Computers & Security 132 (2023) 103309

Contents lists available at ScienceDirect

Computers & Security

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

Learning from cyber security incidents: A systematic review and future research agenda

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

University of Kent, Kent, Canterbury CT2 7NZ, UK

ARTICLE INFO

Article history:
Received 19 December 2022
Revised 22 March 2023
Accepted 24 May 2023
Available online 28 May 2023

Keywords:
Cyber security
Incident investigation
Incident response
Lessons learned
Learning process
Organisational learning
Post-incident review
Security incident
Systematic literature review
Research agenda

ABSTRACT

Cyber security incidents are now prevalent in many organisations. Arguably, those who can learn from security incidents and address the underlying causes will reduce the prevalence of similar ones in the future. This research provides a new examination of how organisations learn from incidents by systematically reviewing academic research on organisational learning from cyber security incidents and identifying further research needed in this area. To do this, it considers three research questions: what research has been conducted on learning from cyber security incidents, what learning practices in organisations have been found by research and what improvements have been recommended, and what further research is needed as organisations learn from such incidents. Using the PRISMA method, a total of 3,986 articles were extracted and, from these, a relevant set of 30 were selected for analysis to map the body of research, and to identify future research avenues. Despite learning lessons being recommended by both researchers and industry standards, our findings suggest that this advice is not being fully adopted by organisations. Importantly, these studies have found inadequate participation in learning activities, with superficial causal investigations, scarce effort on ensuring lessons are implemented and no evaluation of whether the actions taken actually reduce future security incidents. More research is needed to understand the right level and which learning practices to invest in for the greatest impact. For practitioners, this review discusses the essential elements of an effective process to learn from incidents. This review provides academics with a novel synthesis of the research undertaken on this topic, enabling them to incorporate the significant findings into their work and potentially explore the research agenda suggested.

© 2023 The Author(s). Published by Elsevier Ltd.
This is an open access article under the CC BY-NC-ND license
(http://creativecommons.org/licenses/by-nc-nd/4.0/)

1. Introduction

The rapid digitalisation of our society has created complex webs of interwoven and interdependent systems across commerce, education, health and governments (World Economic Forum, 2022). Recent headlines about vulnerabilities in software such as Solar Winds, Kaseya and Log4j have heightened organisations' awareness of their dependence on suppliers and the intricate nesting of software within their systems (Tuttle, 2022). These risks are increasingly being exploited by financially motivated criminal enterprises and by state-sponsored actors to leverage political influence or cause disruption (Connolly and Wall, Nov. 2019). Despite an expected spend of $170 billion on investment in security and risk management in 2022 (Moore, Oct. 13, 2022), the number and impact of incidents continues to grow. Statistics on the rate of incidents are fraught with challenges around definitions and most reports produced are from those in the business of selling security services. However, in one of the few independent reports, the UK government's 2022 survey of 1200 businesses and charities found around half had experienced at least one cyber security incident in the past year (72% if phishing incidents are included) (NCSC, 2022).

Unfortunately, it is essential for today's organisations to acknowledge that incidents will occur, and they need to be prepared to respond and then learn from them. In addition to the rise in incidents, many organisations now face more security regulations, higher consumer expectations and new reporting requirements related to data privacy and infrastructure resilience. Therefore, to address the increased incident risks they cannot just work harder particularly as many face a shortage of cyber security skills (de Zan, 2019). Learning from incidents is a vital strategy that can help improve risk awareness, protective measures, and organisation response capability (Connolly and Wall, 2019). An organisation's ability to learn requires systemic thinking and recognising incidents can have multiple, and sometimes less than obvious, causes (Schein, 2017). By resolving the underlying causes, security teams

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

https://doi.org/10.1016/j.cose.2023.103309
0167-4048/© 2023 The Author(s). Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license
(http://creativecommons.org/licenses/by-nc-nd/4.0/)

can stop the increase in incidents, which in turn will help them manage their workload (Gonzalez, 2005; Sveen et al., 2007).

Many studies have been conducted into organisational learning and although the literature has been summarised (Fiol and Lyles, 1985; Huber, 1991; Easterby-Smith and Lyles, 2012; Argote, 2013) there is no generally accepted definition. Argote (2013) described it as a change in the organisation's knowledge as a function of experience. Fiol and Lyles (1985) in their definition of organisational learning include translating this new knowledge into actions taken by the organisation. Argote and Ophir (2017) refer to it as a process where changes are made as a result of experiences. The research into general organisational learning is vast and much of it has focused on using knowlege to improve the productivity or competitiveness of organisations (for example, Peter Senge's popular 1990 business book The Fifth Discipline: The art and practice of the learning organization (Senge, 2010)) or, it has focused on enhancing skills and emergent team learning (Argote and Levine, 2017). Rather than an extensive review of the theories of organisational learning in this paper, we have sought to leverage existing models which fit our research focus.

To understand learning from cyber security incidents, we needed to look at research into how organisations intentionally identified and implemented lessons learned from incidents. Research into how organisations learn specifically from incidents has been focused in the safety discipline, with prominent studies into public disasters such as the Deepwater Horizon Macondo oil rig, the Challenger space shuttle and the Fukushima nuclear power plant (Swuste et al., 2020).

Safety has a more established field of research into learning from incidents with many years of research exploring how to reduce the number and impact of incidents (Le Coze, 2013; Jaatun et al., 2009). It shares many similarities with cyber security as they both seek to reduce the risk of incidents. Evans et al. (Evans et al., 2019) recognised the value of applying the techniques developed in the safety field to understand human reliability causes of safety incidents applied to security incidents. Similarly, other authors (Kaur et al., 2021; Murphy et al., 2021; Brostoff and Sasse, 2001) have commented that cyber security can learn from safety science research particularly in how to address human causes of incidents. There is an opportunity to borrow concepts from research on learning from safety incidents to advance the field of cyber security (Line and Albrechtsen, 2016). Murphy et al. (2021) defined three interconnected forms of learning from incidents, firstly at the individual level and then at both the formal and informal organisational learning levels. Schilling and Kluge (2009) also modelled learning at distinct levels, from the individual to organisational level. Individual learning is part of the process, but for an organisation to learn, it needs to go beyond and include shared knowledge interpreted in an organisational way (Curado, 2006).

This systematic literature review (SLR) will focus on formal learning at the organisational level from cyber security incidents, as our focus is on the changes to systems, procedures and technology as a result of an incident. This review exclusively covers cyber security incidents, rather than generic IT incidents such as hardware failures and performance issues. The objective is to help organisations improve their overall security posture by understanding and addressing the complex causes of incidents. Therefore, this review analyses how organisations learn post-incident rather than learning in real time during incident response. For transparency, it excludes; operational technology, including industrial control systems or home devices, digital forensics techniques and national security or warfare.

Shedden et al. (2010) reviewed the literature available in 2010 to understand how organisational learning research could be applied to security incident response. At the time there had been scant research into how organisations learn from cyber security incidents. More recent literature reviews have studied the complete security incident management process and, whilst also partially covering learning briefly, they do not cover the topic in depth (Line and Albrechtsen 2016; Grispos et al., 2014; Horne et al., 2020). In our SLR we address this gap by building upon previous research to provide an up-to-date overview of the literature focused specifically on learning from incidents. From this analysis we identified many areas of learning from security incidents, which remain unstudied which we used to highlight future research avenues.

This SLR presents a critical review of the academic literature on learning from incidents and proposes an agenda for further research. It enables academics to explore these research gaps and it allows practitioners to consider opportunities for improvements. By contributing to the knowledge of how to improve the resilience of organisations against security incidents, this research aims to help reduce the security risks society faces from its dependence on technology. To do this, it addresses the following research questions (RQs):

(1) What research has been conducted on learning from cyber security incidents?
(2) What learning practices in organisations have been found by research and what improvements have been recommended?
(3) What further research is needed in organisational learning from incidents?

The remainder of this paper is structured as follows. In Section 2 we present the research method used in this study. The results outlining existing research are detailed in Section 3 while Section 4 discusses the organisational learning practices found by research and the gaps identified from our systematic search of the literature to explore future research opportunities and provide future research questions. In this section we also outline the practical implications of this work and the limitations. Finally, in Section 5 we conclude by summarising the insights of our work for security researchers and practitioners.

2. Research method

2.1. Search strategy

Following the principles of repeatability described by Kitchenham et al. (Kitchenham et al., 2010), this section gives transparency to the search approach used. Our approach adopts the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework to explain our rationale for the decisions taken on the search strategy, sources, eligibility criteria, selection process, and how the studies were analysed (Moher et al., 2009). PRISMA is now a common technique used in cyber security research (Uchendu et al., 2021; Khan et al., 2022).

The search terms used were refined iteratively. We began with terms which naturally link to the topic ('security incident' and 'learning'), then refined these search terms according to the results. This refinement was also guided by a set of gold standard papers on the topic (i.e., those on our exact topic area) which were discovered early on in our search. An example of a search refinement was as follows: the term 'learning' returns many results related to machine learning rather than organisational learning; therefore, terms such as 'organisational learning' and 'lessons learned' were used. After this refinement process, the final search string was defined, which combined several critical search terms: ("security incident" OR "incident response" OR CSIRT[1]) AND ("organisational

[1] Cyber Security Incident Response Team

Table 1
Screening criteria.

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

learning" OR "organizational learning" OR "lessons learned" OR "lessons learnt"). This allowed us to balance being too narrow and missing publications or being too broad and generating unwieldy initial results. Full text searches were conducted and there were no date restrictions or other filters applied. The searches were conducted in September 2022. For transparency, details of the exact search strings and databases searched are included (see Appendix A).

2.2. Eligibility criteria

The returned papers were reviewed using the screening criteria set out in Table 1 and were included if the research covered learning from incidents even if this was not their main focus.

2.3. Information sources

We selected the following online sources to conduct the search: ACM Guide to Computing Literature, IEEE Xplore, ScienceDirect, Wiley Online Library, SpringerLink, ProQuest One Literature and Publicly available content Database (excluding Global Theses and Dissssertations), Scopus, and the Web of Science Core Collection. These sources include both journals and conferences aimed specifically at cyber security, as well as other disciplines which may have covered organisational learning in a cyber security context. This increased the chances of finding relevant peer-reviewed studies which met our inclusion criteria 1 and 2, in Table 1. Google Scholar was not included due to the limitations of its search functionality, such as a lack of full Boolean operator support and inconsistent reproducibility (Gusenbauer and Haddaway, 2020).

2.4. Study selection

The results of the database searches identified 3,986 papers which were screened according to exclusion criteria 1–4, in Table 1. Firstly, 664 duplicate studies were discarded. Another 11 papers not written in English or those where the full text was not accessible, and 861 non-academic and non-peer reviewed articles were removed. Titles, abstracts and keywords were reviewed for the remaining 2450 articles to assess their relevance in answering our research questions. This resulted in 2333 studies being excluded and another 95 excluded after a full-text review, leaving 22 papers selected through the initial search.

There are no perfect search terms and it is particularly challenging for IT research, as the terms are constantly evolving and the publication databases can treat search terms differently (Zhang et al., 2011). Therefore, the initial search string results were enhanced through a process of interpretation and understanding (Boell, 2014). This extra process included searching journal databases, inspecting the table of contents of known cyber security journals and examining relevant conference proceedings. We also reviewed the citations of articles on the topic and used Connected Papers[2] and Web of Science[3] to identify relevant articles citing those already found. The Google Scholar Author pages for all the authors of the selected articles were also reviewed to identify missed articles. The search results were compared with the bibliographies of existing literature reviews (Line and Albrechtsen, Mar. 2016; Shedden et al., 2010; Grispos et al., 2014; Tøndel et al., 2014; Horne et al., 2020) to ensure that all previously identified articles were found in the search process. The additional articles identified through these supplementary methods were then also reviewed against the eligibility criteria in Table 1. This resulted in 8 additional papers being added to the list. Fig. 2 illustrates a PRISMA flow diagram of the selection process to obtain the final 30 articles.

2.5. Data collection

As directed by PRISMA, the data items collected against each research question are set out in Table 2. To present an overview of the types of research conducted and published in this area, the selected articles were analysed by original publication details and by the research methods used. To understand how researchers have assessed the learning practices for cyber security incidents, we reviewed the foundation they used to frame their studies.

To analyse which cyber security learning incident practices the studies had covered we looked at how other researchers had described the practices of learning from incidents. We found those which were most relevant to learning from cyber security incidents were studies into learning from safety incidents (Littlejohn et al., 2017; ESReDA, 2015; Vastveit et al., 2015; Drupsteen et al., 2013). These practices are also applicable to learning from cyber security incidents due to the similarities between safety and security recognised by several authors (Kaur et al., 2021; Cockram and Lautieri, 2007; Kriaa et al., 2015; Lisova et al., 2019).

There have been a range of models used within safety research aligned to the different angles from which the topic has been studied (Le Coze, 2013). Murphy et al. (2021)analysed learning from safety incidents using the 3-P model of workplace learning. This has three phases: presage, process and product. Their study was focused on the perspective of the frontline worker. In contrast, Le Coze (2013) in his overview of research into learning from safety incidents used a broad framework covering: industry, countries nations, actors, intensity of event, disciplines and steps. It is the steps element which is more relevant for this study as it includes the learning activities; reporting, selection, investigation, dissemination and prevention. For this review we wanted to analyse the learning process in more depth to understand the activities the organisation conducted to learn from incidents so identified learning process models with more depth. Drupsteen et al. (2013) developed a learning from incidents process model based on a review of safety literature and consulting with safety experts from industry. This model provided more emphasis on investigating the cause to acquire the knowledge and then how that knowledge is translated into actions. This included an evaluation step to assess the effectiveness of implementing the lessons learnt.

[2] https://www.connectedpapers.com
[3] http://www.webofscience.com/

Table 2
Data items collected.

Data item	Description	RQ
Publication venue details	Where the article was published and the year of publication.	1
Research details	Countries and the industries in which the research was conducted, if stated. The type of research method (e.g., case study, interviews, theory-based research).	1
Research foundation	The models and standards used to frame the research, (such as ISO/IEC 27035 or NIST 800–61[b]), or models borrowed from management science (such as double-loop learning (Argyris, 1976) or from safety such as Goal Structured Notation (The Assurance Case Working Group ACWG, 2021).	1, 3
Learning practices	Which parts of the learning process are covered by the study, either completely or partially. What practices were found and what improvements were recommended.	2, 3

[b] ISO/IEC 27035 information security incident management (van Court Hare 18, 2021a; van Court Hare, 2021b; van Court Hare, 2022; so/IEC, 2023) and National Institute of Standards and Technology SP 800−61Computer Security Incident Handling Guide (Cichonski, 2012).

Lukic et al. (2012) also developed a framework for learning from safety incidents based on the literature and validated the model at two organisations. Littlejohn et al. (2017) built on this model in their more recent study and included input from other sites and companies and sharing lessons learned with others. They also looked at the learning process through the context, participants, type of incident and knowledge. Despite safety research being relatively mature compared to cyber security research on learning from incidents, it has yet to develop a unifying theory (Swuste et al., 2020). To create a practical tool to collect data on the learning practices, the process definitions were combined from both the Littlejohn et al. (2017) and Drupsteen et al. (2013) studies to include the end-to-end process, as these two studies provided the most comprehensive analysis of the learning process activities organisations can perform.

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

Participation in the learning process includes how the learning might be organised and the involvement of different areas of the organisation. Causal analysis includes reporting incidents, categorising incidents and analysing the causes. Both these improvement categories include determining and prioritising actions, allocating accountability, dedicating resources and tracking the actions to completion. The participation of different teams and the learning approach taken will impact the breadth of causes considered and the causes found will impact the improvements made. How these are implemented can impact the security of the organisation. The final learning evaluation phase includes ensuring that actions are taken, as well as confirming that the action actually enabled the anticipated improvement. It also evaluates how well the organisation is learning from incidents. Insights from this phase help an organisation to improve its learning process. A poor learning process would be evident through recurrence of incidents which have similar causes or similar impacts and the organisation has not adapted its protection, detection and response capabilities.

The phases of the learning process set out in Fig. 1 were used to collect the data in Table 2 using a deductive approach to examine and describe the coverage of learning.

3. Results

The structured literature review resulted in the identification of 30 relevant papers as shown in the PRISMA flowchart in Fig. 2. These are analysed in this section to present the research conducted on the topic of organisational learning from cyber security incidents. Despite the rise in cyber security incidents there have been surprisingly few dedicated studies on how organisations can learn from them to reduce their impact and frequency. Studies are only reported against a data collection category if it is clear from the article. For some studies, there are multiple articles on the same piece of empirical work[4].

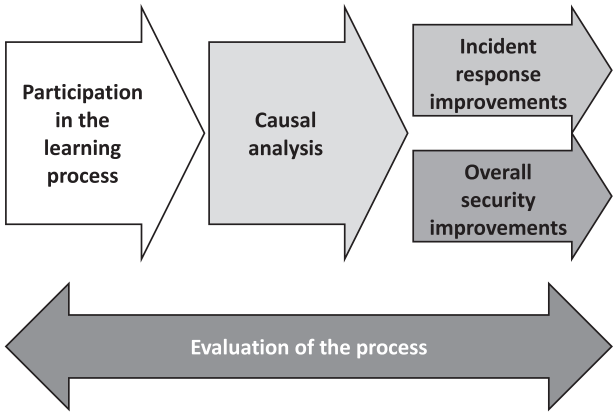

Fig. 1. The phases of the learning process adapted from Littlejohn et al. (2017) and Drupsteen et al. (2013).

3.1. Research and publication details

All selected articles were published in the last 16 years. There is no distinct trend in the timing of the publications; there was a relative flurry of publications between 2014 and 2016, but with small numbers such variation is expected. There has been a continued level of interest in the topic; as illustrated in Fig. 3. The most common publication venue was the Computers & Security journal with four studies published on the topic but, overall, there was a wide range of venues (for example, the International Journal of Information Management and Hawaii International Conference on System Sciences).

The geographical location in which the studies were conducted is shown in Table 3. The majority of the selected studies were conducted in four countries and in only four sectors; Norwegian energy industry (Jaatun et al., 2009; Line et al., 2006; Line, 2013;

[4] Jaatun et al. (2009), Line et al. (2006) relate to the same research project "Incident Response MAnagement" (IRMA), funded by the IKT SoS programme of the Research Council of Norway and The Norwegian Oil Industry Association (OLF), 2005 to 2007. Line (2013), Bartnes et al. (2016) relate to the same research programme at power distributors in Norway. Grispos et al. (2015), Grispos et al. (2017), Grispos et al. (2019) relate to the same research project at a UK financial organisation. He et al., (2014a), He and Johnson (2015), He and Johnson (2017) relate to the same research project at a Chinese healthcare provider and and He et al. (2014b) and He et al. (2015) relate to the same research on the usability of GSN.

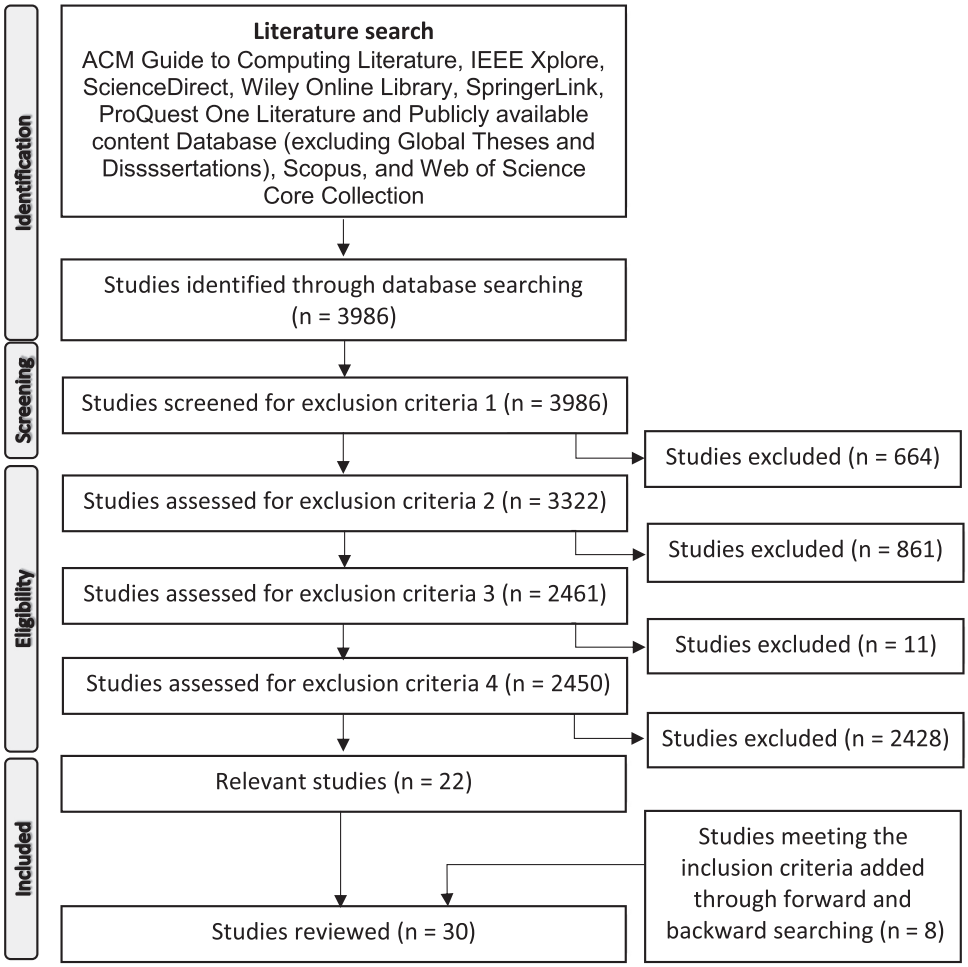

Fig. 2. PRISMA flow diagram presenting the inclusion process.

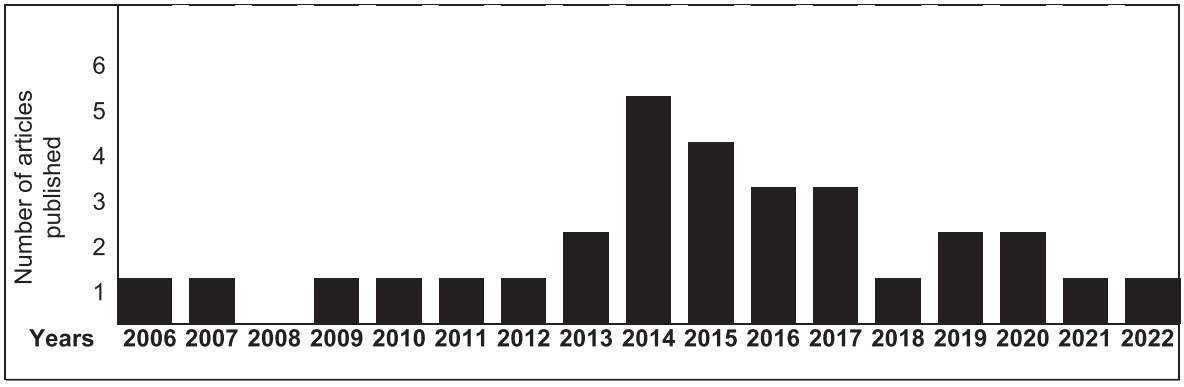

Fig. 3. The publication year of the articles analysed.

Line et al., 2016; Bartnes et al., 2016), Australian (Shedden et al., 2011; Ahmad et al., 2012; Ahmad et al., 2015) and UK financial services (Grispos et al., 2017; Grispos et al., 2019), and Chinese (Y. He et al., 2014; He and Johnson, 2015; He et al., 2015; He and Johnson, 2017) and UK healthcare (He et al., 2022). There were 8 studies where the location was not specified or not applicable (for example, articles presenting literature reviews).

Table 4 shows the wide range of research methods which have been applied to studying the topic. Studies reviewing existing literature include Shedden et al.'s (2010) study on organisational learning, Tøndel et al.'s (2014) review of the current practice of incident management and Line and Albrechtsen's (2016) paper on how the theories and techniques from industrial safety could be applied to the cyber security field. The study by Grispos et al. (2014) evaluated the standards for incident management and is focused on using Agile concepts in incident management yet does highlight the importance of learning and encourages organisations to learn throughout the incident lifecycle. Horne et al. (2020) reviewed academic literature and industry standards focusing on the governance of incident response, but they also drew attention to the lessons learnt phases in both the standards and the literature. Additionally, there were theoretical studies which whilst they com-

Table 3
Geographical location where the analysed studies were conducted.

Geographical location of where the study was conducted	No. of studies	References
Australia	5	Shedden et al. (2011), Ahmad et al. (2012), Ahmad et al. (2015), Ahmad et al. (2020), Lakshmi et al. (2021)
China	5	He et al. (2014a), He et al. (2014b), He and Johnson (2015), He et al. (2015), He and Johnson (2017)
Europe (specific countries not listed)	1	Baskerville et al. (2014)
Netherlands	1	van der Kleij et al. (2017)
Norway	5	Jaatun et al. (2009), Line et al. (2006), Line (2013), Line et al. (2016), Bartnes et al. (2016)
UK	5	Grispos et al. (2014), Grispos et al. (2015), Grispos et al. (2017), Grispos et al. (2019), He et al. (2022)
Unspecified or not applicable	8	Sveen et al. (2007), Evans et al. (2019), Line et al. (2016), Shedden et al. (2010), Tøndel et al. (2014), Horne et al. (2020), Bernsmed and Tøndel (2013), Tatu et al. (2018)

Table 4
Research methods used by the articles analysed.

Research Methods Used	No. of studies	References
Case study	9	Evans et al. (2019), Ahmad et al. (2012), Line (2013), Baskerville et al. (2014), Ahmad et al. (2015), Bartnes et al. (2016), He et al. (2017), Grispos et al. (2017), Grispos et al. (2019)
Combination of methods (interviews, case studies, questionnaires and workshops, or incident analysis)	1	Jaatun et al. (2009)
Focus groups	1	Shedden et al. (2011)
Interviews	8	Line et al. (2006), He et al. (2014a), Grispos et al. (2015), He and Johnson (2015), Line et al. (2016), van der Kleij et al. Dec. (2017), Tatu et al. (2018), Lakshmi et al. (2021)
Literature review	5	Line and Albrechtsen Mar. (2016), Shedden et al. (2010), Grispos et al. (2014), Tøndel et al. (2014), Horne et al. (2020)
Systems Thinking	1	Sveen et al. (2007)
Theoretical study	5	Bernsmed and Tøndel (2013), He et al. (2014b), He et al. (2015), Ahmad et al. (2020), He et al. (2022)

mented on existing literature, they also introduced new models or approaches to analysing the topic (Bernsmed and Tøndel, 2013; He et al., 2014b; He et al., 2015). Other studies developed models and applied them to a fictitious case study or publicly available data (Ahmad et al., 2020; He et al., 2022).

Many studies used interviews or focus groups (Line et al., 2006; Shedden et al., 2011; He et al., 2014a; Grispos et al., 2015; He and Johnson, 2015; Line et al., 2016; van der Kleij et al., 2017; Tatu et al., 2018; Lakshmi et al., 2021). Interviews are a valuable method to understand social processes and the views of participants, but responses must be carefully interpreted within the context in which they are given (Silverman, 2017). As they are quicker to conduct than an in-depth case study, they can allow more organisations to be studied (Line et al., 2006; Line et al., 2016; van der Kleij et al., Dec. 2017; Lakshmi et al., 2021) or to give a wider perspective by interviewing multiple participants from the same organisation (He et al., 2014b; Grispos et al., 2015; He and Johnson, 2015; Tatu et al., 2018).

Most of the research has used case studies (Evans et al., 2019; Ahmad et al., 2012; Line, 2013; Baskerville et al., 2014; Ahmad et al., 2015; Bartnes et al., 2016; He and Johnson, 2017; Grispos et al., 2017; Große et al., 2020; Grispos et al., 2019). Case studies were also applied in combination with other research methods (Jaatun et al., 2009). They are a useful method to understand real-world perspectives of the practices organisations follow to answer how or why research questions (Yin, 2018). Although the ability to generalise the findings of one case study is constrained, as there have been multiple case studies with similar findings about learning from incidents, it enables researchers to construct a more general view of how organisations approach learning. It can be difficult to gain access to organisations to perform this type of work, particularly since there can be sensitivity around the confidentiality of incidents that have occurred (Ahmad et al., 2012; Bartnes et al., 2016).

The frequent use of case studies has given insight into how organisations perform learning from incidents. However, most of this research was conducted five to ten years ago, when the frequency and severity of incidents were lower for many organisations. In addition, few concentrated specifically on learning and the majority only commented on the lessons learned as a small part of a wider study. Considering the pace of change in cyber security, there is the need for more recent research specifically focusing on learning from incidents.

3.2. Research foundations

To gain insight into how researchers had designed their studies, we analysed the foundations used to frame the research. Table 5 shows safety research was the most common foundation applied to frame existing studies. Management science was the next most common research foundation others made use of IT standards to structure their research and some have applied constructs from software engineering, with a few adopting psychology approaches.

Both ISO/IEC 27035 and NIST 800–61 have frequently been utilised within our selected studies: ISO/IEC 27035 (Line et al., 2006; Line, 2013; Line et al., 2016; Jaatun et al., 2016; Bartnes et al., 2016) and NIST 800–61 (Grispos et al., 2015; Ahmad et al., 2020). As they have learning as part of their end-to-end processes, this has encouraged studies to gather information on this step. For example, Grispos et al. (2015) conducted a case study in a global Fortune 500 financial organisation in the UK, which included an exploratory set of interviews using the NIST 800–61 phases as a framework to present the Security Incident Response Criteria (SIRC), which can be employed to evaluate cyber security incident response solutions.

Table 5
Research foundations used to frame the studies.

Research foundations used	Origin	No. of studies	Refs.
4I model	Management Science	2	Ahmad et al. (2015), Ahmad et al. (2020)
Agile Manifesto	Software engineering	3	Grispos et al. (2014), Grispos et al. (2017), He et al. (2022)
Goal Structuring Notations (GSN)	Safety	5	He et al. (2014a), He et al. (2014b), He and Johnson, (2015), He et al. (2015), He and Johnson (2017)
Human Error Assessment and Reduction Technique (HEART) & Human Reliability Analysis (HRA)	Safety	1	Evans et al. (2019)
Incident Response MAnagement (IRMA) & Sequential Timed Events Plotting (STEP)	Safety	1	Jaatun et al. (2009)
Incident-centred security	Security	1	Baskerville et al. (2014)
ISO/IEC 27,035	IT Standard	5	Line et al. (2006), Line (2013), Line et al. (2016), Bartnes et al. (2016), He and Johnson (2017)
Needs Assessment	Psychology	1	van der Kleij et al. (2017)
NIST SP 800–61	IT standard	4	Line et al. (2006), Grispos et al. (2015), He and Johnson (2017), Ahmad et al. (2020)
Organisational learning such as double-loop learning	Management Science	4	Shedden et al. (2010), Shedden et al. (2011), Ahmad et al. (2012), Ahmad et al. (2020)
Resilience based Early Warning Indicators (REWI)	Safety	1	Bernsmed and Tøndel (2013)
Sensemaking	Psychology	1	Lakshmi et al. (2021)
Systems Thinking	Management Science	1	Sveen et al. (2007)
Theory of involvement	Psychology	1	Tatu et al. (2018)
Unspecified or not applicable	–	3	Tøndel et al. (2014), Horne et al. (2020), Grispos et al. (2019)

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

The ISO/IEC 27035 lessons learnt phase encourages organisations to identify lessons which could improve their controls and risk assessments, as well as their incident management. It also suggests identifying trends that could give an early warning of potential future incidents. NIST 800–61 and ISO/IEC 27035 both list questions to ask in the post-incident meeting, but these questions are only aimed at improving incident response. As these two standards do not cover learning in much detail, studies that have applied them to structure their research have borrowed models from management science (Sveen et al., 2007; Shedden et al., 2010; Shedden et al., 2011; Ahmad et al., 2012; Ahmad et al., 2015; Ahmad et al., 2020) or the safety discipline (Jaatun et al., 2009; Evans et al., 2019; Bernsmed and Tøndel, 2013; He et al., 2014a; He et al., 2014b; He and Johnson, 2015; He et al., 2015; He and Johnson, 2017).

For example, many of our studies refer to the concept of 'double-loop learning', which originates from the work of Argyris in the 1970s (Argyris, 1976). Although Argyris was writing in 1976 and not specifically about learning from incidents, his observation that as "problems become increasingly complex and ill-structured, the need for learning increases, but so does the difficulty in carrying out effective learning" (Argyris, 1976) [Page 365] could be applicable to the cyber security space today. His research at the time found that people in organisations were encouraged to learn as long as they did not question the "fundamental design, goals and activities of their organisations", which is single-loop learning. Double-loop learning is used to understand not only the governing variables that led to the immediate obvious consequences, but also to dig deeper to understand what factors may have contributed to or enabled the incident, see Fig. 4. In a cyber security context, single loop learning would be indentifying the cause of an incident, such as an unpatched software package, and taking an action, such as to apply the patch. Double loop learning would be questioning the governing variables which prevented the timely patching. Addressing these underlying factors would reduce the likelihood of recurring problems, such as of any software remaining unpatched in the future. The double-loop model has been applied to learning from incidents in studies included in our selection (Shedden et al., 2010; Shedden et al., 2011; Ahmad et al., 2012; Ahmad et al., 2020). For example, Ahmad et al.'s (2012) study builds on a model from safety incidents Cooke (2003) and is inspired by double-loop model, to develop a model of a cyber security incident learning system.

This double-loop learning theme is continued in a subsequent study by Ahmad et al. (2015) which uses the 4I (intuiting, interpreting, integrating, institutionalizing) organisational learning framework, building on work by Zietsma (Zietsma et al., 2002) in management science. One of the reasons this model was selected was its use of double-loop learning principles enabling the challenge of an organisations' norms. The model has three layers that cover stakeholders, learning processes, and learning activities that embed learning within the organisation. This attempts to explain how learning can happen within an organisational context. Ahmad et al.'s (2020) study again highlights the importance of double-loop learning. Using the analogy of a shield, the paper describes single-loop learning as fixing holes in the shield and double-loop learning as changing the shape and thickness of the shield. The models of double-loop learning have been recommended by cyber security researchers (Shedden et al., 2010; Shedden et al., 2011; Ahmad et al., 2012; Ahmad et al., 2020), yet the models themselves give little guidance to practitioners in how to move an organisation towards this type of learning. Grispos et al. (2017) explained without a commitment to learning, the organisation did not act to address the underlying causes. For an organisation unfamiliar with causal analysis and organisational learning, it may be a challenge to successfully implement the model without further support.

The Norwegian oil and gas industry developed a method for Incident Response MAnagement (IRMA[5]) incorporating Argyris's (1976) double-loop learning concept. This IRMA model uses phases from the ISO 27035 and NIST 800–61 standards. It emphasised the post-incident learning phase from the Sequential Timed Events Plotting (STEP) method introduced in 1986 by Hendrick and Benner in their 'Investigating Accidents with STEP' book (Hendrick et al., 1986). The model aimed to help teams identify root causes and weak points in the barriers they have implemented to prevent incidents.

[5] IRMA is the abbreviation of Incident Response Management.

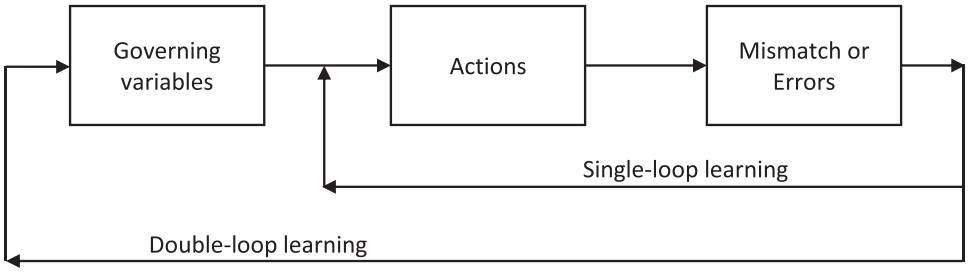

Fig. 4. Double loop learning adapted from (Argyris, 1990).

Bernsmed and Tøndel (2013) adapted the Resilience based Early Warning Indicators (REWI) method employed to address safety incidents in the Norwegian energy sector to cyber security incidents. REWI categorised the attributes needed for resiliency against incidents as risk awareness, response capacity and support (technical, human and organisational). It emphasised that it is important for organisations to learn from incidents, including the success stories, as resilience is about enhancing the capacity of an organisation to respond.

In five studies, He et al. (2014a), He et al. (2014b), He and Johnson (2015), He et al. (2015), He and Johnson (2017) explored the use of the Goal Structuring Notations (GSN) safety engineering approach, which was extended from applications in safety-critical systems, as a technique to understand the potential causes of cyber security incidents. GSN was developed over several years by the Safety-Critical Systems Club to enable organisations to build safety cases for critical infrastructure (The Assurance Case Working Group ACWG, 2021). The aim of the notation is to demonstrate the causes of incidents in terms of failures of controls or policies.

He et al. (2014b) conducted two studies with students, the first training them in GSN techniques and asking them to evaluate it. The second asked students to map the causes of a simplified incident using the GSN template to build a safety case. GSN was then trialled at a Chinese healthcare provider (He et al., 2014a; He and Johnson, 2017). Feedback was mixed; while they found it could be a valuable template for some groups such as those within the incident response team, it had some limitations for use with a wider audience. It is a technique to explain the hierarchy of causes where these are clearly defined. Drawing on a mechanistic perspective, it represents incidents as a failure in a component of the system. It assumes the relationship between components is known and linear, as it was designed to assess infrastructure rather than to elicit underlying and more socio-technical causes.

Others have borrowed the Agile approach from software engineering (Grispos et al., 2014; Grispos et al., 2017; He et al., 2022). The Manifesto for Agile Software Development has gained popularity in the development of software products (Beck et al., 2001). Grispos et al. (2017) conducted a trial of using it to learn from security incidents. Whilst agility in incident response is essential, the application of some elements of the Agile approach is challenged by the core principles of design and planning products versus the inherently reactive nature of incident response. Agile does emphasize continuous learning and refinement of the product and this learning focus could be useful in engaging software developers familiar with the Agile philosophy in learning from incidents.

Several researchers have applied psychology models. Lakshmi et al. (2021) borrowed the lens of sensemaking which is typically used to analyse socio-cognitive and socio-organisational activities. They included the socio-technical perspective as they applied it to Cyber Security Incident Response Teams (CSIRT) activities. The study did not go into depth on learning from incidents but did explain how people created their own narratives about what happened. They found the incident responders made sense during the incident response through "Enactment", "Selection" and "Retention". Van der Kleij et al. (2017) applied four needs assessment categories: Organisation, Team, Individual and Instruments, as a tool to understand the skills CSIRTs needed. They found organisational learning from incidents needed to be improved and recommended improving performance by implementing a lessons learnt procedure. Tatu et al. (2018) adapted involvement theory to apply it to security, and in particular the "knowledge" dimension became "experience sharing" and included lessons learned from security incidents. They studied an organisation which had experienced a ransomware incident and found people's security awareness had improved, which could protect the organisation from similar incidents. Overall, the literature has used a variety of models; yet, there has not been a comparison of models proposed by researchers or recommendations on which approach organisations should adopt in specific scenarios.

3.3. Learning practices

The selected articles coverage of the learning process was assessed using the five phases set out in Fig. 1.

The coverage of the five parts of the learning process, shown in Fig. 1, is represented using the following graphic symbols:

(a) ● "Substantial coverage" represents articles that fully cover this part of the process.

(b) ◑ "Partial coverage" where the topic is discussed but not all relevant aspects are mentioned, for example, suggesting an approach to causal analysis but not considering how this would be conducted in the context of organisational politics and agendas, or suggesting improvements without including prioritisation or tracking of actions.

(c) ◔ "Light touch" when a paper only briefly comments on the topic, such as only referring to the distribution of a post-incident report to management, but not covering any other aspects of participation, such as who was involved in analysing the causes or deciding the lessons learned.

(d) ○ "None" there is no explicit mention of the topic.

The lack of consensus on a framework for researching learning practices results in inconsistent approaches to describing the learning expected or found by researchers, as can be seen in Table 6.

3.4. Participation in the learning process

Most researchers did not comment on who in the organisation participated in learning from incidents, with less than a third covering it in any depth. Those who looked at this aspect of the learning process found that formal learning from incidents was reserved for major incidents (Ahmad et al., 2012; Line, 2013; Ahmad et al., 2015; Line et al., 2016). Researchers recommended organisations

Table 6
Coverage of the learning process by the articles analysed.

Articles	Participation in the learning process	Causal analysis	Incident response improvements	Overall security improvements	Evaluation of the process
(Grispos et al., 2015; He et al., 2015; He et al., 2014b)	○	◑	◔	◔	○
(Line et al., 2006)	◑	◑	◑	◑	◑
(Sveen et al., 2007)	○	◔	◑	◑	◔
(Jaatun et al., 2009)	◔	◑	◔	◔	○
(Shedden et al., 2010)	◔	◔	●	◑	○
(Shedden et al., 2011)	○	○	●	◔	○
(Ahmad et al., 2012)	●	●	●	●	○
(Bernsmed & Tøndel, 2013)	○	◔	◑	◔	◔
(Line, 2013)	○	○	◔	○	○
(Baskerville et al., 2014)	○	◑	◑	◑	○
(Tøndel et al., 2014)	●	◑	◑	◑	◔
(He, et al., 2014a)	◔	◑	◑	◑	○
(Grispos et al., 2014)	○	◑	◔	◔	○
(Ahmad et al., 2015)	●	●	●	●	◔
(He & Johnson, 2015)	○	◑	◔	◑	○
(Line et al., 2016)	◔	◔	○	○	○
(Line & Albrechtsen, 2016)	◑	◑	◔	◔	○
(Bartnes et al., 2016)	●	◔	◔	◔	●
(He & Johnson, 2017)	◔	◑	◑	◑	◔
(van der Kleij et al., 2017)	○	○	◑	◔	◔
(Grispos et al., 2017)	◑	◑	●	●	●
(Tatu et al., 2018)	○	○	○	◔	○
(Grispos et al., 2019)	○	◑	◔	◔	○
(Evans et al., 2019)	○	●	◔	◔	○
(Ahmad et al., 2020)	○	●	◑	◑	◔
(Horne et al., 2020)	○	◔	◔	◔	○
(Lakshmi et al., 2021)	◑	●	◑	◔	○
(He et al., 2022)	◔	◔	◑	◑	○

consider the learning opportunities from a wider range of incidents. Ahmad et al. (2015) emphasised the chance to learn about critical assets, technology risks and the causal structures of security incidents from a wider selection of incidents. These major incident reviews were also restricted to those directly involved with the specific incident (Jaatun et al., 2009; Ahmad et al., 2012; Ahmad et al., 2015; Grispos et al., 2017). For example, Ahmad et al. (Ahmad et al., 2012; Ahmad et al., 2015) found only the technical teams were involved in the post-incident learning, which may restrict the identification of underlying causes to those of a technical nature. Grispos et al. (Grispos et al., 2017) recognised the limitation of the incident response team not developing actions on the lessons learnt for areas outside their responsibility. Bartnes et al. (Bartnes et al., 2016) suggested that organisations should consider the use of trained facilitators to help the effectiveness of looking back to identify lessons from an incident although how this may help has yet to be studied.

Furthermore, the researchers found that the identified lessons were not shared beyond incident teams (Jaatun et al., 2009; Ahmad et al., 2012; Ahmad et al., 2015; Grispos et al., 2017). Line et al. (2006) emphasises the importance that lessons from incidents are shared with all parts of the organisation including management, suppliers and employees. There were some exceptions where the lessons were shared. He and Johnson (2017) found the healthcare provider they studied held informal meetings to share the lessons learned with different stakeholders. Baskerville et al.'s (2014) case study of three organisations (rail, postal, and military) found the postal organisation also began sharing more incident data with its competitors following a serious incident.

The impact of sharing the lessons with different stakeholders and peers was not covered in the literature. Jaatun et al. (2009) advocate the importance of learning from incidents and recommend the IRMA model, in which learning is fed back into the preparation step. However, when Jaatun et al. (2009) conducted their field work, few of the respondents had experienced a security incident. For those which had experienced an incident, the time between incidents was between one and two years, which gave the authors fewer actual examples to study (Jaatun et al., 2009). The study did additionally find there was a cultural hesitancy to report incidents, so potentially the respondents may not have been aware of all the incidents that were happening. The learning phase was considered important by many of the interviewees, but not all, as some felt it would have little effect and would quickly be forgotten (Jaatun et al., 2009). It is unclear why there was a difference in opinion.

The organisations studied by Bartnes et al. (2016) also had not experienced any major cyber security incidents, but since the organisations conducted post-incident reviews for other types of incidents, they expected that they would do so for security incidents, if they were to occur. The main issues identified were; not prioritising learning activities, the limited efforts to understand

the underlying causes, and missing the opportunity to apply lessons to improve the whole security posture of the organisation. Bartnes et al. (2016) highlighted minor incidents could be a source of lessons for organisations and recommended they explore double-loop learning when they do experience even minor incidents. The benefits of analysing minor incidents was not studied. In a study by Shedden et al. (2011), informal learning within CSIRTs is explored through a focus group of five security professionals. They saw an opportunity for organisations to embrace both formal and informal learning as these two learning approaches reinforce each other. While it encourages organisations to leverage their informal learning capability, this paper does not provide specific details on how to enable it.

3.5. Causal analysis

This part of the learning process from incidents received the most attention from researchers. In several studies, respondents supported the need for learning, but researchers found little evidence of thorough investigations to find the underlying causes (Jaatun et al., 2009; Ahmad et al., 2012). Grispos et al. (2015) found seven out of ten respondents said root cause analysis was performed post-incident and all ten saw an opportunity to improve security measures using post-incident analysis.

Shedden et al. (2010) found most research on incident response had been technically focused and there was an opportunity to apply double-loop learning principles to identify underlying causes which could be addressed to strengthen incident response and the security of organisations. Baskerville et al. (2014) found that in one of the three companies studied, double-loop learning was applied after serious incidents, although there are few details on this in the article. In a more recent study, Ahmad et al. (2020) explored the theme of how two teams, security management and incident response, could be better integrated using a double-loop learning model. Using a theoretical incident, they developed a conceptual framework to demonstrate that if the two teams were more integrated, they created better learning opportunities, which improved the security of the organisation. Ahmad et al. (2020) explained how double-loop learning assists organisations in reassessing the assumptions underpinning their information security management system. Lakshmi et al. (2021) found post-incident reviews can update the mental maps incident responders hold in their heads of the causes, which can help them make sense of subsequent incidents.

Evans et al. (2019) adapted the Human Error Assessment and Reduction Technique (HEART) to analyse human error and underlying causes for a year's worth of security incidents reported at a service provider. This data was utilised to calculate human error probabilities. They found the actual likelihood of an incident being caused by human error was lower than the predictions and there would need to be further recalibrations to enable more accurate predictions. Based on the causes identified in the post-incident reports, they found just over half were caused by human error. The article recommends that organisations dig deeper into the causes to identify the conditions which allow errors to occur to enable them to prevent future incidents. Although how organisations investigate the causes of incidents was studied, a deeper analysis into which tools and techniques are the most effective was not covered in the literature.

3.6. Incident response improvements

While most studies covered the benefits to security that could be derived from lessons learned, more attention was paid to improving the incident response team compared to broader changes to security measures (Shedden et al., 2010; Bernsmed and Tøndel, 2013; van der Kleij et al., Dec. 2017; Lakshmi et al., 2021). The Agile retrospectives in Grispos et al. (2017) helped the incident response teams identify incident response related improvements. There is little detail in the literature on how organisations decided on the improvements to make, prioritised resources or tracked progress. There appears to be an implicit assumption that once a team has identified the causes they will naturally implement the improvements required. Whereas the definition of organisational learning by Fiol and Lyles (1985) makes a clear distinction between knowledge and action.

3.7. Overall security improvements

In the company studied by Ahmad et al. (2015), there was no link between post-incident analysis and the information security team, which some respondents in the study saw as a missed opportunity to improve policies based on lessons from incidents. The researchers suggest that the reason could be cost pressures. Line and Albrechtsen (2016), looking at the literature through the lens of ISO/IEC 27035, urged organisations to consider using more adaptive approaches rather than update incident management standards or add more procedures. They recommended further empirical research on adapting industrial safety approaches to managing cyber security incidents.

3.8. Evaluating the learning

While the existing research assessed the learning practices, there was little discussion of the learning process itself and how organisations evaluated how well they were learning. Grispos et al. (2017) trialled lightweight Agile retrospectives in a financial organisation. They introduced two types of retrospectives, the first explored what worked and what did not during the incident response and the second type 'meta-retrospectives' looked back on the effectiveness of implementing the lessons from the incidents. They found the retrospectives did help enhance the identification of post-incident actions to improve security measures (Grispos et al., 2017). Bartnes et al. (2016) found that the organisations they studied did not invest in learning to improve their incident response capability. The study suggested that management commitment is an essential enabler of learning. Although they acknowledged as the organisations had not experienced significant incidents at the time, they perhaps did not yet recognise the risk and therefore the value of investing time in learning.

None of the studies reported that the organisations were exploring how to learn better or had any measures in place to assess their ability to learn and the effectiveness of the improvements made following incidents (Line, 2013; Ahmad et al., 2015). However, it is unclear whether the researchers had sought data on evaluation practices directly. In the Ahmad et al. (2012) study, the company attributed the significant reduction in incidents to their learning practices although how this was measured is not detailed in the paper. In their paper on incident response metrics, Line et al. (2006) proposed using a five orders of feedback model based on work by van Court Hare (1967) on learning from experience. They also suggested incorporating a learning metric across organisations, but neither were empirically tested with organisations.

4. Discussion and research agenda

This section highlights gaps in the current academic literature and, from these, presents avenues for future research and future research questions. There have been few studies into specifically how organisations learn from incidents and many of the articles explicitly call for further research into how organisations can learn

from incidents (Line and Albrechtsen, 2016; Shedden et al., 2010; Tøndel et al., 2014; He et al., 2014b).

4.1. Learning practices

Whilst it is generally agreed that organisations would benefit from improving how they learn from incidents, there is less consensus on how best to achieve this or what is good practice. There is a lack of consensus on a consistent model and a common nomenclature to describe learning, which slows the sharing of ideas and the propagation of good practice. This is not unusual for a relatively new field of research such as cyber security and even in established fields such as management science, the use of models evolves over time (Piazza and Abrahamson, 2020). However, without any coalescing around a shared view of how to assess learning from incidents, the progress of both academic research and the adoption by practitioners will be slower.

There are opportunities to expand the research on learning practices to more industries and countries. In particular, research in less regulated and process-orientated organisations is needed, as the current literature has predominantly focused on the energy, finance and healthcare sectors. For instance, the public sector, technology and critical national infrastructure, where the impact of incidents could be significant, are important to study. Tøndel et al. (2014) also recommended collecting data from more organisations and studying them over a longer time frame.

Future research questions:

- What learning from incident practices are the most commonly used?
- How do organisations in the public sector / technology sector / critical national infrastructure sector learn from incidents?

4.2. Evaluating the learning capability

There has been little attention to-date on how organisations examine how effective they are at learning. It is unclear how organisations should reflect on their own learning capability and continuously improve it. There has been extensive research into learning organisations in the management science field such as Garvin et al. (2008) who recommended enhancing learning capability by creating a supportive learning environment, establishing learning processes and ensuring leadership reinforces learning. However, we are not aware of any studies yet to assess if these approaches would also apply to how cyber security teams can improve their learning from cyber security incidents. To fully understand this, future research needs to assess whether the measures implemented due to lessons from incidents actually reduce the prevalence of future incidents.

In the selected studies, none reported an attempt to measure how learning from incidents improved security or reported the organisations studied evaluated their own ability to learn. Granted as already mentioned, it is difficult to robustly measure incidents, but much of the research conducted is based on an implicit assumption that learning from incidents is positive without seeking explicit evidence to confirm this view. Researchers found that post-incident reviews are typically only conducted on major incidents and not necessarily those with the greatest learning opportunities or time invested in learning from systemic causes (Ahmad et al., 2015; Bartnes et al., 2016). Few studies acknowledge the dilemmas faced by organisations in taking the time and resources to invest in learning. Ahmad et al. (2015) suggested that further research is needed on the competing priorities of security management and incident response teams to understand how these can be balanced to maximise the security of an organisation's technology. Whilst researchers have urged organisations to not only focus on high impact incidents and have wider participation, more research is needed to understand the sweet-spot where investment in learning activities is outweighed by the benefits. This could be studied by comparing organisations or divisions within organisations which have invested different amount of time in learning activities and assessing the impact on the prevalence of incidents. However, the ability to make comparisons would need each organisation to be facing a similar volume of incidents as a baseline.

However, using data to measure the efficacy of learning in reducing the number of future incidents is extremely difficult due to the lack of independent or reliable sources of incident data readily available to academic researchers (Salane and Jay, 2011). As Ryan and Jefferson (2003) concluded "In the information security arena, there is no reliable data upon which to base decisions. Unfortunately, there is unreliable data that is masquerading as reliable data". Even though this study was nearly twenty years ago, not much has changed and similar challenges were found in a study published by Neto et al. (2021). Measuring the impact is a challenge, but perhaps future studies could explore whether the investment in learning led to fewer significant incidents within an organisation based on their own incident metrics on frequency and impact, as well as other performance indicators such as time to restore. Another option would be an exploration of repeat incidents or recurrent types of causes which could indicate improvements were needed to the learning process (for example, several incidents attributed to vulnerabilities being introduced through insecure coding practices). Furthermore, research could be expanded to study the perspective of other stakeholders in the organisation, such as audit and risk committees, business leaders, boards, and regulators.

Organisations need to balance the effort between learning from incidents with responding to them. However, addressing underlying causes, if they have been correctly identified, should reduce the number of incidents. Sveen et al. (2007) and Gonzalez (2005) drawing on systems thinking, map this feedback loop in their systems diagrams of incident response teams but none of the research has studied this trade-off within organisations to understand the optimal balance. Researchers could adopt a design science approach to test how to address the practical challenges of balancing incident response with taking the time to investigate and learn from incidents.

Future research questions:

- How do organisations examine how effective they are at learning from incidents?
- How effective is learning from incidents in reducing the prevalence of future incidents?
- What are the perspectives of stakeholders outside of cyber security incident response teams on the effectiveness of learning from incidents?
- What is the optimal investment of time and resources in learning from incident activities and how is this determined?

4.3. Participation in learning

The studies report the broader organisation is rarely involved with post-incident reviews and reports are often not shared beyond the incident response team and their immediate management (Ahmad et al., 2012; Ahmad et al., 2015). Lukic et al. (2012) found with safety incidents there was a contradiction in people wanted to be included in the learning activities but were concerned about the extra effort. This further highlights the importance of researchers considering the commercial reality of investing time and resources in learning. Except for the work by He et al. (2014a), most studies have concentrated on incident response teams, not the wider organisations outside of IT, who can

also learn from incidents (Russell Vastveit et al., 2015). In the organisation Tatu et al. (2018) studied, they did find user awareness improved following a ransomware incident, however, more studies are required into how the lessons from cyber security incidents can be learnt by the wider organisation. More exploration is required to ascertain the value of different participants in investigating the causes of incidents, including the effects of involving people from other parts of IT, legal, HR, frontline staff and third party experts, as well as the ideal mix of seniority.

Jaatun et al. (2009) pointed to the inadequacy of involving suppliers in post incident learning. Increasingly, organisations depend on an eco-system of suppliers. More research is needed to clarify the relationships that organisations have with suppliers on learning from incidents, including contractual terms, participation in post-incident reviews, sharing of information and implementing the lessons learned. Further case-studies and observation of post-incident reviews would be help to give insights into the challenges organisations face in learning from incidents.

Future research questions:

- What is the value of participants from different functions and levels of seniority in investigating the causes of incidents?
- Which strategies are effective in working with suppliers on learning from incidents?

4.4. Investigating the causes

Studies researching the incident management process have often applied the ISO/IEC 27035 or the NIST SP-800–61 standards. This is good as these standards include lessons learnt as a critical step which has broadened the studies that have included learning in their research. While the standards prescribe learning they fall short of explaining how to effectively extract the lessons and, crucially, to actually use them to reduce the likelihood and impact of incidents in the future (Ahmad et al., 2020). The standards appear to presume organisations are able to identify valuable lessons without guidance on the optimal approach to elicit them. It is as if they imply the lessons are there waiting to be collected and reported, rather than the reality of how the lessons are co-created by those performing the investigation (Lundberg et al., 2009; Lundberg et al., 2010).

To study how lessons are identified, researchers have borrowed models from psychology, management science, or safety science (which also build on organisational learning with the use of double-loop learning) (Jaatun et al., 2009; Shedden et al., 2010; Line et al., 2006; Ahmad et al., 2012; Ahmad et al., 2015; Ahmad et al., 2020). Some take the lessons from existing incident reports to present the findings in a new format (He et al., 2014a; He et al., 2014b; He and Johnson, 2015; He et al., 2015). In cyber security research to-date there is little discussion of the politics and other organisational barriers to effective learning, which have been studied by safety researchers (Schilling and Kluge, 2009; Murphy et al., 2018; Zwetsloot et al., 2017). Grispos et al. (2017) found retrospectives helped as a tool to identify underlying causes, but even though they had this additional causal information it was not employed to improve security and further work is needed to understand what prevented better learning.

There seems to be broad agreement across researchers that tackling the underlying causes is essential to reducing the likelihood of future incidents. Although double-loop learning was frequently mentioned in the studies and its importance in addressing underlying causes, researchers found little evidence of it happening in practice. The literature indicated this shared thread has enabled a theme to emerge that organisations studied are not delving into the underlying causes. Despite the recommended double-loop learning models adapted for cyber security incidents by researchers, most have not been validated through further empirical research in organisations to test eliciting the underlying causes of security incidents. He and Johnson (2015) and He et al. (2015)did evaluate the use of the GSN approach to represent causes in a healthcare provider, but these diagrams were based on the causes already identified by the organisation.

Further investigation is needed to identify the most effective mechanisms to identify lessons. Such studies could evaluate the tools recommended in the CREST guidance (Creasey, 2013) or those tools used in accident investigations. For example, Franco et al. (2019) applied the AcciMap[6] tool to analyse a Denial of Service (DoS) attack on a telecoms operator and found it enabled more lessons to be identified. However, they found it required significant effort to perform and it can be a challenge to avoid blame being assigned during the discussions. Another avenue is to use sociology tools to understand the narratives assigned to risks, which allowed the underlying causes to exist and the incident to occur, similar to safety studies such as the challenger shuttle launch by Vaughan (2016).

Many of the studies recognised the potential value in learning from incidents to tackle underlying issues which could improve the broader security of the organisation. Yet, as the greatest coverage of the learning process was in the causal analysis phase, Ahmad et al. (2020) stated “there has been little recognition of the potential role of incident response as a tool for learning and feedback for wider organisational objectives in particular security management”.

Future research questions:

- What are the most effective mechanisms and tools to identify lessons from incidents?
- In what ways do organisations allow the underlying causes to exist and incidents to occur?

4.5. Organisation structure and culture

Ahmad et al. (2020) suggested there was an opportunity to integrate the incident response and security management teams to improve learning opportunities. However, this may not be a solution for all institutions, as which team structure works best varies according to different organisations depending on a number of factors. The interpretation of the organisation structures by employees and the relationship of their leaders with the team and other stakeholders can have a greater impact than only the official structure (Schein, 2017). More research is needed to better understand optimal organisation governance structures to enable decision making and accountability for improvements based on lessons learned.

It is also recognised that much of the research to-date has centred on the technical aspects of incident management rather than learning (Shedden et al., 2010; Ahmad et al., 2012). The existing research has not established the organisational conditions which determine effective learning such as a culture which values reflection and experimentation (Schein, 2017). Whilst there have been many studies on cyber security culture (Uchendu et al., 2021), these have not addressed how culture impacts an organisation’s ability to learn from incidents. Structured observation and analysis of learning process artefacts could provide insights into how an organisation’s behavioural norms shape their approach to learning from incidents.

Additionally, studies that determine how to overcome barriers that prevent learning would be valuable. One angle to explore this

[6] The AcciMap tool was developed by Rasmussen for accident analysis for more details see Waterson et al. (2017).

through is to identify particular organisations or industries which are learning from incidents and study what has enabled this to happen. Unlike safety's review of High Reliability Organisations (HRO), to understand how some high risk organisations manage to maintain a low level of safety incidents (la Porte, 1996), remarkably there appears to be scant research into organisations which learn from cyber incidents and adapt well. Ahmad et al., (2020) suggested the use of their conceptual framework to study cyber security in HROs.

Future research questions:

- What are the optimal governance structures to enable decision-making and accountability for implementing lessons learned?
- How does culture impact the ability of an organisation to learn from incidents?
- What are the barriers that prevent organisations learning from incidents and how might these be overcome?
- When compared, what enables some organisations / some industries to be more effective at learning from incidents than others?

4.6. Practical implications

Researchers have found little evidence of organisational learning beyond the incident management team improving their processes. The incident management industry standards intentionally allow organisations the flexibility to determine how to implement them and they are centred on incident management rather than how lessons could improve the overall security posture of an organisation. However, if incident management teams do not take accountability for learning from incidents they can find themselves overwhelmed with an increasing number of incidents with rising severity, as the underlying causes are not being addressed (Gonzalez, 2005). In contrast to safety science, how organisations learn to learn from cyber security incidents or the barriers to such learning has not been explicitly studied. It is evident more research in this area would be valuable.

Most of the publications analysed have advocated for a more thorough causal analysis to identify the underlying causes. This is even more important in today's complex and entwined IT systems within the context of an organisation and their IT providers. Organisations need to consider the social aspects of incident investigations and how to facilitate the most beneficial causal analysis (Tavris and Aronson, 2020; Edmondson, 2018). There is a risk organisations assemble a team of people involved in a specific incident and unintentional hindsight bias leads them to miss critical contributory factors (Cook, 1998). Security practitioners can start by evaluating how well their organisation has been learning from incidents using the process outlined in Fig. 1. This will enable them to consider; if the right people are involved (as this impacts the potential lessons learned), how well systematic causes are identified and addressed, and then assess if this helps to reduce the prevalence of incidents.

4.7. Limitations

This study focused on learning from cyber security incidents. It is possible research in other fields of technology, safety, natural disasters and other types of incidents could offer additional insights. Whilst steps were taken to ensure all relevant papers within the cyber security domain were identified, there remains a possibility some were missed due to the reliance on search strings, the indexing, categorisation, and search capabilities of the online databases. We only included articles written in English for which the full text was accessible, which resulted in 11 papers being excluded. Therefore, there is a risk some conclusions about the research in this area were missed. However, considering the number of studies reviewed and the similarity of findings, it is assumed this had a minimal impact on our assertions.

5. Conclusion

Security incidents pose a huge threat to society. There is more data than ever before, and the complex web of systems and suppliers means we are more vulnerable to incidents. The standards used by practitioners recommend learning from incidents, but these documents do not provide much guidance on how to do this well. Yet there has been relatively few studies on this topic in cyber security. This Systematic Literature Review (SLR) and research agenda have structured the existing research into how organisations learn from cyber security incidents and suggested where future research is needed to propel the field forward. By providing an overview of the topic, we hope the analysis of the literature will serve as a valuable resource for those researchers interested in exploring the future research opportunities highlighted.

The literature has more emphasis on acquiring knowledge through post-incident investigations with less attention on the implementation of the lessons. There has been no consistent model applied to assess how organisations learn from incidents. Those studies which have been conducted, recommend organisations should improve learning from incidents with wider participation and sharing of post-incident reports, often suggesting using double-loop learning in the investigations to address systemic causes. The research has shown organisations are not yet benefitting as much as possible from learning from incidents and are not evaluating if their learning is effective.

The analysis of the literature highlighted unanswered questions which were organised into a future research agenda. Fourteen research questions have been suggested and how these could be studied discussed. Further studies are recommended to explore what prevents organisations from understanding the underlying causes to identify the improvements needed and to implement them to reduce the risk of incidents in the future. In addition, approaching it from the opposite side and researching High Reliability Organisations (HRO) that learn well would be beneficial.

Identifying the valuable lessons within an organisation's social and political environment requires effort. Ensuring the lessons lead to useful changes that prevent further incidents requires organisations to evaluate how well they are learning. Further research is needed to identify how organisations can invest in learning to see the greatest benefits. By improving how organisations learn from incidents it is hoped they can reduce the likelihood and impact of cyber security incidents happening in the future. This will help to reduce the risks society faces from its dependence on IT.

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.

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.

Data availability

The data used in this article is not available.

Funding

This research is funded by a PhD scholarship from the Institute of Cyber Security for Society (iCSS), University of Kent (UK).

Appendix A. Literature search queries

All databases were queried in September 2022.

Source	Search query
The ACM Guide to Computing Literature	AllField:("security incident" OR "security incidents" OR "incident response" OR "CSIRT") AND AllField:("organisational learning" OR "organizational learning" OR "lessons learned" OR "lessons learnt")
IEEE Xplore	("security incident" OR "security incidents" OR "incident response" OR "CSIRT") AND ("organisational learning" OR "organizational learning" OR "lessons learned" OR "lessons learnt")
ScienceDirect	("security incident" OR "security incidents" OR "incident response" OR "CSIRT") AND ("organisational learning" OR "organizational learning" OR "lessons learned" OR "lessons learnt")
SpringerLink	("security incident" OR "security incidents" OR "incident response" OR "CSIRT") AND ("organisational learning" OR "organizational learning" OR "lessons learned" OR "lessons learnt")
ProQuest (One Literature and Publicly Available Content Database NOT the Global Theses and Dissertations)	("security incident" OR "security incidents" OR "incident response" OR "CSIRT") AND ("organisational learning" OR "organizational learning" OR "lessons learned" OR "lessons learnt")
Scopus	("security incident" OR "security incidents" OR "incident response" OR "CSIRT") AND ("organisational learning" OR "organizational learning" OR "lessons learned" OR "lessons learnt")
Wiley Online Library	("security incident" OR "security incidents" OR "incident response" OR "CSIRT") AND ("organisational learning" OR "organizational learning" OR "lessons learned" OR "lessons learnt")
Web of Science Core Collection	("security incident" OR "security incidents" OR "incident response" OR "CSIRT") AND ("organisational learning" OR "organizational learning" OR "lessons learned" OR "lessons learnt")

References

Ahmad, A., Hadgkiss, J., Ruighaver, A.B., 2012. Incident response teams - Challenges in supporting the organisational security function. Comput. Secur. 31 (5), 643–652. doi: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. doi:10.1016/j.ijinfomgt.2015.08.001.

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. doi:10.1002/asi.24311.

Argote, L., Levine, J.M., 2017. The Oxford Handbook of Group and Organizational Learning. Oxford University Press doi:10.1093/oxfordhb/9780190263362.001.0001.

Argote, L., Ophir, R., 2017. Intraorganizational learning. In: in The Blackwell Companion to Organizations. Blackwell Publishing Ltd, Oxford, UK, pp. 181–207. doi:10.1002/9781405164061.ch8.

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

Argyris, 1990. Overcoming Organisational Defenses: Facilitating Organisational Learning. Allyn and Bacon, Needham Heights, MA.

Argyris, C., 1976. Single-loop and double-loop models in research on decision making. Adm. Sci. Q. 21 (3), 363–375. doi:10.2307/2391848.

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. doi:10.1016/j.cose.2016.05.004.

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. doi:10.1016/j.im.2013.11.004.

Beck K. et al., "Manifesto for agile software development," 2001. Accessed May 04, 2022: https://agilemanifesto.org/

Bernsmed, K., Tøndel, I.A., 2013. Forewarned is forearmed: indicators for evaluating information security incident management. In: Proceedings of the 7th International Conference on IT Security Incident Management and IT Forensics, IMF, pp. 3–14. doi:10.1109/IMF.2013.14 2013.

Boell, S., 2014. A hermeneutic approach for conducting literature reviews and literature searches. Aisel. Aisnet. Org. 34, 257–286. Accessed: May 23, 2022. Available https://aisel.aisnet.org/cais/vol34/iss1/12/ .

Brostoff, S., Sasse, M.A., 2001. Safe and sound: a safety-critical approach to security. Proceedings of the Workshop on New Security Paradigms doi:10.1145/508171.508178.

Cichonski, P., 2012. Computer security incident handling guide. National Institute of Standards and Technology doi:10.6028/NIST.SP.800-61r2.

Cockram, T.J., Lautieri, S.R., 2007. Combining security and safety principles in practice, pp. 159–164. doi:10.1049/cp:20070458.

Connolly, L.Y., Wall, D.S., 2019. The rise of crypto-ransomware in a changing cybercrime landscape: taxonomising countermeasures. Comput. Secur. 87. doi:10.1016/j.cose.2019.101568.

Cook, R.I., 1998. How Complex Systems Fail. University of Chicago, Chicago IL.

Cooke, D.L., 2003. Learning from incidents. 21st System Dynamics Conference 3 (22), 1–30.

Creasey, J. 2013. Cyber security incident response guide version 1. Available: http://www.crest-approved.org/

Curado, C., 2006. Organisational learning and organisational design. Learn. Organ. 13 (1), 25–48. doi:10.1108/09696470610639112/FULL/HTML.

de Zan, T., 2019. Mind the gap: the cyber security skills shortage and public policy interventions. Oxford. Accessed: Dec. 04, 2022. Available: https://www.ctga.ox.ac.uk/article/mind-gap-cyber-security-skills-shortage-and-public-policy-interventions.

Drupsteen, L., Groeneweg, J., Zwetsloot, G.I.J.M., 2013. Critical steps in learning from incidents: using learning potential in the process from reporting an incident to accident prevention. Int. J. Occup. Saf. Ergon. 19 (1), 63–77. doi:10.1080/10803548.2013.11076966.

Easterby-Smith, M., Lyles, M.A., 2012. Handbook of Organizational Learning and Knowledge Management, 2nd ed. John Wiley & Sons Ltd, Chichester Accessed: Feb. 23, 2023. Available: [PDF] nibmehub.com.

Edmondson, A.C., 2018. The Fearless organization: Creating psychological Safety in the Workplace For learning, innovation, and Growth. John Wiley & Sons.

ESReDA, 2015. Guidelines for preparing a training toolkit in event investigation and dynamic learning. Available: www.esreda.org

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. doi:10.1016/j.cose.2018.09.002.

Fiol, C.M., Lyles, M.A., 1985. Organizational Learning. Source Acad. Manag. Rev. 10 (4), 803–813.. Available https://www.jstor.org/stable/258048?seq=1&cid=pdf.

Franco, Z. et al., 2019. Applying generic accimap to a DDOS attack on a western-european telecom operator. Proceedings of the 16th ISCRAM Conference, 528–535.

Garvin, D.A., Edmondson, A.C., Gino, F. 2008. Is yours a learning organization? Harvard business review, 86(3). Available: www.hbr.org

Gonzalez, J.J., 2005. Towards a cyber security reporting system-a quality improvement process. Lect. Notes Comput. Sci. 3688, 368–380. doi:10.1007/11563228_28.

Grispos, G., Glisson, W.B., Storer, T., 2014. Rethinking security incident response: the integration of agile principles. In: Proceedings of the20th Americas Conference on Information Systems.

Grispos, G., Glisson, W.B., Storer, T., 2015. Security incident response criteria: a practitioner's perspective. In: Proceedings of the 21st Americas Conference on Information Systems. Accessed: Dec. 11, 2022. Available:.

Grispos, G., Glisson, W.B. and Storer, T., 2019. How good is your data? Investigating the quality of data generated during security incident response investigations. Proceedings of The 52nd Hawaii International Conference on System Sciences. doi:10.24251/hicss.2019.859.

Grispos, G., Glisson, W.B., Storer, T., 2017. Enhancing security incident response follow-up efforts with lightweight agile retrospectives. Digit Investig. 22, 62–73. doi:10.1016/j.diin.2017.07.006.

Große, C., Nyman, M., Sundberg, L., 2020. Information technology consulting firms' readiness for managing information security incidents. In: Communications in Computer and Information Science, 1221. CCIS, Springer, pp. 48–73. doi:10.1007/978-3-030-49443-8_3.

Gusenbauer, M., Haddaway, N.R., 2020. Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of google scholar, pubmed, and 26 other resources. Res Synth Methods 11 (2), 181–217. doi:10.1002/jrsm.1378.

He, Y., Johnson, C., 2015. Improving the redistribution of the security lessons in healthcare: an evaluation of the generic security template 84 (11), 941–949. doi: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. Inf. Health Soc. Care 42 (4), 393–408. doi:10.1080/17538157.2016.1255629.
He, Y., Johnson, C., Lu, Y., Lin, Y., 2014a. Improving the information security management: an industrial study in the privacy of electronic patient records. In: Proceedings of the IEEE Symposium on Computer-Based Medical Systems, pp. 525–526. doi:10.1109/CBMS.2014.121.
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 6th International Conference on Computer Science and Information Technology, CSIT, pp. 178–188. doi:10.1109/CSIT.2014.6805998.
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). doi:10.1186/s40493-015-0016-2.
He, Y., Zamani, E.D., Lloyd, S., Luo, C., 2022. Agile incident response (AIR): improving the incident response process in healthcare. Int. J. Inf. Manag. 62. doi:10.1016/j.ijinfomgt.2021.102435.
Hendrick, K., Benner Jr, L., Benner, L., 1986. Investigating accidents with step, 13. CRC Press.
Horne, C.A., Maynard, S.B. , Ahmad, A., 2020. Towards governance of information security incident response. Proceedings of the 15th Pre-ICIS Workshop on Information Security and Privacy. Available: https://aisnet.org/general/custom.asp?page=SeniorScholarBasket
Huber, G.P., 1991. Organizational learning: the contributing processes and the literatures. Organ. Sci. 2 (1), 88–115. Available https://www.jstor.org/stable/2634941.
ISO - ISO/IEC 27035-3: - information technology — information security incident management — part 3: guidelines for ict incident response operations. Accessed Feb. 01, 2022. https://www.iso.org/standard/74033.html
Jaatun, M.G., Bartnes, M., Tøndel, I.A., 2016. Zebras and Lions: better incident handling through improved cooperation. Commun. Comput. Inf. Sci. 648, 129–139. doi:10.1007/978-3-319-49466-1_9.
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. Crit. Infrastruct. Prot. 2 (1–2), 26–37. doi:10.1016/j.ijcip.2009.02.004.
Kaur, M., van Eeten, M., Janssen, M., Borgolte, K., Fiebig, T., 2021. Human factors in security research: lessons learned from 2008 to 2018. Available: http://arxiv.org/abs/2103.13287
Khan, N.F., Yaqoob, A., Khan, M.S., Ikram, N., 2022. The cybersecurity behavioral research: a tertiary study. Comput. Secur. 120, 102826. doi:10.1016/j.cose.2022.102826.
Kitchenham, B., Brereton, P., Li, Z., Budgen, D., Burn, A., 2010. Repeatability of systematic literature reviews doi:10.1049/ic.2011.0006.
Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., Halgand, Y., 2015. A survey of approaches combining safety and security for industrial control systems. Reliab. Eng. Syst. Saf. 139, 156–178. doi:10.1016/j.ress.2015.02.008.
la Porte, T., 1996. High reliability organizations- unlikely, demanding and at risk. J. Contingencies Crisis Manag. 4 (2), 60–71.
Lakshmi, R., Naseer, H., Maynard, S., Ahmad, A., 2021. Sensemaking in Cybersecurity Incident Response- The Interplay of Organizations, Technology and Individuals, 29. ECIS 2021 Research-in-Progress Papers Accessed: Dec. 09, 2022. Available: https://aisel.aisnet.org/ecis2021_rip/29 .
Le Coze, J.C., 2013. What Have We Learned About Learning from Accidents? Post-Disasters Reflections. Elsevier doi:10.1016/j.ssci.2012.07.007.
Line, M.B., Albrechtsen, E., 2016. Examining the suitability of industrial safety management approaches for information security incident management. Inf. Comput. Secur. 24 (1), 20–37. doi:10.1108/ICS-01-2015-0003.
Line, M.B., Albrechtsen, E., Johnsen, S.O., Longva, O.H., Hillen, S., 2006. Monitoring of incident response management performance. In: Proceedings of the International Conference on IT-Incident Management & IT-Forensics. Accessed: Dec. 11, 2022. Available.
Line, M.B., Tøndel, I.A., Jaatun, M.G., 2016. Current practices and challenges in industrial control organizations regarding information security incident management - Does size matter?. Information security incident management in large and small industrial control organizations Int. J. Crit. Infrastruct. Prot. 12, 12–26. doi:10.1016/j.ijcip.2015.12.003.
Line, M.B., 2013. A case study: preparing for the smart grids - Identifying current practice for information security incident management in the power industry. In: Proceedings of the 7th International Conference on IT Security Incident Management and IT Forensics, IMF, pp. 26–32. doi:10.1109/IMF.2013.15 2013.
Lisova, E., Šljivo, I., Čaušević, A., 2019. Safety and security co-analyses: a systematic literature review. IEEE Syst. J. 13 (3), 2189–2200. doi:10.1109/JSYST.2018.2881017.
Littlejohn, A., Margaryan, A., Vojt, G., Lukic, D., 2017. Learning from incidents questionnaire (LFIQ): the validation of an instrument designed to measure the quality of learning from incidents in organisations. Saf. Sci. 99, 80–93. doi:10.1016/J.SSCI.2017.02.005.
Lukic, D., Littlejohn, A., Margaryan, A., 2012. A framework for learning from incidents in the workplace. Saf. Sci. 50 (4), 950–957. doi:10.1016/j.ssci.2011.12.032.
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. Accid. Anal. Prev. 42 (6), 2132–2139. doi:10.1016/J.AAP.2010.07.003.
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. doi:10.1016/J.SSCI.2009.01.004.
Moher, D., Liberati, A., Tetzlaff, J., Altman, D.G., 2009. Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. BMJ Online 339 (7716), 332–336. doi:10.1136/BMJ.B2535.
Moore, S., 2022. Gartner identifies three factors influencing growth in security spending Available: https://www.gartner.com/en/newsroom/press-releases/2022-10-13-gartner-identifies-three-factors-influencing-growth-i#:%E2%88%BC:text=Security/.
Murphy, V.L., Littlejohn, A., Rienties, B., King, S., Bryden, R., 2018. Where does information on incidents come from? In: Proceedings of the Society of Petroleum Engineers - SPE International Conference and Exhibition on Health, Safety, Security, Environment, and Social Responsibility, p. 2018. doi:10.2118/190526-ms.
Murphy, V.L., Littlejohn, A., Rienties, B., 2021. Learning from incidents: applying the 3-P model of workplace learning. J. Workplace Learn. doi:10.1108/JWL-04-2021-0050.
NCSC, Cyber security longitudinal survey wave 1, 2022. Accessed: May 26, 2022. Available: https://www.gov.uk/government/publications/cyber-security-longitudinal-survey-wave-one/cyber-security-longitudinal-survey-wave-1
Neto, N.N., Moraes De Paula, A.G., Borges, N.M, 2021. Developing a global data breach database and the challenges encountered. J. Data Inform. Qual. 13 (1). doi:10.1145/3439873.
Piazza, A., Abrahamson, E., 2020. Fads and fashions in management practices: taking stock and looking forward. Int. J. Manag. Rev. 22 (3), 264–286. doi:10.1111/ijmr.12225.
Russell Vastveit, K., Boin, A., Njå, O., 2015. Learning from incidents: practices at a Scandinavian refinery. Saf. Sci. 79, 80–87. doi:10.1016/j.ssci.2015.05.001.
Ryan, J.J.C.H., Jefferson, T.I., 2003. The use, misuse, and abuse of statistics in information security research. In: Proceedings of the ASEM National Conference.
Salane, D.E., Jay, J., 2011. Are large scale data breaches inevitable? Center for cybercrime studies, 9. Cyber Infrastructure Protection, pp. 51–80.
Schein, E.H., 2017. Organizational Culture and Leadership, 5th ed. John Wiley & Sons inc, Hoboken, New Jersey.
Schilling, J., Kluge, A., 2009. Barriers to organizational learning: an integration of theory and research. Int. J. Manag. Rev. 11 (3), 337–360. doi: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 ed 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 doi:10.4225/75/57b6771734788.
Shedden, P., Ahmad, A., Ruighaver, A.B., Shedden, P., Ahmad, A., Informal learning in security incident response teams, 2011, p 1. Available: http://aisel.aisnet.org/acis2011/37.
Silverman, D., 2017. How was it for you? The interview society and the irresistible rise of the (poorly analyzed) interview. Qual. Res. 17 (2), 144–158. doi:10.1177/1468794116668231.
Sveen, F.O., Sarriegi, J.M., Rich, E., Gonzalez, J.J., 2007. Toward viable information security reporting systems. Manag. Comput. Secur. 15 (5), 408–419. doi:10.1108/09685220710831143.
Swuste, P., van Gulijk, C., Groeneweg, J., Zwaard, W., Lemkowitz, S., Guldenmund, F., 2020. From clapham junction to macondo, deepwater horizon: risk and safety management in high-tech-high-hazard sectors: a review of English and Dutch literature: 1988–2010. Saf. Sci. 121, 249–282. doi:10.1016/j.ssci.2019.08.031.
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. doi:10.1016/J.COSE.2014.05.003.
Tatu, T., Ament, C., Jaeger, L., 2018. Lessons learned from an information security incident: a practical recommendation to involve employees in information security. In: Proceedings of the 51stHawaii International Conference on System Sciences doi:10.24251/hicss.2018.471.
Tavris, C., Aronson, E., 2020. Mistakes Were Made (But Not By Me): Why We Justify Foolish Beliefs, Bad Decisions and Hurtful acts, 3rd Ed. Pinter & Martin Ltd.
The Assurance Case Working Group (ACWG) , 2021. Goal structuring notation community standard version 3 the assurance case working group (ACWG). SCSC-141C, 2021. Accessed: Feb. 09, 2022. Available: https://scsc.uk/scsc-141C
Tuttle, H., 2022. Cyber landscape tuttle. Risk Manag. 69 (1), 18–23. Feb. 01 Accessed: Dec. 11, 2022. Available https://www.rmmagazine.com/articles/article/2022/02/01/2022-cyber-landscape.
Uchendu, B., Nurse, J.R.C., Bada, M., Furnell, S., 2021. Developing a cyber security culture: current practices and future needs. Comput. Secur. doi:10.1016/j.cose.2021.102387.
“ISO - ISO/IEC 27035-1:2016 - Information technology — Security techniques — Information security incident management — Part 1: principles of incident management.” https://www.iso.org/standard/60803.html (accessed Nov. 18, 2021).
“ISO - ISO/IEC 27035-2: - information technology — security techniques — information security incident management — part 2: guidelines to plan and prepare for incident response.” https://www.iso.org/standard/62071.html (accessed Nov. 18, 2021).
van Court Hare, 1967. System Analysis: A Diagnostic Approach. Brace & World, Harcourt. ISBN: 10: 1114236500
van der Kleij, R., Kleinhuis, G., Young, H., 2017. Computer security incident response team effectiveness: a needs assessment. Front. Psychol. 8. doi:10.3389/fpsyg.2017.02179.
Vastveit, K.R., Boin, A., Njå, O., 2015. Learning from incidents: practices at a scandinavian refinery. Saf. Sci. 79, 80–87. doi:10.1016/J.SSCI.2015.05.001.

Vaughan, D., 2016. The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA, Enlarged Edition. The University of Chicago Press, Ltd, London.

Waterson, P., Jenkins, D.P., Salmon, P.M., Underwood, P., 2017. 'Remixing rasmussen': the evolution of accimaps within systemic accident analysis. In: Appl. Ergon., 59, pp. 483–503. doi:10.1016/j.apergo.2016.09.004.

World Economic Forum, The global risks report 2022 17th (Ed.), 2022. Accessed: Feb. 01, 2022. https://www.weforum.org/reports/global-risks-report-2022.

Yin, R., 2018. Case Study Research and applications: Design and Methods, 6th ed. SAGE Publications, Inc..

Zhang, H., Babar, M.A., Tell, P., 2011. Identifying relevant studies in software engineering. Inf. Softw. Technol. 53 (6), 625–637. doi:10.1016/j.infsof.2010.12.010.

Zietsma, C., Ziet, C., Branzei, O., 2002. The war of the woods: facilitators and impediments of organizational learning processes. Br. J. Manag. 13 (S2), S61–S74. doi:10.1111/1467-8551.13.s2.6.

Zwetsloot, G.I.J.M., Kines, P., Ruotsala, R., Drupsteen, L., Merivirta, M.L., Bezemer, R.A., 2017. The importance of commitment, communication, culture and learning for the implementation of the zero accident vision in 27 companies in Europe. Saf. Sci. 96, 22–32. doi:10.1016/j.ssci.2017.03.001.

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 an Associate Professor 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 Assistant 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.