emotional challenge. The impact of serious incidents often took a toll on the affected teams, and once normal operations were restored, there was a tendency to move on rather than revisit the incident's causes. As one participant stated, "*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*" [P4].

The quality of post-incident investigations heavily relied on having the right individuals involved at the right time. Combining people with operational knowledge and those with sufficient seniority was seen as crucial for developing meaningful lessons and actions. However, securing the necessary participation proved challenging due to limited availability and competing demands on individuals' time. As one participant *emphasised, "I'm a very big fan of having business representation because they do ask the right questions"* [P2].

Organisational politics and individual defensiveness were also identified as significant barriers to identifying causes. The multidimensional nature of cyber incidents made it difficult to assign blame, resulting in individuals shifting responsibility or pointing to external factors to avoid being held accountable. Overcoming these dynamics was seen as requiring a cultural shift towards a climate of learning and improvement rather than one of blame and defensiveness. One participant suggested involving the internal audit team to assess the quality of after-action reports instead of solely focusing on the frequency of issues [P1].

Organisations recognised the value of analysing incidents classified with lower severity ratings to identify trends and underlying causes. However, this process depended on consistent labelling of causes and required dedicated data analytic resources. Many participants expressed the need for improvement in tracking themes and trends related to incident causes, acknowledging that their organisations were not yet fully equipped to perform this analysis effectively. As one participant noted, "*Could we do better in terms of tracking themes or trends? Absolutely. I don't think we're there yet*" [P7]. Overall, these challenges highlight the complexities involved in understanding the causes of incidents and underscore the importance of addressing organisational culture, resource allocation, and trend analysis capabilities to enhance the effectiveness of incident investigations and learning processes within organisations. This theme assumes if the causes of an incident are fully understood there is an opportunity to learn and improve the security of the organisation.

4.4. Challenges of implementing the lessons

Implementing the lessons identified from incidents pose significant challenges for organisations, as highlighted by the participants in the study. There was a notable variation among organisations in how they tracked the implementation of lessons and who was accountable for ensuring their execution. In mature and regulated industries (e.g. banking), there was a more rigorous reporting mechanism through senior risk committees to monitor the progress of implementing lessons [P5, P16, P20, P21, P33]. However, in other organisations, the accountability of the incident response team often ended once a post-incident report was issued, and actions were distributed across the organisation without further oversight. As one participant explained, "*They tend to be passed out and left locally to manage*" [P12]. Conversely, some organisations had centrally tracked and documented actions, and would continually chase responsible parties until remediation occurred. A participant described this approach as "*the non-automated nagware*" [P28]. It was acknowledged that broader improvement actions were not as effectively tracked as immediate fixes [P10].

Even with high-profile incidents, the interest and enthusiasm for implementing the identified fixes often fades over time. Participants pointed out that the energy and focus during an incident could wane once the situation was contained, and recovery efforts were underway. Also, individuals who were not directly involved in handling the incident might lack the same sense of urgency or momentum to address broader improvement actions. As one participant expressed, "*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*" [P10].

Fixing structural issues and making significant investments posed another challenge. There was a tendency within organisations to delay major system replacements or upgrades for as long as possible. However, participants recognised that this delay could lead to increased costs and exacerbate the problem. As one participant explained:

"*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*" [P32].

The difficulty of prioritising cyber investments was a common explanation given by participants for the failure to implement the lessons learned from incidents. Some organisations focused solely on investments with a direct return on investment (ROI) and, as a result, overlooked incidents as valuable learning opportunities. However, several participants saw incidents as a chance to secure funding for security initiatives, capitalising on the attention generated by the event. One participant stated, "*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*" [P14].

On the other hand, it was noted that budget allocation decisions were not always based on a comprehensive assessment of the incident's impact, but rather on individual experiences and perspectives within security teams. As one participant highlighted, "*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*" [P17]. Participants described a phenomenon where initially implemented lessons eroded over time as organisations slipped back into old behaviours or as the threat landscape evolved the security of systems degraded. This erosion emphasised the need for ongoing vigilance and adaptive responses to ensure sustained improvement [P30].

Furthermore, few organisations conducted systematic reviews or tests to evaluate the effectiveness of implemented lessons. The focus tended to be on meeting project deadlines and completing tasks rather than on assessing whether the underlying problem had been truly fixed. As one participant noted, "*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?*" [P6].

These challenges underscore the need for organisations to establish robust mechanisms for tracking the implementation of lessons, maintain momentum in addressing improvement actions, prioritise strategic investments, and conduct periodic evaluations to ensure the effectiveness of actions taken in response to incidents. A comprehensive and continuous approach to learning and improvement is essential to enhance cyber resilience in organisations.

5. Discussion

5.1. Organisations' current learning from cyber incidents

This study identified significantly more mature incident learning practices compared to earlier research, including studies by Jaatun et al. (2008, 2007, 2009), Line et al. (2006), Ahmad et al. (2012, 2015) and Bartnes et al. (2016). This shift could be attributed to the escalating volume of cyber attacks, their increased complexity and the growing adoption of normative processes since those earlier studies. Despite the diverse nature of industries, we found uniformity in the practices of learning from incidents, with the exception of more formalised action tracking in regulated businesses. This consistency across industries suggests a level of professionalisation among security practitioners and widespread adoption of normative processes, indicating isomorphic pressures.

The findings of our study provide support for the neo-institutional theory, which suggests that isomorphic pressures lead organisations to adopt similar practices without explicitly evaluating their effectiveness or applicability within their own context. Or as Alvesson and Spicer (2019) describe organisations adopting practices to "create an image of rationality" and "a sheen of legitimacy" rather than because they know the practices are effective. Rae and Provan (2019) discovered that post-incident reviews fulfil a significant social function by showcasing the organisation's commitment to addressing incidents seriously. This process provides a sense of comfort to individuals by making them familiar with the established procedures. Their research also highlighted how the reports and recommendations resulting from post-incident reviews tend to mirror the existing power dynamics within an organisation. In our study, participants similarly observed that recommendations were influenced by the attendees of review sessions, the allocation of budgets across different teams, and the prior experiences of the Chief Information Security Officer (CISO). Some participants noted that incidents were occasionally leveraged to support investments that were already desired within the organisation.

Our interview participants revealed that incident reports submitted by security teams to executives and risk committees are often accepted without thorough scrutiny of the organisational learning process by which lessons were derived. This finding aligns with the organisational defence mechanisms and paradoxes identified in organisational learning theory. Incident reports delivered to senior management are typically presented at a higher, more abstract level and are designed to rationally explain localised actions (Argyris, 1999). As per the organisational learning theory, senior leaders are motivated to ensure issues are addressed, yet their behaviour, coupled with the incomplete information provided in these reports, unintentionally fosters defensiveness within their teams. In response, team members tend to present single-loop actions, which they can be held accountable for delivering. 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.

Surprisingly, participants expressed strong concerns regarding the legal and regulatory ramifications associated with incident learning. Husák et al. (2023) also noted that GDPR regulations led to a decrease in organisations' willingness to share security data, despite the regulations permitting such sharing. This underscores how regulations can prompt organisations to exhibit excessive caution rather than investing additional effort to comprehensively grasp the specifics and identify compliant pathways for information sharing. These findings align to neo-institutional theory coercive pressures shaping learning practices. This unintended consequence arises from our society's increasing emphasis on holding organisations accountable for data protection and the interwoven dependencies in today's IT supply chains. While these efforts are intended to ensure accountability, they may inadvertently hinder the sharing of valuable lessons, impeding organisations from effectively learning and improving their data protection practices. We suggest that regulators explore a role in facilitating the exchange of information between companies, ensuring that shared knowledge does not result in fines or additional regulatory scrutiny. The multiple jurisdictions and multiple uncoordinated regulatory requirements increase

the coercive pressures, but do not necessarily improve the effectiveness of practices (Khan et al., 2022). Some government agencies have facilitated the sharing of threat intelligence, for example, the UK NCSC CISP[1] communities, but it is clear more still needs to be done.

Moreover, the concern regarding legal implications has not only limited the transparency of suppliers but also posed challenges for organisations in obtaining incident information from them, resulting in delays in assessing the impact of incidents. These issues align with the results of a study on the supply chain by Friday et al. (2021). They found the two incentives for making a profit and reducing the cost of services which were built into the legal contracts were unhelpful in a crisis. These incentives can work against the goal to restore services and learning from the incident as each party is focused on optimising only for their own short-term gain. Similar concerns about the lack of transparency in the supply chain were found by Jaatun and Tøndel (2015) in cloud computing and similarly in a study on the Capital One cyber security incident (Khan et al., 2022). To address these challenges, it is crucial to align commercial incentives with open sharing of incidents and near-misses. The recent guidance on securing the software supply chain by Enduring Security Framework (2022)[2] falls short in providing specific guidance beyond establishing an incident reporting and response initiative. Therefore, there is a need for governments and industry bodies to play a more active role in assisting organisations in building more resilient supply chains.

Participants emphasised the importance of fostering open communication with suppliers to enable proactive action and collaboration. However, participants also expressed the difficulty of sharing information before fully understanding the incident, reflecting the paradox of sharing information too soon or delaying for better quality (Ashraf et al., 2022). Nevertheless, participants called for the industry to mature in its ability to freely share incident lessons, with the understanding that early sharing, even with limited details, should be encouraged while acknowledging that a comprehensive view of an incident may take weeks to develop through a thorough investigation. Recent research on inter-organisational cyber security information sharing underscores the imperative for additional studies to comprehensively address the associated challenges (Albakri et al., 2018; Wagner et al., 2019; Zibak and Simpson, 2019).

All organisations in our study had mechanisms for classifying incidents, which aligns with the concept of normative pressures. However, there was variation in the classification systems used, and some participants mentioned deliberate deviations from standard classifications. This suggests a more conscious assessment of the effectiveness of their classification approaches which counteracts the isomorphic pressures. The lack of a widely accepted taxonomy for incidents may hinder the sharing of incident data and best practices among organisations. Establishing a widely accepted and standardised incident taxonomy would facilitate the ease of sharing information and improve collective incident learning efforts.

Participants also emphasised the challenges of quantifying cyber risk and ensuring that organisational leadership fully comprehends its implications. Yet, the World Economic Forum (2023) found some cyber security professionals were not able to articulate risks so they were understood and acted upon by senior leaders. 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). As a means to convey the seriousness of cyber risks and promote 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.

While organisations expressed keen interest in learning from incidents that occurred in other organisations, they acknowledged that such incidents did not receive the same priority or funding as if they had occurred internally. However, some participants provided examples where they had invested in security following incidents that had affected other organisations. This suggests that incidents occurring in peer organisations can serve as catalysts for organisations to allocate resources and enhance their security measures. This supports the mimetic pressures of neo-institutional theory.

In summary, our findings highlight the influence of isomorphic pressures on incident learning practices within organisations. Whilst this research did not seek to measure the comparative levels of these pressures, all three (i.e., normative, coercive and mimetic pressures) were found to play a role. Concerns regarding legal and regulatory ramifications, the need for aligned commercial incentives, variations in incident classification systems, the challenge of quantifying cyber risks, and the differential classification of incidents all shape the current state of incident learning. These also highlight the challenges organisations face in attempting to adopt organisational learning theory's double-loop learning approach. Addressing these challenges will require regulatory considerations, the development of standardised incident taxonomies, and a more comprehensive understanding of the dynamics driving incident learning practices within organisations.

5.2. Challenges to learning from cyber incidents

Our interviewees emphasised the importance of fostering an open attitude and encouraging the reporting of incidents within organisations. Security awareness training around reporting was an example of normative behaviour although some mandatory training was driven by regulatory – coercive pressures. This is aligned with Hielscher et al. (2023) findings. While many participants claimed that their organisations had a blame-free culture, none reported having assessed the veracity of this claim. A UK government cyber security breaches survey (2023) found post-incident reviews were seen as a way to engage with employees on the cyber security topic. Participants provided examples of employees who had fallen victim to phishing or other social engineering techniques and were subsequently viewed as victims rather than perpetrators of a crime. These individuals willingly shared their stories to encourage others to come forward and report incidents.

The participants' acknowledgment of the significance of fostering a blame-free culture resonates with prior research findings (Catino, 2008; Edmondson, 2018; Schilling and Kluge, 2009). In a study by Ballreich et al. (2023), it was emphasised that it is not only pivotal to establish a benevolent culture but also crucial for employees to comprehend the practicalities of defining an incident and the proper procedures for reporting it. This study, albeit limited in scale, underscores the necessity for further exploration to gain a comprehensive understanding of the perspectives of those asked to report cyber incidents. The challenges associated with transforming organisational culture have been extensively documented in organisational studies Alvesson and Spicer (2019) and warrant further study within the context of reporting cyber security incidents. Additionally, our participants drew attention to the hurdles related to investigating incident causes, including the identification of appropriate participants, selection of investigation methods, and the need to balance the investigation's depth and resources invested.

While previous research has explored ways to enhance cyber security incident investigations (Ahmad et al., 2012, 2015; Evans et al., 2019; He et al., 2014b, 2015) much of this research has primarily approached

[1] 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.

[2] The Enduring Security Framework (ESF) is a public-private partnership, cross-sector working group of the Critical Infrastructure Partnership Advisory Council (CIPAC) 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/.

cause analysis in a reductionist manner. This approach often reflects an engineering background and may not fully consider how causes are socially constructed within organisations. Edmondson (2023) insightfully suggests that while the concept of learning from incidents is perceived as rational, the complexities of actual work introduce emotions that can hinder the detachment needed for a clear, analytical review of incidents and the required actions. Further research is essential to identify not only the most effective tools and techniques for cause analysis but also the optimal approaches to conducting investigations.

The organisational learning theory of delving into the underlying causes of incidents, while invaluable, is time-consuming and frequently competes with other organisational priorities. Moreover, individuals, after enduring the emotional toll of an incident, may be reluctant to engage in detailed investigations to ascertain what went wrong. Organisations that have not assessed the effectiveness of their investigative approaches might find themselves either overinvesting or underinvesting in these efforts. Our participants noted that budget allocations often favoured investments known to the Chief Information Security Officer (CISO) rather than reflecting a thorough analysis of incident causes. Elliott and Macpherson (2010) also found the lessons identified can reflect the knowledge of those leading the investigation efforts or even a power struggle within an organisation. Manfield and Newey (2018) highlighted a tendency to rely on familiar practices rather than developing new ones. According to the organisational learning theory, individuals tend to feel more at ease recommending actions that address errors without questioning the governing variables.

Effective post-incident investigations require navigating organisational politics and addressing individual defensiveness, as highlighted by Argyris (1990). The unreliability of human memory, as noted by Tavris and Aronson (2020), further complicates the process by allowing individuals to self-justify their actions and rewrite their memories to align with positive self-perceptions. Petrie and Swanson (2018) posit that effective leaders facilitate their teams to think in a systems way but recognise the challenge where it is reported over 50% of the population in business tends to think in a reductionist way, which may not help people to understand causes in a complex IT ecosystem or determine ways to fix them. This poses challenges for honest self-reflection within organisations regarding the choices and decisions that contributed to incidents. In the context of double-loop learning, individuals must confront potentially embarrassing or threatening issues. However, to evade this, they inadvertently adopt defensive mechanisms that distort information about the underlying causes. The presence of ambiguity regarding systemic causes often makes them more challenging to resolve. Additionally, organisational norms tend to discourage open disagreements, limiting the scrutiny of interpretations related to events contributing to an incident (Argyris, 1999). NIST's Incident handling guide 800-61 R2 (Cichonski, 2012) suggests organisations use a skilled facilitator in the post-incident meetings.

Organisations must resist the temptation to conduct quick post-incident investigations that focus solely on implementing easy actions, such as updating a policy or providing user education. These actions may not adequately address the underlying factors that contributed to the incident as it is important to understand why people have not behaved in the expected secure manner (Demjaha et al., 2019; Kirlappos et al., 2014). A focus on controls can assume there is a single root cause, however, there are often multiple contributory causes. Researchers into how organisations learn from incidents have urged organisations to consider double-loop learning (Ahmad et al., 2012, 2020; Shedden et al., 2010, 2011). This type of learning goes beyond the immediate apparent facts of an incident to question the reasons and decisions behind them (Argyris, 1994).

Even if organisations conduct thorough investigations to identify significant lessons, the effectiveness of these lessons hinges on taking action to address them. NIST (Cichonski, 2012) and other industy guidance assumes once lessons are captured, corrective actions will be implemented. In cases when lessons and owners were agreed upon, organisations still reported difficulties in ensuring that the necessary actions are implemented. Elliott and Macpherson (2010) emphasised the difference between lessons being identified and translating these into changes in practices. Edmondson (2002) highlighted this distinction between having the "look" of reflective learning, but not actually taking action to make a change. Additionally, Manfield and Newey (2018) found leaders possessed a "bounded rationality" which limited their motivation to embed lessons, particularly in organisations where a lot of change was already happening.

Many participants expressed concerns about the complexity of their IT environments and the ongoing drive to digitise their businesses for improved efficiency. New technical developments such as generative Artifical Intelligence (AI) and Internet of Things (IOT) increase the scope of what needs to be protected and poses challenges in addressing structural causes. Shifting toward a "secure by design" approach is ideal, but many organisations still rely on legacy systems, and the ever-evolving nature of cyber security makes it difficult to anticipate all potential security threats during system development and integration into the organisation's expanding IT infrastructure. Opportunities may arise to leverage these new technologies for action implementation. For instance, McIntosh et al. (2023) found that, in certain contexts, AI Generative Pre-trained Transformers (GPTs) generated policies surpassed human-generated ones and could also enhance the employee training experience.

Practitioners believed their senior leaders did not fully understand the cyber security risks and the investments needed. This is aligned with recent research by the World Economic Forum (2023) which found organisations struggled to have leaders agree on the actions needed to address cyber risks. Many participants raised the challenge of prioritising cyber security investments particularly when it is hard to demonstrate a ROI. However, they noted they experienced extra investment following a significant incident. This finding is consistent with the research conducted by Demjaha et al. (2019) which revealed that incidents can prompt a surge in investment. However, they also noted that some of these investments may be directed towards "security theatre" measures which prioritise giving the perception of security rather than necessarily actually improving it. Moore et al. (2016) also identified compliance as a key driver for budget allocation in cyber security. This underscores the influence of coercive pressures on cyber security practices. Nevertheless, one of the major constraints reported in their study was the scarcity of skilled cyber security resources available. Organisational learning theory underscores the significance of the ability to learn about the process of learning (Drupsteen, 2014). Moreover, although few participants reported suffering repeated similar incidents, only a limited number of organisations assessed whether the actions they had taken had actually made the anticipated difference in addressing the contributing factors identified during the investigations. These challenges highlight the need for stronger follow-up of action implementation and a review of the effectiveness to ensure lessons lead to improvements in security.

Our study aligns with institutional theory, demonstrating that practices are influenced by isomorphic pressures rather than organisations' assessments of their efficacy. It also highlights various challenges associated with the adoption of effective organisational learning practices. These challenges encompass the need to cultivate a blame-free culture, conduct rigorous casual investigations, address organisational politics and defensiveness, avoid superficial post-incident actions, and ensure the effective implementation and evaluation of corrective measures. Addressing these challenges requires further research, the development of supportive organisational cultures, and a focus on proactive cyber security practices that consider the complexities of their IT ecosystems and the evolving threat landscape.

5.3. Practical implications

This research highlights significant opportunities for organisations to

enhance the benefits derived from incident learning. Table 2 presents the practical implications associated with our findings and offers recommendations based on the themes created. The recommendations outlined in this study are tailored for implementation by security practitioners operating within larger organisations that frequently encounter security incidents. Formulation of these recommendations was rooted in the empirical evidence collected from practitioner interviews, which delved into the challenges faced by organisations and their implications on the effectiveness of learning practices. Through the rich dataset derived from these interviews, specific practices adopted by some organisations to address identified challenges were extrapolated. Moreover, practitioners were probed about factors that could enhance incident learning, and these insights were rigorously evaluated and incorporated into the preliminary recommendations.

To augment these findings, a comprehensive review of the research literature was conducted to identify analogous challenges and corresponding recommendations. The study also sought evidence illustrating successful approaches adopted by organisations facing similar challenges. Subsequently, the feasibility of applying these recommendations to the realm of cyber security was carefully assessed. The recommendations were iteratively refined to ensure comprehensive coverage of the identified challenges.

First and foremost, organisations should explicitly assess the effectiveness of their current learning practices by taking time to reflect on what is working well and where learning practices can be fine-tuned for greater efficacy. Executives should ensure the strengths and weaknesses of their learning processes is understood and enable organisations to make targeted improvements.

Secondly, the organisations we studied expressed concerns about not being fully informed about incidents, particularly within their supply chains. This echos the findings of the World Economic Forum security outlook 2023, which reported 90% of respondents reported concerns about the cyber resilience of the third parties they relied upon. The challenges related to regulators and litigation are complex and not immediately solvable. However, there are opportunities to foster a culture of greater openness within organisations and across industries. For example, some participants [P12, P30] cited the aviation industry as one that embraces a culture of openness and information sharing.

Thirdly, when incidents are investigated, it is crucial for organisations to carefully consider 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. Elliott and Macpherson (2010) found organisations needed diverse teams to identify lessons as people's prior experience constrained the actions they could imagine. Depending on the organisation's culture, size, and nature, different causal analysis techniques may be appropriate. Leaders need to enable iterative learning and experimentation to address complex issues (Argyris, 1994). However, it is important to make a conscious choice regarding the most effective technique for the organisation and the specific incident. Employing these techniques can facilitate structured discussions that delve deeper into the underlying factors contributing to an incident beyond its immediate cause.

Fourthly, it is important to recognise that knowledge of a lesson, alone, does not protect an organisation. Cyber resilience is enhanced only when actions are taken to address the contributing factors. Organisations may have different governance structures and methods for tracking progress on actions, but it is vital to follow up and ensure that the necessary actions are implemented. 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 allocation of resources, prioritisation, and recognition, to enable their organisations to make progress on these demanding changes.

In conclusion, this study provides practical implications for organisations seeking to enhance their learning from cyber incidents. Table 2 summarises the themes, the associated potential implications and our practical recommendations. 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, accompanied by strong leadership and a commitment to ongoing improvement, can contribute to a more robust and proactive approach to cyber security.

Table 2
Theoretical and practical contributions of the study.

Themes	Associated potential implications	Practical recommendations
Isomorphic pressures on organisational learning practices	An organisation's practices for learning from incidents can become mere rituals, that are shaped by the requirements of standards, executives and security professionals, with limited evaluation of their efficacy	• Evaluate the effectiveness of the learning process • Build evaluation into the process
Challenges of uncovering incidents	Opportunities to learn are missed if incidents or lucky near misses are not reported within and shared between organisations	• Demonstrate an openness to hearing about incidents • Promote knowledge sharing with peers and supply chain
Challenges of identifying the causes	If investigations are superficial and only focused on technology causes, with limited participation, this constrains the possible lessons which can be identified	• Ensure effective participation in post-incident reviews • Delve into underlying causes and trends
Challenges of implementing the lessons	Sustainable changes to structural cyber security are not achieved, leaving organisations vulnerable to incidents with similar contributory causes	• Champion addressing structural causes • Drive the implementation of lessons and testing

5.4. Limitations and future research

While this study provides valuable insights into learning from cyber incidents, there are several limitations that should be acknowledged. First, qualitative research, although valuable in gaining a deep understanding of people's experiences and explanations, has limited generalisability. As researchers, we are inextricably part of the world in which we seek to understand (Pilgrim, 2014) and the themes we have identified reflect our own experiences, therefore, other researchers may interpret the data differently (Braun and Clarke, 2022). The sample size of 34 practitioners interviewed in this study falls within the normal range for qualitative research. However, it may not be statistically representative of the entire population of organisations. The sampling approach, relying on professional networks and snowballing, introduces the possibility of skewing the participant pool, which is an acknowledged limitation of our sampling method.

Additionally, the voluntary participation of interviewees introduces the risk of self-selection bias, as those with a strong interest in the topic may be more likely to participate. Participants may also present themselves positively due to social desirability bias, particularly when being interviewed as "leaders". There is also a risk participants are sharing their "espoused theory of action" which is how they intellectually perceive their actions which may be different during the stress of a major incident (Argyris, 1994). To mitigate these biases, techniques such as indirect questioning, providing assurances, and seeking more information or examples were employed in the interview approach. Nevertheless, it is important to recognise that the information shared in the interviews reflects the social construction of the interviewees rather than an independent existence of phenomena. The reliance on

participant accounts without independent verification is a limitation of this research, as only one participant from each organisation was interviewed.

Secondly, this study focuses solely on the perspective of security practitioners, neglecting the viewpoints of other stakeholders within organisations regarding the security function's ability to learn from incidents. While this research aimed to capture the perspectives of security practitioners across various organisations for broader applicability, future research could include a representative sample of individuals outside the security function in fewer organisations to gain a deeper understanding of the perceptions of organisational learning by different groups.

Thirdly, this study sought participants from a UK-based network, which could impact the transferability of findings, although the majority of the organisations are multi-national and most of the participants have an international remit. Further research is necessary to explore whether the findings apply to other countries or legal contexts. Although a range of industries was purposively sampled, only a few organisations were included from each sector and the study focused on larger organisations. Conducting additional research to determine potential variations across sectors and covering smaller entities, such as owner manged businesses or small public bodies would be beneficial. Moreover, this study represents a snapshot in time and may not capture the evolving nature of organisations. As the cyber security landscape rapidly changes, the research findings can become outdated as organisations adapt. Longitudinal studies involving data collection from multiple organisations over an extended period of time would provide a more comprehensive understanding of organisational learning. Additionally, further studies are needed to improve investigations into underlying contributing causes and explore the social and political influences on the learning process. Potentially ethnographic studies in organisations which are conducting learning from incidents would provide interesting insights. This research emphasises isomorphic pressures on learning from incidents, and the challenges of implementing deeper casual analysis. Further in-depth studies are required to evaluate the effectiveness of organisational learning practices and assess the value of investments in learning from incidents activities.

6. Conclusion

This research illuminates the challenges organisations face in effectively learning from cyber incidents and highlights the crucial need for conscious evaluation of learning practices. The isomorphic pressures identified in this study align with the neo-institutional theory, emphasising the importance of examining the factors influencing learning from incidents. The interviewees explained the challenges they face in conducting the double-loop learning prescribed in the organisational learning theory. Our study represents one of the initial endeavours to understand these challenges comprehensively.

Organisations must assess whether they are effectively learning from all incidents, fostering psychological safety for incident reporting, and cultivating relationships to facilitate collective learning across their supply chains. Incident classification plays a pivotal role in determining which incidents are selected for learning. While some organisations have begun to leverage opportunities for broader learning, such as peer collaboration and simulation exercises, these could be pursued due to mimetic pressures to copy others rather than driven by an assessment of their own learning capability. Many of the participants expressed a strong desire to expand the analysis of lower-level incidents and near-misses to uncover underlying themes and address systemic issues.

Recognising the need to include more diverse viewpoints in the learning process, organisations should strive to engage with different teams during post-incident reviews. The inclusion of a wider range of perspectives can enrich the identification of contributory causes and generate impactful lessons that resonate throughout the organisation. Further research is required to explore the value of diverse participation, as engagement in learning activities must be balanced with other organisational priorities.

Organisations often find themselves caught in the inertia of the status quo, impeding their ability to challenge existing paradigms and delve into the underlying causes of incidents. To overcome this reluctance, leaders must foster an environment that empowers individuals to challenge existing practices and identify potentially radical actions to enhance their security posture. Our study uncovers contexts in which participants acknowledged the risk of overlooking causes and evading the most onerous lessons. Overcoming defensiveness emerged as a significant obstacle, as individuals may hesitate to identify issues for fear of being held solely responsible for their resolution. To address this challenge, organisations should consider employing causal analysis tools and trained facilitators to uncover systemic causes and engender a more proactive learning culture. Nevertheless, as Meyer and Rowan (1977) noted, the use of external consultants can sometimes serve to enhance the perceived legitimacy of a process rather than directly contributing value.

Importantly, our study highlights the imperative for organisations to move beyond merely treating the symptoms of incidents and conducting superficial reviews. Instead, they should strive to identify and implement lessons that yield substantial and meaningful improvements to their security posture. Although we observed increased learning from incidents compared to previous research, there are still ample opportunities for improvement. To harness the full benefits of incident learning, we offer a series of practical recommendations aimed at maximising the benefit that organisations derive from their incidents.

In conclusion, this research underscores the necessity for organisations to evaluate the effectiveness of their learning practices and proactively address the challenges associated with incident learning. By doing so, organisations can enhance their cyber resilience, foster a culture of continuous improvement, and effectively respond to the evolving cyber security landscape. The findings and recommendations presented in this study contribute to the growing body of knowledge on applying the neo-institutional theory and the organisational learning theory in the cyber security field and serve as a foundation for further research and practical implementation.

CRediT authorship contribution statement

Clare M. Patterson: Conceptualization, Investigation, Methodology, Writing – original draft, Writing – review & editing. **Jason R.C. Nurse:** Methodology, Supervision, Writing – review & editing. **Virginia N.L. Franqueira:** Supervision, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The data that has been used is confidential.

Acknowledgments

The authors would like to thank the interviewees for their participation in this study and the reviewers for their feedback.

Appendix A – Participant information

#	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 1000 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 B – Interview protocol

Interview protocol		
Study: organisational learning from cyber security incidents		
Date:	Time:	Location:
Interview type (virtual / F2F):		
Researcher:		
Interviewee:		
Name (pseudonym):	Organisation (pseudonym):	Role:

(*continued on next page*)

(*continued*)

Interview protocol		
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?
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 learnt? Who are these outputs shared with (internally and externally)?
Current practice intervention	How does your organisation plan interventions based on what is learnt 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?
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 (eg 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 C – Codebook

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
CHALLENGE OF IDENTIFYING THE CAUSES	Challenges of reporting from OT environments
	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 D – Industry standards and guidance

Organisations	Learning phase	Guidance given in the document
CREST Cyber Security Incident Response Guide	Follow up	Encourages organisations to use incidents to improve incident response and overall cyber security posture and involve relevant parties. It recommends organisations conduct thorough investigations, report the incident to stakeholders, carry out a post incident review, communicate, build on lessons learnt, and update key information controls and documents.
Information Systems Audit and Control Association (ISACA) Security Incident Management Audit Program (ISACA, 2020)	Lessons learned	Suggests internal auditors assess the enterprise's lessons learned protocol to check it includes all stakeholders involved or affected by the incident, procedural deficiencies are documented, and lessons learned are documented to be used in future tabletop exercises to prevent similar incidents and improve incident response times.
International Standards Organisation / International Electrotechnical Commission ISO - ISO/IEC 27035-2:2023 - Information Technology. Information Security Incident Management. Part 2: Guidelines to Plan and Prepare for Incident Response (The British Standards Institution, 2023)	Lessons learned	Recommends organisations identify and learn lessons, ensuring these are acted upon. These lessons could include improving incident response, security controls, security risk assessment and management, and other areas which can streamline operations. It recommends the identified areas for improvement should be fed into the organisation's information security incident management plan and a summary analysis of incidents should be produced at the organisation's management information security forum.
NIST.SP.800-61r2 Computer Security Incident Handling Guide (Cichonski, 2012)	Post-incident activity	Guides organisations to conduct a lessons learned session involving all relevant parties following a major incident, and periodically after minor incidents as resources allow and possibly address multiple incidents within a single lessons-learned meeting. In these meetings organisations should examine the incident details, the effectiveness of the response and what corrective actions can prevent similar incidents in the future. It also suggests a skilled facilitator can be valuable in these meetings and organisations should generate a follow-up report to help with training team members and responding to similar incidents.
National Cyber Security Centre (NCSC) UK Cyber Assessment Framework (CAF) guidance, D.2 Lessons learned (NCSC, 2019)	Lessons learned	Guides organisations to learn lessons as to why the incident happened and prevent the issue from reoccurring. It suggests organisations solve underlying causes and gives the example of going beyond merely applying the missing patch, but also addressing the overall patch management process. Lessons should be documented and fed into protective security as well as the incident response plans. These lessons should be shared with all relevant stakeholders and organisations such as the NCSC who can provide insights on trends.
SysAdmin, Audit, Network, and Security (SANS) Incident handlers handbook (Kral, 2012)	Lessons learned	Recommends conducting the lessons learned meeting with the incident team, suggesting organisations discuss and document the who, what, where, why, and how phases of the incident response process. This documentation can serve as valuable training material for onboarding new team members and should encapsulate insights on enhancing overall team effectiveness in future incidents.

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. J. Assoc. Inf. Sci. Technol. 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. Comput. Secur. 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. Int. J. Inf. Manag. 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. University of Oxford.

Albakri, A., Boiten, E., De Lemos, R., 2018. Risks of sharing cyber incident information. In: 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. Electron. J. Inform. Syst. Dev. Ctries. 88 (5) https://doi.org/10.1002/isd2.12223.

Alvesson, M., Spicer, A., 2019. Neo-institutional theory and organization studies: a mid-life crisis? Organ. Stud. 40 (2), 199–218. https://doi.org/10.1177/0170840618772610.

Argote, L., 2013. Organizational Learning, 2nd ed. Springer US. https://doi.org/10.1007/978-1-4614-5251-5.

Argote, L., Ophir, R., 2017. Intraorganizational learning. The Blackwell Companion to Organizations. Blackwell Publishing Ltd, pp. 181–207. 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. Adm. Sci. Q. 21 (3), 363–375. https://doi.org/10.2307/2391848.

Argyris, C., 1994. Chris Argyris Harvard business review good communication that blocks learning. Harv. Bus. Rev. 72 (4), 77–85.

Argyris, C., Schön, D.A., 1978. Organizational Learning II: Theory, Method, and Practice. Addison-Wesley Publishing Company.

Ashraf, M., Jiang, J.X., Wang, I.Y., 2022. Are there trade-offs with mandating timely disclosure of cybersecurity incidents? Evidence from state-level data breach disclosure laws. J. Financ. Data Sci. 8, 202–213. https://doi.org/10.1016/j.jfds.2022.08.001.

Ballreich, F.L., Volkamer, M., Müllmann, D., Berens, B.M., Häußler, E.M., Renaud, K.V., 2023. Encouraging organisational information security incident reporting. In: Proceedings of the 2023 European Symposium on Usable Security, pp. 224–236. https://doi.org/10.1145/3617072.3617098.

Bartnes, M., Moe, N.B., Heegaard, P.E., 2016. The future of information security incident management training: a case study of electrical power companies. Comput. Secur. 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. Comput. Secur. 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. Inf. Manag. 51 (1), 138–151. https://doi.org/10.1016/j.im.2013.11.004.

Boin, A., McConnell, A., Hart, P.T., 2008. Governing After Crisis: The Politics of Investigation, Accountability and Learning. Cambridge University Press.

Braun, V., Clarke, V., 2006. Using thematic analysis in psychology. Qual. Res. Psychol. 3 (2), 77–101. https://doi.org/10.1191/1478088706qp063oa.

Braun, V., Clarke, V., Maher, A., Carter, E., 2022. Thematic Analysis: A Practical Guide. SAGE Publications Asia-Pacific Pte Ltd.

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. J. Res. Nurs. 8, 652–661. https://doi.org/10.1177/1744987120927206.

Catino, M., 2008. A review of literature: individual blame vs. organizational function logics in accident analysis. J. Contingencies Crisis Manag. 16 (1), 53–62.

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. Inform. Manag. 52 (4), 385–400. https://doi.org/10.1016/j.im.2014.12.004.

Check Point Research Team. (2022, January 10). Check point research: cyber attacks increased 50% year over year. https://blog.checkpoint.com/security/check-point-research-cyber-attacks-increased-50-year-over-year/#:~:text=This%20trend%20reached%20an%20all,corporate%20networks%20compared%20to%202020.

Cichonski, p. (2012). Computer security incident handling guide (national institute of standards and technology). In Special Publication (NIST SP) - 800-61 Rev 2. https://doi.org/10.6028/NIST.SP.800-61r2.
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.
Crossan, M.M., Lane, H.W., White, R.E., 1999. An organizational learning framework: from intuition to institution. Acad. Manag. Rev. 24 (3), 522–537. https://doi.org/10.2307/259140.
CrowdStrike. (2023). 2023 Global Threat Report. www.crowdstrike.com.
Cyert, R.M., March, J.G., 1963. A Behavioral Theory of the Firm, 2nd ed. Englewood Cliffs.
De Reuver, M., Sørensen, C., & Basole, R.C. (2017). The digital platform: a research agenda. https://doi.org/10.1057/s41265.
Demjaha, A., Caulfield, T., Sasse, M.A., Pym, D., 2019. 2 fast 2 secure: a case study of post-breach security changes. In: Proceedings of the 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 192–201. https://publications.parliament.uk/pa/cm201617/cmselect/cmcumeds/148/.
Dimaggio, P.J., Powell, W.W., 1983. The iron cage revisited: institutional isomorphism and collective rationality in organizational fields. Am. Sociol. Rev. 48 (April), 147–160. https://doi.org/10.2307/j.ctv1f886rp.7.
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.
Easterby-Smith, M., Lyles, M.A., 2012. Handbook of Organizational Learning and Knowledge Management, 2nd ed. John Wiley & Sons Ltd.
Edmondson, A., 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. Organ. Sci. 13 (2), 128–146. https://doi.org/10.1287/orsc.13.2.128.530.
Edmondson, A.C., 2018. The Fearless Organization: Creating Psychological Safety in the Workplace for Learning, Innovation, and Growth. John Wiley & Sons.
Elliott, D., Macpherson, A., 2010. Policy and practice: recursive learning from crisis. Group Organ. Manag. 35 (5), 572–605. https://doi.org/10.1177/1059601110383406.
Enduring Security Framework. (2022). Securing the software supply chain-Recommended practices guide for customers.
Evans, M., He, Y., Maglaras, L., Janicke, H., 2019. HEART-IS: a novel technique for evaluating human error-related information security incidents. Comput. Secur. 80, 74–89. https://doi.org/10.1016/j.cose.2018.09.002.
FBI's Internet Crime Complaint Center (IC3), 2022. Federal Bureau of Investigation Internet Crime Report.www.ic3.gov
Fiol, C.M., Lyles, M.A., 1985. Organizational learning. Acad. Manag. Rev. 10 (4), 803–813. https://www.jstor.org/stable/258048?seq=1&cid=pdf.
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. J. Humanit. Logist. Supply Chain Manag. 11 (2), 248–271. https://doi.org/10.1108/JHLSCM-07-2020-0061.
Gale, M., Bongiovanni, I., Slapnicar, S., 2022. Governing cybersecurity from the boardroom: challenges, drivers, and ways ahead. Comput. Secur. 121, 102840 https://doi.org/10.1016/j.cose.2022.102840.
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/10.1007/11563228_28.
Grispos, G., 2016. On The Enhancement of Data Quality in Security Incident Response Investigations. University of Glasgow.
Grispos, G., Glisson, W.B., Storer, T., 2017. Enhancing security incident response follow-up efforts with lightweight agile retrospectives. Digital Investig. 22, 62–73. 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/10.24251/hicss.2019.859.
Hasan, S., Ali, M., Kurnia, S., Thurasamy, R., 2021. Evaluating the cyber security readiness of organizations and its influence on performance. J. Inf. Secur. Appl. 58 https://doi.org/10.1016/j.jisa.2020.102726.
He, Y., Johnson, C., 2015. Improving the redistribution of the security lessons in healthcare: an evaluation of the generic security template. Int. J. Med. Inform. 84 (11), 941–949. 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. Inform. Health Soc. Care 42 (4), 393–408. https://doi.org/10.1080/17538157.2016.1255629.
He, Y., Johnson, C., Evangelopoulou, M., Lin, Z.-S., 2014a. Diagraming approach to structure the security lessons: evaluation using cognitive dimensions. In: Proceedings of the International Conference on Trust and Trustworthy Computing. Cham. Springer. https://doi.org/10.1007/978-3-319-08593-7_19.
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. J. Trust Manag. 2 (1) https://doi.org/10.1186/s40493-015-0016-2.
He, Y., Johnson, C., Renaud, K., Lu, Y., Jebriel, S., 2014b. An empirical study on the use of the generic security template for structuring the lessons from information security incidents. In: Proceedings of the 2014 6th International Conference on Computer Science and Information Technology, CSIT 2014 - Proceedings, pp. 178–188. https://doi.org/10.1109/CSIT.2014.6805998.
He, Y., Johnson, C.W., 2012. Generic security cases for information system security in healthcare systems. In: Proceedings of the IET Conference Publications, 2012(607 CP). https://doi.org/10.1049/cp.2012.1507.
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. In: Proceedings of the 32st USENIX Security Symposium. https://www.forbes.com/sites/bobzukis/2022/04/18/the-sec.
Hove, C., Tårnes, M., Line, M., 2014. Information Security Incident Management an Empirical Study of Current Practice. Norwegian University of Science and Technology.
Hu, Q., Hart, P., Cooke, D., 2007. The role of external and internal influences on information systems security - a neo-institutional perspective. J. Strat. Inf. Syst. 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. Organ. Sci. 2 (1), 88–115. https://www.jstor.org/stable/2634941.
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 Res. Pract. https://doi.org/10.1145/3611391.
Hüsch, P., & Sullivan, J. (2023). Global approaches to cyber policy, legislation and regulation: a comparative overview. https://www.isc2.org/.
ISACA. (2020). Security incident management audit program. ISACA ®. https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KoDPEA0.
ITIL - IT Infrastructure Library - United Kingdom|IBM. (n.d.). Retrieved February 1, 2022, from https://www.ibm.com/uk-en/cloud/learn/it-infrastructure-library.
Jaatun, M., 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. Int. J. Critical Infrastruct. Prot. 2 (1–2), 26–37. https://doi.org/10.1016/j.ijcip.2009.02.004.
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?. In: Proceedings of the 10th International Conference on Availability, Reliability and Security, ARES 2015, pp. 467–473. https://doi.org/10.1109/ARES.2015.38.
Jeyaraj, A., Zadeh, A., 2020. Institutional isomorphism in organizational cybersecurity: a text analytics approach. J. Organ. Comput. Electron. Commer. 30 (4), 361–380. https://doi.org/10.1080/10919392.2020.1776033.
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.
Khan, N.F., Yaqoob, A., Khan, M.S., Ikram, N., 2022. The cybersecurity behavioral research: a tertiary study. Comput. Secur. 120, 102826 https://doi.org/10.1016/j.cose.2022.102826.
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.
Kral, P. (2012). SANS Incident Handlers Handbook 2012. https://www.sans.org/white-papers/33901/.
Line, M.B., Albrechtsen, E., 2016. Examining the suitability of industrial safety management approaches for information security incident management. Inform. Comput. Secur. 24 (1), 20–37. https://doi.org/10.1108/ICS-01-2015-0003.
Line, M.B., Albrechtsen, E., Jaatun, M.G., Tøndel, I.A., Johnsen, S.O., Longva, O.H., Wærø, I., 2009. A structured approach to incident response management in the oil and gas industry. In: Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 5508 LNCS, pp. 235–246. https://doi.org/10.1007/978-3-642-03552-4_21.
Line, M.B., Albrechtsen, E., Johnsen, S.O., Longva, O.H., Hillen, S., 2006. Monitoring of incident response management performance. In: Proceedings of the International Conference on IT-Incident Management & IT-Forensics. https://dblp.org/db/conf/imf/imf2006.html.
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. Saf. Sci. 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 Anal. Prev. 42 (6), 2132–2139. https://doi.org/10.1016/J.AAP.2010.07.003.
Manfield, R.C., Newey, L.R., 2018. Resilience as an entrepreneurial capability: integrating insights from a cross-disciplinary comparison. Int. J. Entrep. Behav. Res. 24 (7), 1155–1180. https://doi.org/10.1108/IJEBR-11-2016-0368.
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. Comput. Secur. 134, 103424 https://doi.org/10.1016/j.cose.2023.103424.
Meyer, J.W., Rowan, B., 1977. Institutionalized organizations: formal structure as myth and ceremony. Am. J. Sociol. 83 (2), 340–363. https://about.jstor.org/terms.
Miranda, P.J., 2020. Workplace Learning for Efficiency and Effectiveness in Not-for-Profit Organisations. Monash University.
Moore, T., Dynes, S., Chang, F.R., 2016. Identifying how firms manage cybersecurity investment. In: Proceedings of the Workshop on the Economics of Information Security (WEIS),, pp. 1–27.
Morgan, S. (2023, May 24). 2023 Cybersecurity Almanac: 100 Facts, Figures, Predictions, and Statistics. Cybercrime Magazine. https://cybersecurityventures.com/cybersecurity-almanac-2023/.

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. Comput. Secur. 128 https://doi.org/10.1016/j.cose.2023.103162.
NCSC CAF guidance - D.2 Lessons learned. Version 3.0. (2019). https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/d-2-lessons-learned.
NCSC. (2022a). Cyber security longitudinal survey wave 1. https://www.gov.uk/government/publications/cyber-security-longitudinal-survey-wave-one/cyber-security-longitudinal-survey-wave-1.
NCSC. (2022b). NCSC annual review 2022. Annual Review. https://www.ncsc.gov.uk/collection/annual-review-2022/threats-risks-and-vulnerabilities/state-threats.
Nese, A., 2018. Improving Security Posture By Learning from Intrusions. Norwegian University of Science and Technology.
Niekerk, J.V., von Solms, R., 2004. Organisational learning models for information security. In: Proceedings of the ISSA 2004 Enabling Tomorrow Conference, 30. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.106.4619&rep=rep1&type=pdf.
NIST. (2018). Risk management framework for information systems and organizations: https://doi.org/10.6028/NIST.SP.800-37r2.
NIST Computer Security Resource Center CSRC. (n.d.). NIST glossary. Glossary. Retrieved February 25, 2022, from https://csrc.nist.gov/glossary/term/incident.
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.
O'Reilly, M., Parker, N., 2013. Unsatisfactory saturation": a critical exploration of the notion of saturated sample sizes in qualitative research. Qual. Res. 13 (2), 190–197. https://doi.org/10.1177/1468794112446106.
Patterson, C.M., Nurse, J.R.C., Franqueira, V.N.L., 2023. Learning from cyber security incidents: a systematic review and future research agenda. Comput. Secur. 132, 103309 https://doi.org/10.1016/j.cose.2023.103309.
Paulus, T.M., 2021. Doing Qualitative Research in a Digital World. SAGE.
Petrie, D.A., Swanson, R.C., 2018. The mental demands of leadership in complex adaptive systems. Healthc. Manag. Forum 31 (5), 206–213. https://doi.org/10.1177/0840470418778051.
Pilgrim, D., 2014. Some implications of critical realism for mental health research. Social Theory Health 12 (1), 1–21. https://doi.org/10.1057/sth.2013.17.
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. Saf. Sci. 111, 119–127. https://doi.org/10.1016/j.ssci.2018.07.001.
Rządca, R., Strumińska-Kutra, M., 2016. Local governance and learning: in search of a conceptual framework. Local Gov. Stud. 42 (6), 916–937. https://doi.org/10.1080/03003930.2016.1223632.
Sarbanes-oxley act of 2002. In The public company accounting reform and investor protection act, Pub. L. No. 55, Washington DC: US Congress (2002). https://sarbanes-oxley-act.com/.
Schilling, J., Kluge, A., 2009. Barriers to organizational learning: an integration of theory and research. Int. J. Manag. Rev. 11 (3), 337–360. https://doi.org/10.1111/J.1468-2370.2008.00242.X.
Senge, P.M., 2010. The Fifth Discipline: The Art and Practice of the Learning Organization (Century business), 2nd, Kindle Edition. Random House Business Books.
Shedden, P., Ahmad, A., Ruighaver, A.B., 2010. Organisational learning and incident response: promoting effective learning through the incident response process. In: 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.
Shortell, S.M., 2016. Applying organization theory to understanding the adoption and implementation of accountable care organizations: commentary. In: Medical Care Research and Review, 73. SAGE Publications Inc, pp. 694–702. https://doi.org/10.1177/1077558716643477.
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.
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 British Standards Institution. (2023). BS ISO/IEC 270352:2023 - Information security incident management. Part 2: guidelines to plan and prepare for incident response. In The British Standards Institution. BSI Standards Limited 2023. https://bsol.bsigroup.com/Search/Search?searchKey=bs+iso%2Fiec+27035-2%3A2023&OriginPage=Header+Search+Box&autoSuggestion=true.
Tøndel, I.A., Line, M.B., Jaatun, M.G., 2014. Information security incident management: current practice as reported in the literature. Comput. Secur. 45, 42–57. https://doi.org/10.1016/J.COSE.2014.05.003.
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.
Van der Kleij, R., Kleinhuis, G., Young, H., 2017. Computer security incident response team effectiveness: a needs assessment. Front. Psychol. 8 (DEC) https://doi.org/10.3389/fpsyg.2017.02179.
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. Comput. Secur. 87 https://doi.org/10.1016/j.cose.2019.101589.
Wiik, J., Kossakowski, K.-P., 2005. Dynamics of incident response. In: Proceedings of the 17th Annual FIRST Conference on Computer Security Incident Handling. Singapore. www.cert.org.
Willig, C., 2022. Introducing Qualitative Research in Psychology : Adventures in Theory and Method, 4e. Open University Press. https://www.mheducation.co.uk/professionals/open-university-press/olc/willig-qualitative-research.
World Economic Forum (in collaboration with Accenture), 2023. Global Cybersecurity Outlook 2023.
Zibak, A., Simpson, A., 2019. Cyber threat information sharing: perceived benefits and barriers. In: Proceedings of the ACM International Conference Proceeding Series. https://doi.org/10.1145/3339252.3340528.

Clare M. Patterson is a research student in cyber security in the School of Computing at the University of Kent, UK. She received her MSc degree in information security from Royal Holloway University of London, UK in 1999. Her research interests include incident management, security transformation initiatives and security leadership. Clare also has over 25 years of experience in industry across IT and cyber security project management and leadership roles.

Jason R. C. Nurse is a Reader in Cyber Security in the Institute of Cyber Security for Society (iCSS) & School of Computing at the University of Kent, UK. He also holds the roles of Visiting Fellow in Defence & Security at Cranfield University, UK and Associate Fellow at the Royal United Services Institute for Defence and Security Studies (RUSI). He received his PhD from the University of Warwick, UK. His research interests include cyber resilience, security risk management, security culture, cyber insurance, corporate communications and cyber security, and insider threat. Jason was selected as a Rising Star for his research into cybersecurity, as a part of the UK's Engineering and Physical Sciences Research Council's Recognising Inspirational Scientists and Engineers (RISE) awards campaign. Dr Nurse has published over 100 peer-reviewed articles in internationally recognised security journals and conferences, and he is a professional member of the British Computing Society.

Virginia N. L. Franqueira is an Associate Professor in Cyber Security in the Institute of Cyber Security for Society (iCSS) & School of Computing at the University of Kent, UK. She received her M.Sc. from the Federal University of Espirito Santo (Brazil), and her Ph.D. from the University of Twente (the Netherlands). She has around 60 publications and her research interests include digital forensics, studies related to cybercrime and interpersonal crimes (e.g., cyberstalking and domestic abuse), connected vehicles, critical infrastructure security, cyber security education and protection against online harm for children. She is a Fellow of The Higher Education Academy.