



Cultural, organisational, and individual factors contributing to cyber incident reporting: A systematic literature review

Rick van der Kleij^{a,b,*}, Olivier Spinnler^a, Julia Broderick-Hale^a, Katie Hendriks^c,
Anthonie Drenth^c, Joshua van Wijgerden^c

^a Netherlands Organisation for Applied Scientific Research (TNO), P.O. Box, The Hague, 96864, the Netherlands

^b Avans University of Applied Sciences, Onderwijsboulevard 215, 's-Hertogenbosch, 5223 DE, the Netherlands

^c National Cyber Security Centre (NCSC), Turfmarkt 147, The Hague, 2511 DP, the Netherlands

ARTICLE INFO

Keywords:

Cybersecurity culture
Cyber resilience
Security behaviour
Human factors
Incident handling

ABSTRACT

Incident reporting behaviour is a critical yet underexplored human factor in organisational cyber resilience, shaping how organisations learn from incidents and adapt to evolving digital threats. This systematic literature review synthesises evidence from 106 peer-reviewed studies across cyber resilience, healthcare, and aviation to examine how cultural, organisational, technological, and psychological factors influence employees' reporting behaviour. The review identifies five thematic clusters of antecedents—organisational, psychological, technical, social, and motivational—and shows how their interaction can either facilitate or hinder incident reporting behaviour. Building on these findings, we propose a novel, integrative multilevel conceptual model that extends the Cybersecurity Culture–Behaviour (CSCB) framework of Sutton and Tompson (2024) by incorporating a widely used behaviour-change framework, perceived consequences of reporting, and the moderating roles of incident characteristics and reporter attributes. The results highlight the importance of multilevel, human-centred interventions that foster psychological safety, provide timely and meaningful feedback, and align managerial practices with principles of a just culture. This study advances understanding of incident reporting behaviour as a socio-technical behaviour and offers a unifying framework for designing interventions to strengthen cyber resilience through improved human reporting practices.

1. Introduction

Digitalisation offers tremendous opportunities for society and the economy. Automation and digital tools streamline operations, reduce manual labour, and accelerate business processes. However, digitalisation also increases cybersecurity risks by providing more opportunities for cybercriminals to exploit digital systems, devices, and data flows. Moreover, due to the interconnected nature of processes within the digital ecosystem, the consequences of a cyber incident can affect anyone—even when the incident initially appears distant. In this way, digitalisation also increases societal vulnerability.

The likelihood of cyber incidents is increasing across sectors, including the business domain. What qualifies as a cyber incident may vary across organisations, but generally, an incident is defined in the literature as an event that has the capacity to cause significant harm to business operations, finances, or reputation (Furnell et al., 2020; World Economic Forum, 2024, p. 5). Not only is the likelihood of cyber

incidents increasing, but companies, institutions, and government bodies are also under constant attack. These attacks are often carried out by cybercriminals seeking financial gain, but may also involve sabotage, espionage, and subversion by foreign state actors. Intelligence agencies and criminal actors actively target digital infrastructure and data, as highlighted in the National Security Strategy of the Kingdom of the Netherlands (NCTV, 2023). A malicious actor can cause extensive damage by gaining control of a system or by stealing, altering, or deleting data.

Being digitally resilient means ensuring secure systems and keeping hackers at bay. It also refers to the ability to recover quickly and effectively from an attack under any circumstances. In addition, resilience entails the ability to learn from such incidents and to adapt systems and practices to reduce the likelihood of recurrence. By learning from incidents, organisations can strengthen their defences and protect themselves against future threats (Van der Kleij, 2025).

In this paper, we adopt the term cyber resilience over cybersecurity.

* Corresponding author. Netherlands Organisation for Applied Scientific Research (TNO), P.O. Box, 96864, The Hague, the Netherlands.

E-mail address: Rick.vanderkleij@tno.nl (R. van der Kleij).

<https://doi.org/10.1016/j.chb.2026.109127>

Received 15 April 2026; Received in revised form 19 June 2026; Accepted 11 July 2026

Available online 14 July 2026

0747-5632/© 2026 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

Although these concepts are often used interchangeably, cyber resilience reflects a broader perspective (Ahmed et al., 2023; Araujo et al., 2024; Linkov & Kott, 2019; World Economic Forum, 2024). Cybersecurity typically focuses on preventing harm caused by disruption, failure, or misuse of IT systems (see, for instance, Gisladdottir et al., 2017). It often evokes the metaphor of a fortress: an impenetrable barrier against external attacks and disruptions (Van Boheemen et al., 2020). In contrast, cyber resilience encompasses not only the prevention of harm, but also the ability to seize unexpected, positive opportunities to enhance security, as well as to respond to, recover from, and adapt to adverse events or activities (Hollnagel, 2022). It is therefore a more dynamic concept than cybersecurity, acknowledging that absolute security is unattainable (Kott & Linkov, 2021). Consequently, organisations must operate under the assumption that significant cyber incidents will occur (Van der Kleij, 2025).

Four capabilities are commonly central to definitions of cyber resilience: preparation, response, recovery, and adaptation (National Research Council, 2012). Preparation involves anticipating disruptions and strengthening preventive measures. Response aims to maintain critical functions during a crisis, emphasising monitoring, communication, and collaboration. Recovery seeks to restore systems to their pre-crisis state, including rebuilding reputation and performance. Adaptation uses lessons learned to improve the system's resilience to future challenges, encouraging innovation and potential transformation (Van der Kleij, 2025). Ideally, the adaptation phase is followed by a transition back to the preparation phase (Eken et al., 2024). In line with NIST and systems-engineering definitions, a 'system' in this context refers to an integrated whole of hardware, software, networks, data, processes, and people working together to deliver essential functions and services (ISO/IEC/IEEE 15288). The idea is that firewalls, antivirus software, proxy servers, and so forth (technology) mean little if they are not used correctly (process) and if the right team is not in place to operate them (people). In this paper, we focus specifically on the system's capacity for adaptation, namely, the ability to modify system components based on insights gained from incidents or near misses to achieve incremental improvements in resilience (see also, Häring et al., 2016).

Despite its importance, there is limited research on how organisations can enhance their adaptive capacity in the context of cyber resilience. A key assumption is that incident experiences play a key role in this process (Patterson et al., 2023). By learning from incidents, organisations can strengthen their defences and protect themselves against future threats. Organisations can learn from their own incident experiences, but they can also attempt to learn from incidents that have occurred in other organisations (Verweijen, 2022). The advantage of such vicarious learning is that organisations do not suffer the negative impact of an incident themselves yet can still draw lessons from others to improve their own cyber resilience.

A crucial factor in the ability to learn from incidents is incident reporting behaviour (IRB). IRB refers to the actions and practices of individuals within an organisation related to reporting incidents, such as accidents, near misses, hazardous situations, deviations from procedures, or other safety and security risks. This behaviour also includes reporting intuitive suspicions that something may be wrong, even in the absence of concrete evidence. Incident reporting is a cornerstone of effective cyber resilience management. Both incidents and near-incidents serve as wake-up calls for organisations, highlighting security weaknesses and offering opportunities for learning (Patterson et al., 2024). Although IRB is often framed as an internal organisational process, its implications extend far beyond the boundaries of a single entity. Timely incident reporting across organisations is critical when the first signs of a cyberattack emerge. In 2021, VDL Group, an industrial and manufacturing company based in the Netherlands, became the target of such an attack. Amid the ensuing crisis, VDL Group proactively reached out to other companies that were potentially at risk, providing early warnings and enabling them to take preventive measures. This act of

inter-organisational communication not only helped VDL Group regain control of its own situation but may have also shielded others from similar harm. This example illustrates how cyber incident reporting—beyond governmental channels and into the industrial ecosystem—amplifies cyber resilience. It enables faster containment, reduces duplication of effort, and allows national cybersecurity resources to be allocated more strategically. Hence, this case underscores the importance of IRB as a mechanism for collective defence. Organisations that engage in proactive reporting not only protect themselves but contribute to a broader security posture across sectors.

Despite these benefits, the widespread adoption of proactive incident reporting faces significant challenges. Organisations struggle with fragmented and overlapping regulatory requirements, unclear thresholds for what constitutes a reportable incident, and concerns about legal liability and reputational risk. Additional barriers include the operational burden of compliance, limited incident response maturity, and uncertainty about confidentiality and data-sharing mechanisms (Marotta & Madnick, 2023). These challenges may create hesitation and inconsistency in reporting practices, even as policymakers and industry emphasise its critical role in improving cybersecurity resilience.

A further challenge in the ability to learn from incidents lies in the human element. Notwithstanding the fact that receiving security reports from employees provides organisations and industrial ecosystems with many opportunities for improvement, in practice, employees often do not report cyber incidents, or do not report them consistently (Briggs et al., 2017). Recent research conducted by Crayon (2025) indicates that while a significant majority of employees (83%) report being able to recognize suspicious digital activities—such as phishing emails—this awareness does not consistently translate into action. In practice, nearly one-third (29%) of respondents do not report their suspicions to IT departments or supervisors. This lack of follow-up may result in missed opportunities to detect and mitigate cyber threats in a timely manner, potentially increasing organisational vulnerability.

Underreporting can result from several factors, including inconvenient reporting processes, ignorance of what constitutes a reportable event and fear of punishment (Ebbers et al., 2025, 2026). However, underreporting is not merely influenced by procedural or psychological factors; it is also deeply influenced by the cultural organisational context in which employees operate. For instance, Patterson and colleagues (2023) and Ebert et al. (2023) emphasise the influence of cultural factors in promoting learning from cyber incidents, such as having an open culture or fostering transparency. Understanding these cultural pathways is therefore crucial for designing interventions that foster more transparent, responsive, and resilient reporting practices.

1.1. The current research

In recent years, several studies have examined IRB, with a primary focus on phishing and safety incidents. Several predictors of reporting behaviour emerged across these studies, many of which are psychological in nature (Ebbers et al., 2025, 2026). For example, building on prior research into phishing detection and reporting, Kwak et al. (2020) identified several psychological constructs that significantly influence spear-phishing email reporting behaviour. Among these, self-efficacy emerged as a critical determinant; individuals who possess a strong belief in their ability to recognize and report phishing attempts, as well as to implement protective measures, demonstrate a markedly higher likelihood of engaging in reporting behaviours. This finding aligns with broader theories of behavioural intention, which emphasise the role of perceived competence in shaping proactive security actions. In addition, cyber risk beliefs—defined as users' perceptions of the inherent risks associated with their online activities—were shown to exert both direct and indirect effects on reporting intentions. Indirect pathways operated through mediating factors such as self-efficacy, anticipated negative consequences of failing to act, and self-monitoring tendencies. This suggests a complex interplay between cognitive risk appraisal and

behavioural confidence in shaping reporting behaviour.

Recent studies have also examined the factors that influence safety and security culture. For example, Sutton and Tompson (2024) conducted a rapid evidence assessment synthesising 59 studies on cybersecurity culture (CSC). They define CSC as the ‘knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest themselves in people’s behaviour with information technologies (see also ENISA, 2017, p. 5).’ Their findings suggest that CSC should be understood both in the context of the wider organisational culture as well as in the shared employee understanding of CSC that leads to behaviour. Notably, however, the rapid evidence assessment did not include studies specifically addressing IRB.

Similarly, Patterson and colleagues (2023) systematically reviewed research on learning from cyber incidents in organisations. They conclude that, although there have been many studies on CSC, research has not addressed how CSC impacts an organisation’s ability to learn from incidents. They therefore highlight the need for further research examining this relationship.

Building on these observations, the present study aims to review the literature on how CSC influences IRB, following the systematic literature review (SLR) approach (e.g., Estay et al., 2020). An SLR is a structured method for collecting, evaluating, and synthesising scientific research. Its aim is to provide a comprehensive overview of existing knowledge on a specific topic, question, or issue through a series of predefined steps. As such, it helps to obtain an objective and thorough understanding of the available literature and offers a solid foundation for further research.

To guide the review, this paper addresses five research questions:

- 1. How is IRB defined in the literature?
- 2. Why do employees underreport cyber incidents?
- 3. What factors encourage cyber incident reporting?
- 4. How do organisational cultural factors influence IRB?
- 5. What is the impact of IRB on organisational cyber resilience?

This review synthesises academic literature in which three domains consistently emerged—cybersecurity, healthcare, and aviation—as predominant contexts for incident reporting. Although these domains differ in context, they share key characteristics as safety-critical systems in which incident reporting enables organisational learning and risk mitigation. We assume that IRB is a socio-technical behaviour shaped by common psychological, organisational, and technical mechanisms, allowing insights from mature reporting domains to inform the emerging cybersecurity context. Our research consisted of three steps: first, we selected relevant literature and thematically analysed IRB and CSC; second, we critically analysed the influence of cultural factors on IRB; third, we constructed a conceptual model to help organize the findings from the literature review into a coherent whole, thereby clarifying patterns and connections between concepts.

2. Methods

2.1. Systematic literature review

An SLR was conducted to provide a comprehensive and unbiased synthesis of existing research on the topic of IRB within organisations. As mentioned, by following a structured and transparent methodology, SLR ensures the inclusion of relevant studies, minimises bias, and enhances the reliability of findings (Khan et al., 2022). This approach allows researchers to identify trends, gaps, and key insights within the literature, thereby informing future research directions and contributing to the advancement of knowledge in the field by offering a thorough and methodical evaluation of the available evidence (Snyder, 2019). The SLR protocol that was followed is depicted in Table 1. A protocol provides clear guidelines for interpreting and categorising information collected while reading research (Brown et al., 2003).

Table 1
SLR protocol.

SLR parameter	Description
Context for research	By learning from incidents, organisations can strengthen their defences and protect themselves against future threats. A crucial factor in the ability to learn from incidents is IRB.
SLR relevance	The SLR helps to obtain an objective and thorough understanding of the available literature and offers a solid foundation for further research.
Unit of analysis	Published articles in peer-reviewed journals and conference proceedings.
Research questions	1 How is IRB defined in the literature? 2 Why do employees underreport cyber incidents? 3 What factors encourage cyber incident reporting? 4 How do organisational cultural factors influence IRB? 5 What is the impact of IRB on organisational cyber resilience?
Source of data	Scopus
Search strategy	a Use the search engine with the title keyword combinations to obtain a baseline sample. b Filter the baseline sample by using the Inclusion criteria and ASReview to obtain the synthesis sample.
Keyword search combinations	Incident AND report AND (behaviour OR culture)
Inclusion criteria	a Written in English, b With an abstract, c Full text is open access, available through institutional access, or provided by researchers that were contacted for this purpose, d Specifically mentioned one of the topics of interest in the abstract (thematic relevance).

This SLR diverges from the ‘traditional’ methodology through the integration of artificial intelligence (AI) at two critical stages: first, expediting the identification of pertinent studies from a large corpus of search results; and second, enhancing the efficiency of analysing an extensive body of literature. It should be noted that the AI systems were deployed with enterprise data protection on organisation-managed infrastructure within the European Union, ensuring compliance with regional data protection regulations (e.g., GDPR).

2.2. Choice of academic search engine

Scopus was chosen as an initial starting point for this research for the following reasons. Firstly, Scopus provides research papers from approximately 26k active peer-reviewed journals covering a diverse and wide array of disciplines (Elsevier, n.d.; Prancutė, 2021). Cyber resilience is multidisciplinary involving cybersecurity, psychology, law & policy, social sciences, and more. Therefore, Scopus was deemed an excellent resource for conducting research on this topic. In addition, there are regular updates and re-evaluations of indexed content to ensure accuracy, along with the inclusion of a wide range of document types, including articles, reviews, conference papers, and book chapters (Elsevier, n.d.).

2.3. Search strategy

The search query employed was: incident AND report AND (behaviour OR culture). This formulation is deliberately broad to capture a wide range of literature across multiple domains. A conscious decision was made not to restrict the scope to a specific field, such as cybersecurity, information security, or incident management, despite its relevance. This approach is based on the premise that the conceptualisation of an ‘incident’ shares commonalities across various sectors (Basnyat et al., 2006). Moreover, the cultural factors that influence individuals’ attitudes toward incident reporting such as fear of blame, perceived organisational support, and norms are not inherently domain specific. Therefore, a cross-disciplinary perspective is deemed essential to comprehensively understand the dynamics of IRB. For instance, Serrat

(2017) emphasises that incidents regardless of domain are shaped by cognitive, emotional, and behavioural responses, and that these responses are deeply embedded in organisational culture and individual psychology. This supports the idea that the psychological and cultural dimensions of incident reporting are universally applicable across domains, and that insights from diverse fields can meaningfully inform research in this area.

To ensure transparency and completeness, we report the results of the search, identification, and inclusion process in accordance with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses

(PRISMA) guidelines (Moher et al., 2009). These guidelines help ensure that the review includes all necessary information and is reported in a clear and replicable manner. The PRISMA diagram is depicted in Fig. 1. 106 studies were included in the final assessment, 68 from SCOPUS database and another 38 from additional citation analysis.

2.4. Study selection and screening process

Systematic reviews are inherently time- and resource-intensive. In the health sciences, for example, estimates suggest that conducting a full

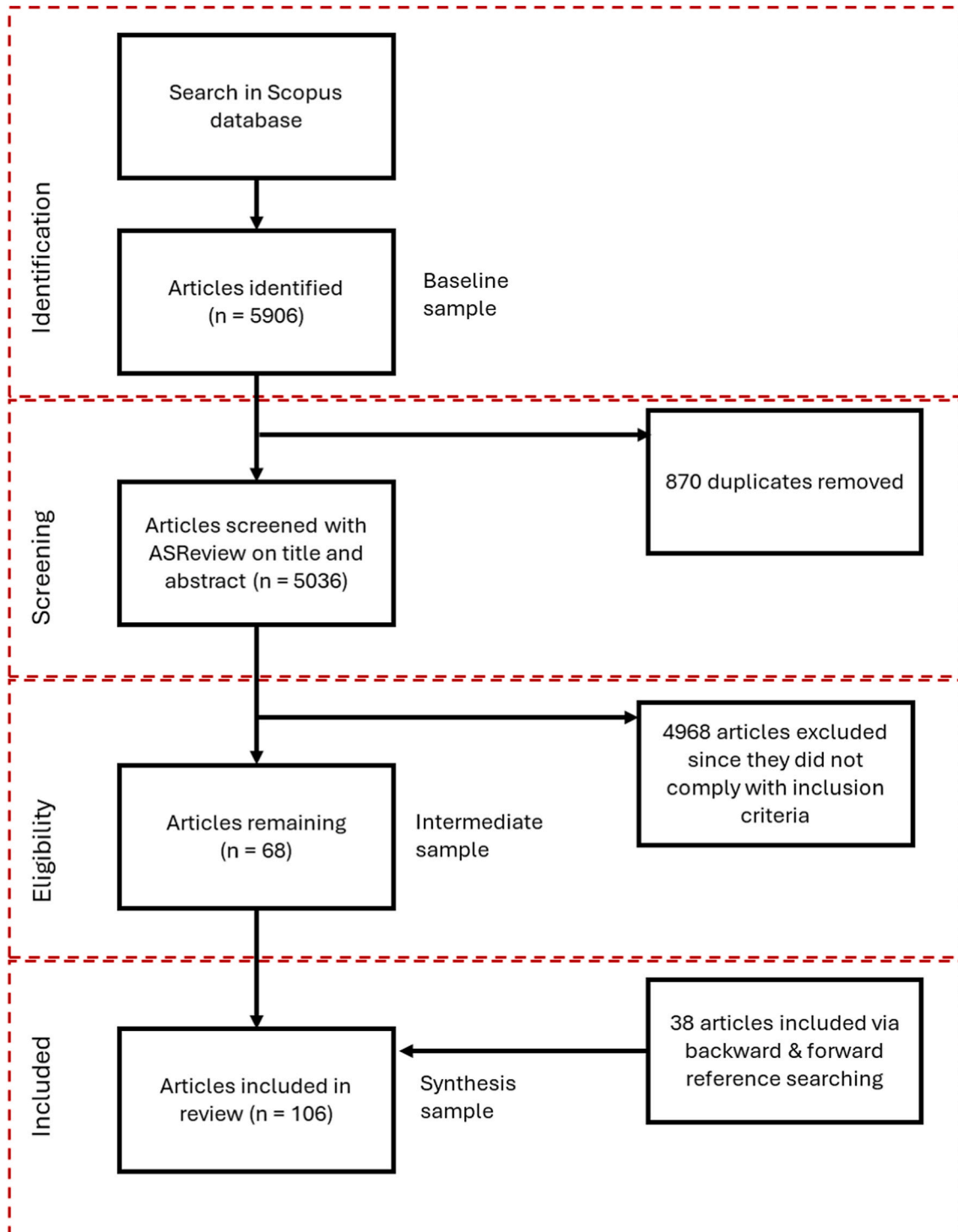


Fig. 1. PRISMA flow diagram presenting the inclusion process.

review may require up to 72 weeks of skilled labour (Smith et al., 2011). Given the exponential growth of scientific literature, relying solely on manual screening is increasingly impractical and unsustainable (Shemilt et al., 2016). A critical step in the review process is the screening of titles and abstracts to assess the relevance of studies identified through initial database searches (Chai et al., 2021). To address the scalability challenge, researchers have increasingly adopted machine learning techniques to support or automate this screening phase (e.g., Campos et al., 2024; Guan et al., 2023; Huang et al., 2022; Zhang et al., 2023). These algorithms prioritise and classify abstracts, enabling efficient identification of studies that merit further evaluation. In the health sciences, such approaches have demonstrated time savings of over 90% compared to manual screening (Van de Schoot et al., 2021).

In this study, we employed ASReview, an open-source software platform designed to run locally without reliance on external vendor servers, intended to facilitate semi-automated screening using active learning algorithms (Adamse et al., 2024; Campos et al., 2024; Van de Schoot et al., 2021). ASReview supports various classification models and operates through an iterative relevance feedback loop. In configuring ASReview, we employed a standard active learning setup using a probabilistic classifier to prioritise relevant records. After an initial configuration and training phase, the algorithm predicts the relevance of all records in the dataset and presents the study deemed most likely to be relevant. The reviewer then assesses this study based on its title and abstract and provides a binary relevance judgment. In this research, this judgement process was performed by two researchers concurrently until consensus was reached. As a result, formal inter-rater reliability metrics (e.g., Cohen's kappa) were not calculated. Instead, consistency was ensured through continuous discussion and alignment between the researchers during the screening and coding process. This consensus-based approach was chosen to maximise interpretative agreement and to reduce ambiguity in the categorisation of complex constructs, which is consistent with qualitative and theory-building systematic review approaches. These consensus relevance judgements were subsequently used as input for the active learning model, which iteratively updated its predictions and prioritised the next most relevant studies. This process continues iteratively, with the model continuously refining its predictions based on user input. ASReview is often used in academic research (Adamse et al., 2024; Sabiri et al., 2025) and is considered as a gain of time (Khat et al., 2024).

To determine when to conclude the screening process, we adopted a data-driven stopping criterion based on predictive irrelevance: the review was terminated after ten consecutive studies predicted as relevant were judged irrelevant by the reviewers (Callaghan & Müller-Hansen, 2020; 2024; Campos et al., 2024). All remaining records in the dataset were automatically excluded based on their low predicted relevance scores.

2.5. Eligibility and inclusion criteria

To ensure the academic rigour and accessibility of the literature reviewed, specific eligibility criteria were established for the inclusion of research papers. First, only papers written in English were considered, as English remains the dominant language of international scholarly communication and facilitates broader dissemination and comprehension of research findings (Graddol, 2006). Second, the selected articles and conference papers had to peer-reviewed, a process that serves as a critical quality assurance mechanism by subjecting manuscripts to evaluation by experts who assess the validity, methodology, and significance of the research (Springer, 2025). This gatekeeping function helps maintain the integrity and credibility of academic discourse. Third, the presence of an abstract was required, as abstracts provide a concise summary of a study's objectives, methods, and key findings, enabling researchers to quickly assess the relevance of a paper to their own work. Fourth, the full text was open access, available through institutional access, or provided by the authors that were contacted for

this purpose. Fifth, papers specifically mentioned one of the topics of interest in the abstract (thematic relevance). These criteria collectively ensure that the studies included in the review are both credible and relevant, thereby strengthening the foundation for subsequent analysis and discussion.

2.6. Data extraction

Using a codebook when conducting an SLR is essential for ensuring methodological rigour and consistency when extracting data from the identified research papers (Brown et al., 2003). The protocol described earlier (see Table 1) facilitates a thorough and transparent review process, enabling researchers to repeat the SLR. This structured approach is particularly valuable in complex and multidisciplinary studies, such as those examining IRB and CSC because those topics involve human psychology, behaviour, cybersecurity, system engineering, and more. The codebook used for data extraction is depicted in Table 2. The codebook is divided into three sections: the general characteristics of the studies, IRB, and the CSC factors of interest. All relevant extracted information was gathered in a Microsoft (MS) Excel data sheet for further analyses.

Given our small team to conduct the analysis on a large number of research papers, and to optimise performance, MS Copilot was used to assist structured data extraction. The interpretation and extraction of insights from data were conducted by the researchers. The use of AI was guided through a structured approach which leverages prompt engineering. Recent academic studies support this approach. Large Language Models (LLMs) are being increasingly used for systematic reviews and enhance the process in many ways (Atkinson, 2024; Bolaños et al., 2024). It is shown that AI can serve as a valuable complement to human oversight particularly in screening and summarising relevant literature (Bernard et al., 2025).

The prompt engineering approach consisted of three steps. The first step included role prompting (Kong et al., 2023; Salewski et al., 2023), which assigns the AI a specific analytical role to align its responses with the task at hand. The second step was context priming, which provides background information and task-specific context to improve relevance and accuracy (Kamath et al., 2024). Lastly, workflow generation or breadcrumbing was applied (Li, Xu, Hua, Rama, Raheja, Wang, & Zhang,

Table 2
Codebook with data extraction elements.

Data extracted	Rationale/description
1. General	
1.1 Author(s)	Author(s) of the publication
1.2 Name of journal	Name of the journal
1.3 publication year	Year of publication
2. IRB within the study	
2.1 Definition	How do authors define the construct in their study? Is it an implicit definition or do they explicitly highlight their definition? Do they provide their own definition of the construct?
2.2 Domain	E.g., health care.
2.3 Type of incident	E.g., self-caused, done by third party, unknown/unclear, or near-miss.
2.4 Antecedents	Concepts that influence IRB and are antecedent to it (also called enabler or protective factors).
2.5 Barriers	E.g., burden of reporting, fear of disciplinary action, or fear of embarrassment.
2.6 Consequences	Concepts that are linked to IRB in terms of being an outcome or a result of it.
3. CSC within the study	
3.1 Definition	How do authors define the construct in their study? Is it an implicit definition or do they explicitly highlight their definition? Do they provide their own definition of the construct?
3.2 Entity	Of what? E.g., organisation, team, or individual?

2024; Zeng et al., 2023), which in our case involved uploading research papers alongside our codebook to MS Copilot to iteratively guide the AI's analysis and maintain methodological consistency.

AI tools were thus integrated to support two distinct tasks. ASReview functioned as a filtering system, identifying the most relevant research papers from the extensive results retrieved via Scopus. MS Copilot was then used to extract specific data from these selected papers, guided by our predefined codebook. This methodological step was refined using the prompt engineering techniques described above. Adequacy was assessed by manually extracting data from ten randomly selected articles using the codebook and comparing the results side-by-side with MS Copilot's output, which was found to be sufficiently consistent.

All AI-assisted tasks were performed exclusively within a secure MS 365 offline work environment, which operates under enterprise-grade security and compliance standards. This means that data never left the organisation-managed infrastructure and that no third-party model training used our data. Web search was deliberately turned off by the researchers to minimize the risk of data leakage and ensure that responses were based exclusively on the uploaded research papers, without being influenced by online sources.

2.7. Conceptual model development

An important aim of this paper is to capture the results of the SLR in a conceptual model. Conceptual models help to represent complex information in a structured and visual manner, making the core ideas and relationships easier to understand. In doing so, the model supports the research objectives by illustrating how key factors and variables relate to each other. It also enhances the communicating of findings by making complex information more accessible and comprehensible.

Beyond its analytical function, the model offers practical value by helping practitioners understand the factors and processes that shape IRB. As such, it serves as a foundation for the development of interventions and strategies aimed at improving reporting practices.

For developing the conceptual model, we followed a structured four-step process, drawing on established approaches to conceptual model development (Naeem et al., 2023; Ravitch & Riggan, 2016):

1. Identification of key concepts
 - The results of the literature review were analysed to identify core concepts, variables, and themes, including relevant factors, processes, outcomes, and relationships.
2. Specification of relationships between concepts
 - The identified concepts were examined to determine their theoretical relationships, including potential causal links, interactions, and dependencies.
3. Model design
 - A visual representation was developed to depict the concepts and their interrelationships, ensuring clarity, coherence, and interpretability.
4. Definition of components and interconnections
 - The components of the model (e.g., variables and processes) and their connections were clearly specified. Arrows and labels were used to indicate relationships, with additional explanations provided where necessary to clarify their nature.

3. Results

This section presents the results of our data extraction and analysis processes. It begins with a general overview of the included studies, highlighting their scope, design, and relevance to the research questions.

Subsequently, the results of the thematic analysis are presented, offering insights into how IRB is conceptualised across the literature and which cultural and contextual variables are most frequently associated with reporting behaviour. This review is based on a descriptive and thematic synthesis of the literature rather than a quantitative meta-analysis. Accordingly, it does not estimate effect sizes or statistically aggregate findings, but instead focuses on identifying recurring patterns and themes across studies. Consequently, the frequency with which antecedents or barriers are reported should not be interpreted as an indicator of their empirical importance or effect size. Finally, this section synthesises these findings into a comprehensive framework for understanding how organisational culture influences IRB.

3.1. Synthesis sample description

The dataset includes contributions from a wide range of scholars, with a total of 371 unique individual authors identified across all studies. Most authors appear only once, indicating a broad and diverse authorship base. The 106 studies included in this review span a wide range of publication years, from 2002 to 2025, with a noticeable increase in research activity over time. The year with the highest number of publications was 2021 (accounting for 12 studies), followed by 2024 (with 11 studies) and 2017 (with 10 studies). This trend suggests growing scholarly interest in IRB, particularly in recent years.

In terms of publication venues, the studies were published across 82 different academic journals, reflecting the interdisciplinary nature of the topic. The most frequently represented journal was *Computers & Security* (which published 8 studies), followed by the *International Journal for Quality in Health Care* (with 6 studies), and three journals with 4 studies each: *Quality and Safety in Health Care*, *Journal of Nursing Management*, and *Information & Computer Security*. An overview of all the studies included in the review and their characteristics is shown in the appendix of the paper (see Table A1).

3.2. Synthesis of definitions of IRB

In this review, 106 scientific articles were analysed to examine how IRB is defined across various domains, including healthcare, cyber resilience, and aviation. The analysis revealed considerable variation in how the construct is conceptualised and operationalised.

Out of the 106 articles, 41 provided an explicit definition of IRB; 37 offered implicit definitions, often through examples or survey items; 28 did not provide a clear definition, instead referring to the concept indirectly or not at all. Among the explicit definitions, several recurring attributes emerged. The most frequently used terms were 'reporting' (41 mentions), 'incident' (26), 'act' (20), 'safety' (19), and 'behaviour' (15). Most definitions framed IRB as 'the act of reporting safety-related incidents or adverse events,' regularly emphasising its voluntary nature and its role in organisational learning and patient or system safety, often within a formal system.

Definitions also varied in their contextual emphasis. In healthcare, the focus was on improving patient safety, learning from errors, and fostering a reporting culture. In cyber resilience, definitions emphasised the reporting of suspicious digital activity, such as phishing or policy violations, often framed within the concept of human-as-a-sensor. In aviation, the behaviour was often linked to safety citizenship, where voluntary reporting contributes to organisational learning and risk mitigation.

A key distinction was observed between definitions that emphasised individual motivation (e.g., willingness, intention, responsibility) and those that focused on systemic or procedural aspects (e.g., formal reporting mechanisms, compliance, documentation). Some definitions also included informal reporting (e.g., verbal communication), while others restricted the concept to structured, system-based reporting.

In conclusion, while there is no universally accepted definition of IRB, the literature converges on a few core elements, defining it as a

behavioural act, often voluntary, aimed at disclosing safety-related events to improve organisational learning, safety culture, and risk management. The diversity in definitions again reflects the interdisciplinary nature of the topic and highlights the importance of contextual clarity in both research and practice.

3.3. IRB domains

The systematic review identified three key industry domains in which IRB has been studied: healthcare, aviation, and cybersecurity (see our synthesis sample in the appendix). Each domain presents distinct organisational cultures, regulatory pressures, and operational contexts that influence how individuals and institutions report incidents.

Healthcare: Out of all included studies, 66 were conducted in healthcare settings, encompassing nursing, hospital-based care, medical education, and multidisciplinary teams. This dominance reflects the long-standing emphasis on patient safety and error reporting in clinical environments. IRB is shaped by strict data protection regulations and a strong emphasis on patient safety. However, studies noted that fear of blame, time constraints, and uncertainty about what constitutes a reportable incident often hinder timely and accurate reporting by healthcare professionals.

Cybersecurity: The second most represented domain was cybersecurity, with 28 studies focusing on topics such as information security, phishing detection, user behaviour, and organisational reporting systems. This growing body of research highlights the increasing recognition of human factors in digital incident reporting and the role of employees as active participants in cyber defence. Several studies focused on incidents within the cybersecurity industry itself, including breaches at security firms, insider threats, and ethical dilemmas faced by professionals. Interestingly, even within the cybersecurity industry itself, reporting behaviour is not immune to organisational and psychological barriers. Professionals may hesitate to report internal incidents due to concerns about how trustworthy or reliable they will appear to others—especially colleagues, managers, or leadership—if they report an internal incident. These dynamics underscore the need for trust-based reporting cultures, even in expert environments.

Aviation: Aviation accounted for 10 studies, often emphasising safety culture, voluntary reporting systems, and learning from near misses—principles that have historically influenced other high-risk industries. The aviation industry has a long-standing culture of safety reporting, which extends into cybersecurity. Reporting mechanisms are often formalised and embedded in risk management systems. Within the aviation domain several recurring barriers to incident reporting were observed. These include: fear of disciplinary action, embarrassment, or reputational damage; concerns about job security and career progression; lack of anonymity and clarity on what constitutes a reportable incident; and perceived futility due to limited feedback or visible outcomes. Cultural norms, such as reluctance to report colleagues, and usability issues with reporting systems further hinder reporting behaviour. These findings underscore the importance of fostering a just culture, improving system design, and enhancing training to support initiative-taking and transparent reporting practices.

These findings suggest that IRB is context-dependent, influenced by sector-specific norms, perceived consequences, and the clarity of reporting procedures. Understanding these domain-specific dynamics is essential for designing effective reporting systems and fostering a culture of transparency and continuous learning.

3.4. Incidents characteristics and reporter attributes

The SLR revealed a diverse range of incidents, which were categorised into four primary types based on their origin and nature. These categories illustrate both the intentional and the unintentional natures of incidents in organisational and in individual contexts.

1. **Self-Caused Incidents:** These incidents involved actions by individuals or organisations, including careless or non-compliant behaviour. A common example from the cybersecurity domain was the accidental leakage of sensitive data due to misconfigured systems or improper handling of information (Ebert et al., 2023).
2. **Third-Party Incidents:** This category encompassed incidents that were entirely caused by external actors, such as vendors, contractors, or service providers. These cases often involved insufficient vetting or oversight of third-party access to critical systems (e.g., Adjekum et al., 2016).
3. **Victim of Attack:** A sizeable portion of the reviewed literature described organisations or individuals as victims of deliberate cyberattacks, including hacking, phishing, ransomware, and other forms of malicious intrusion (e.g., Ahola et al., 2025; Franz, 2022). These incidents typically involved sophisticated threat actors exploiting technical vulnerabilities and are unique to the cybersecurity domain.
4. **Internal Reporting:** A smaller but notable subset of incidents involved internal whistleblowing or peer reporting of unsafe security practices (Alshaikh, 2020). Examples in the cybersecurity domain included employees reporting colleagues who failed to lock their screens or who shared passwords inappropriately (Ballreich et al., 2023; Van Steen et al., 2024). These cases highlight the role of organisational culture and peer accountability.

Together, these categories illustrate the multifaceted nature of incidents, ranging from human error and negligence to targeted external attacks. Understanding the distribution and characteristics of incidents is essential for developing tailored prevention and response strategies.

From this typology, it becomes evident that reporters of incidents can be broadly categorised into three roles: victims, bystanders, and guilty parties. Victims report incidents in which they were directly targeted or harmed (e.g., cyberattacks). Bystanders report unsafe or negligent behaviour observed in others (e.g., internal reporting). Guilty parties may self-report incidents they caused, either accidentally (e.g., misconfigurations) or through negligence. These roles are not mutually exclusive and may shift depending on the context and timing of the report, especially in cases like near misses where multiple perspectives may converge. For example, someone might be both a guilty party (of a misconfiguration) and a victim (of the resulting breach). This classification further helps to clarify the psychological and organisational dynamics that influence IRB. Each role is associated with different motivations and barriers. For instance, victims may fear retaliation or stigma, bystanders may struggle with loyalty or ambiguity, and guilty parties may face concerns about blame, punishment, or reputational harm.

Finally, it is worth mentioning that several studies reported on near misses—situations where a potential incident, regardless of type, was narrowly avoided. These cases often served as valuable learning opportunities and emphasised the importance of initiative-taking in risk identification and mitigation. For instance, Vrbnjak et al. (2016) investigated barriers to reporting of near misses in hospital settings. They indicate that open and honest disclosure of near misses is critical to patient safety and optimization of quality nursing care. But also, that near misses are underreported. Knowledge of the barriers of near miss reporting is important to improve safety. They stress the need for further research and development of measures to overcome these barriers.

3.5. Antecedents of IRB

A thematic analysis of the antecedents mentioned across the reviewed studies revealed a wide range of factors influencing IRB. Thematic analysis is a method to analyse qualitative data. It involves the identification and reporting of patterns in a data set, which are then interpreted for their inherent meaning (Braun & Clarke, 2006). In total, there are 523 unique antecedent factors mentioned in the dataset. The top-ranked antecedents are listed in Table 3, including the number of

Table 3
Top ranked antecedents and number of mentions.

Antecedent	Mentions	Refs.
Training	23	26, 28, 39, 61, 96, 57, 66, 7, 10, 91, 13, 17, 71, 67, 58, 43, 31, 79, 30, 8, 92, 88, 104
Organisational culture	21	25, 65, 60, 61, 96, 66, 12, 13, 62, 49, 31, 29, 59, 55, 73, 47, 72, 23, 19, 93, 106
Leadership support	18	87, 98, 18, 7, 6, 103, 21, 58, 20, 94, 101, 1, 82, 76, 73, 88, 93, 64
Feedback mechanisms	15	45, 2, 75, 7, 50, 21, 17, 71, 94, 90, 30, 72, 19, 83, 81
Knowledge of how to report	12	87, 18, 10, 12, 14, 52, 53, 3, 82, 76, 42, 44
Fear of blame ^a	11	46, 61, 96, 57, 99, 17, 20, 49, 11, 38, 64
Perceived usefulness of reporting	9	87, 7, 97, 33, 3, 1, 59, 34, 106
System usability	9	2, 96, 66, 103, 9, 52, 58, 43, 23
Attitudes towards reporting	8	18, 22, 4, 58, 8, 88, 23, 42
Just culture	8	28, 80, 17, 40, 101, 41, 72, 93
Psychological safety	7	70, 67, 69, 15, 101, 68, 64
Trust in the system	7	98, 28, 49, 11, 69, 72, 81
Cultural norms	7	87, 10, 74, 20, 15, 82, 64
Time constraints	6	57, 103, 52, 53, 79, 19
Managerial support ^b	5	18, 50, 78, 76, 55

^a In the literature, antecedents are typically defined as factors that influence the likelihood or intention to report incidents, whether positively or negatively. While many antecedents are enabling (e.g., leadership support, psychological safety), others are inhibiting antecedents, and ‘fear of blame’ is one of the most frequently cited among them.

^b Although leadership and managerial support overlap, we treat these antecedents as distinct constructs in this study. Leadership support refers to providing vision, inspiration, and psychological safety, helping people understand purpose and feel motivated, whereas managerial support concerns enabling day-to-day work by offering resources, clear expectations, and practical assistance with tasks and processes.

mentions and references to articles in the synthesis sample (see [table A1](#)). It is important to note that the frequency with which antecedents are reported in the literature does not necessarily reflect their empirical importance or effect size. Rather, these frequencies indicate the prominence and recurrence of concepts across studies.

All unique antecedents were grouped, into five overarching themes, each encompassing several specific predictors: organisational, psychological, technical, social, and motivational. This thematic structure provides a clearer understanding of the multifaceted drivers and barriers influencing IRB and provides a structured lens through which to interpret them.

Organisational Antecedents: These refer to structural, cultural, and leadership-related factors within the organisation. Frequently cited elements include organisational culture, leadership support, feedback mechanisms, managerial support, and just culture (see, for example, [Ballreich et al., 2023](#)). These antecedents shape the broader environment in which reporting occurs and influence whether staff perceive the system as fair, supportive, and responsive.

Psychological Antecedents: This cluster captures internal perceptions and emotional states that affect reporting behaviour. This might also include cognitive biases, such as normalization of deviance and optimism bias, that can lead individuals to underestimate risks or dismiss the need for reporting ([Ebert et al., 2023](#); [Pfeifer et al., 2023](#)). Key factors include psychological safety, fear of blame, trust in the system, and fear of consequences. These antecedents reflect the individual's confidence in the reporting process and its outcomes.

Technical Antecedents: These relate to the technical infrastructure through which incidents are reported. System usability emerges as a crucial factor (e.g., [Jausan et al., 2017](#)). Reporting platforms that are intuitive, streamlined, and require minimal effort are more likely to be used. Anonymity and confidentiality are also critical. The presence of features that protect the reporter's identity—such as anonymous

submission options—can mitigate fears of retaliation, embarrassment, or professional consequences. Feedback mechanisms embedded in the system further influence IRB (e.g., [Anderson et al., 2013](#)). Reporters are more likely to engage with systems that acknowledge their input and provide updates on outcomes. Trust and perceived effectiveness of the system also shape IRB. If users believe that their reports will lead to meaningful action, they are more inclined to report. Finally, technological confidence and awareness influence whether individuals feel capable of using the system. In sum, the technical reporting system is not a neutral medium but an active determinant of IRB. Its design and implementation can either lower or raise the threshold for reporting, making it a critical component in any strategy aimed at improving organisational learning and safety culture.

Social Antecedents: Social dynamics and norms within teams and professional groups fall under this category. Examples include cultural norms, peer pressure, subjective norms, and support from colleagues. These antecedents highlight the role of interpersonal relationships and shared expectations in shaping IRB (see, for instance, [Winsvold Prang & Jelsness-Jørgensen, 2014](#)).

Motivational Antecedents: This cluster includes factors that influence willingness to report. Prominent examples are perceived usefulness of reporting, attitudes toward reporting, and perceived behavioural control (e.g., [Anderson et al., 2013](#)). These antecedents reflect both intrinsic and extrinsic motivators that drive or inhibit action.

The most-reported predictors of IRB are training, organisational culture, leadership support, and feedback mechanisms. Together, these findings imply that improving IRB requires a multi-level approach: equipping individuals with the right knowledge and skills (training), embedding reporting in a supportive cultural context (organisational culture), ensuring visible and consistent leadership commitment (leadership support), and maintaining a responsive and transparent system (feedback mechanisms). These elements are mutually reinforcing and should be addressed in an integrated manner to achieve sustainable change.

To further interpret the antecedents of IRB, and help construct the conceptual model, we mapped the five thematic clusters—organisational, psychological, technical, social, and motivational—onto a widely used framework for behaviour change, the COM-B model, which conceptualises behaviour as a function of Capability, Opportunity, and Motivation ([Michie et al., 2011](#)). This mapping revealed that organisational and social antecedents primarily align with the Opportunity component, as they reflect external conditions, such as leadership support, team norms, and cultural climate, which enable or constrain reporting. Technical antecedents, such as system usability and knowledge of reporting procedures, correspond to Capability, representing the individual's psychological and procedural ability to report. Psychological antecedents span both Capability and Motivation, as factors like psychological safety and fear of blame influence both perceived ability and willingness to act. Finally, motivational antecedents—including training, perceived usefulness, and attitudes toward reporting—map directly onto the Motivation component, capturing the internal drivers that energise and direct behaviour.

3.5.1. Amplifying and inhibiting effects on IRB

The SLR revealed not only a wide array of individual antecedents to IRB but also patterns of interaction among them. Through thematic synthesis, it became evident that certain factors amplify or inhibit each other's influence. For example, the usability of a reporting system was frequently found to be more effective in environments characterised by high psychological safety, while its impact diminished in settings marked by fear of blame (see [Ebert et al., 2023](#); [Jausan et al., 2017](#); [Pfeifer et al., 2023](#)). In environments where individuals fear blame or retaliation, even the most intuitive systems may go unused. Similarly, feedback mechanisms were shown to enhance the perceived usefulness of reporting, whereas their absence undermined motivation, even when other conditions were favourable ([Adjekum et al., 2016](#); [Anderson et al.,](#)

2013; Cerrone et al., 2025; Jausan et al., 2017; Winsvold Prang & Jelsness-Jørgensen, 2014). Leadership support consistently emerges as a critical moderator in shaping the impact of fear-related inhibitors on reporting behaviour. When leaders demonstrate openness, transparency, and active engagement, they buffer the negative effects of fear, such as concerns about blame or punitive consequences, and foster a culture of psychological safety that encourages reporting (Jausan et al., 2017; Pfeifer et al., 2023). Conversely, the absence of visible leadership commitment can exacerbate these inhibitors, reinforcing hierarchical barriers and discouraging staff from sharing safety concerns (Wawersik & Palaganas, 2022; Yusuf & Irwan, 2021). Evidence from healthcare and aviation contexts underscores that leadership behaviours—such as providing feedback, modelling accountability, and promoting learning—are not merely supportive but actively shape the organisational climate, determining whether fear-related factors are mitigated or amplified (Ebert et al., 2023). These findings highlight leadership as a dynamic force that can transform reporting systems from compliance-driven tools into mechanisms for continuous improvement. Overall, these interdependencies, observed across diverse empirical contexts, suggest that IRB is shaped by a dynamic system of interacting influences rather than by isolated variables alone.

3.6. Barriers to IRB

The systematic review identified a diverse range of barriers¹ that are reported to inhibit IRB across sectors. A total of 87 distinct barriers were extracted from the literature, with several recurring themes (see Table 4). The most frequently cited barrier was lack of feedback (mentioned in 29 studies), highlighting a widespread perception that reporting does not lead to meaningful change or learning. Time constraints (with 11 mentions) and fear of disciplinary action or punishment (with a combined 18 mentions) were also prominent, reflecting both structural and psychological deterrents. Other common barriers included blame culture (7 mentions), fear of litigation (6), lack of anonymity (4), and perceived futility (4).

These barriers were clustered into five overarching themes:

- (1) Fear-based deterrents (e.g., fear of blame, punishment, litigation);
- (2) Organisational inefficiencies (e.g., time burden, complex systems);
- (3) Cultural and social norms (e.g., blame culture, peer dynamics);
- (4) Lack of procedural clarity (e.g., ambiguity about what to report); and
- (5) Feedback and learning deficits (e.g., lack of follow-up or visible outcomes).

These findings underscore the need for systemic interventions that foster psychological safety, streamline reporting processes, and ensure transparent feedback mechanisms to cultivate a just and learning-oriented reporting culture.

To thematically analyse the psychological and systemic roots of the identified barriers, we again mapped them to the COM-B model (see also Table 4). Each barrier was categorised under one of the COM-B components: Capability, Opportunity, or Motivation.

The analysis revealed that Motivation-related barriers were the most prevalent, encompassing 20 unique barriers and accounting for 82

Table 4

Barriers to IRB, grouped by theme, COM-B components: Capability (C), Opportunity (O), or Motivation (M), including the number of mentions in the synthesis sample, and references to the articles included in the sample (see table A1).

Theme	COM	Barrier	Mentions	Refs.
Fear-Based Deterrents	M	Fear of disciplinary action	9	46, 99, 89, 62, 49, 11, 69, 1, 81
Fear-Based Deterrents	M	Fear of punishment	9	28, 50, 9, 27, 20, 31, 38, 30, 106
Fear-Based Deterrents	M	Fear of blame	5	78, 21, 85, 72, 83
Fear-Based Deterrents	M	Fear of litigation	6	46, 62, 67, 11, 1, 63
Fear-Based Deterrents	M	Fear of retaliation	1	58
Fear-Based Deterrents	M	Fear of retribution	1	79
Fear-Based Deterrents	M	Fear of embarrassment	3	46, 62, 49
Fear-Based Deterrents	M	Fear of being perceived as incompetent	3	89, 69, 106
Fear-Based Deterrents	M	Fear of legal consequences	2	70, 59
Fear-Based Deterrents	M	Fear of vilification and conflict	1	73
Fear-Based Deterrents	M	Fear of harming professional relationships	1	103
Fear-Based Deterrents	M	Fear of damaging relationships	1	87
Fear-Based Deterrents	M	Fear of repercussions	1	8
Fear-Based Deterrents	M	Shame	2	80, 81
Fear-Based Deterrents	M	Guilt	2	94, 88
Organisational Inefficiencies	O	Time constraints	11	45, 87, 18, 37, 66, 10, 97, 103, 21, 17, 58
Organisational Inefficiencies	O	Burden of reporting	2	57, 62
Organisational Inefficiencies	O	Time burden	2	87, 76
Organisational Inefficiencies	O	Administrative burden	2	99, 58
Organisational Inefficiencies	O	Complexity of reporting systems	2	103, 42
Organisational Inefficiencies	O	System complexity	1	9
Organisational Inefficiencies	O	Time-consuming reporting process	1	64
Organisational Inefficiencies	O	High workload	3	45, 67, 105
Organisational Inefficiencies	O	Resource constraints	1	98
Cultural and Social Norms	O	Blame culture	7	46, 39, 66, 31, 76, 30, 105
Cultural and Social Norms	O	Peer pressure	1	22
Cultural and Social Norms	O	Peer tension	1	20
Cultural and Social Norms	O	Cultural norms (e.g., preserving peer harmony)	2	22, 49
Cultural and Social Norms	O	Cultural normalization of violence	1	37
Cultural and Social Norms	O	Concern over ward reputation	1	8
Cultural and Social Norms	O	Not betraying colleagues	1	49
Cultural and Social Norms	O	Gender bias (male victims less likely to report)	1	37

(continued on next page)

¹ While antecedents to IRB include inhibiting factors, we still think it remains analytically valuable to examine barriers in a dedicated section. Barriers are a specific subset of antecedents that actively obstruct reporting, such as fear of blame. Isolating them allows for a more focused analysis of the dynamics that suppress IRB. Moreover, barriers are often more actionable than broader antecedents, making them particularly relevant for designing targeted interventions.

Table 4 (continued)

Theme	COM	Barrier	Mentions	Refs.
Lack of Procedural Clarity	C	Lack of knowledge	3	45, 66, 14
Lack of Procedural Clarity	C	Unclear reporting procedures	1	92
Lack of Procedural Clarity	C	Ambiguity about what constitutes a reportable incident	2	33, 72
Lack of Procedural Clarity	C	Ambiguity about what to report	1	103
Lack of Procedural Clarity	C	Lack of clarity on what to report	3	12, 33, 72
Lack of Procedural Clarity	C	Lack of training	1	28
Lack of Procedural Clarity	C	Uncertainty about what constitutes an error	1	89
Feedback and Learning Deficits	M	Lack of feedback	29	2, 37, 46, 39, 61, 96, 57, 99, 7, 70, 50, 97, 14, 27, 78, 21, 62, 52, 58, 20, 49, 8, 73, 72, 23, 42, 44, 19, 54
Feedback and Learning Deficits	M	Perceived futility	5	87, 46, 99, 14, 72
Feedback and Learning Deficits	M	No visible outcomes	1	94
Feedback and Learning Deficits	M	Distrust in system improvement	1	20
Feedback and Learning Deficits	M	Perception that reports are not acted upon	1	46

mentions across studies. These included fear-based deterrents (e.g., fear of punishment, shame, guilt) and perceptions of futility (e.g., lack of feedback, no visible outcomes). This suggests that psychological and emotional factors are the most mentioned inhibitors of IRB.

Opportunity-related barriers were also prominent, with 10 barriers (26 mentions) linked to physical opportunity (e.g., time constraints, system complexity) and 8 barriers (15 mentions) to social opportunity (e.g., blame culture, peer pressure). These findings highlight the importance of both environmental and interpersonal contexts in shaping IRB.

Capability-related barriers were less frequently reported (7 barriers, 12 mentions), but they remain critical. These included lack of knowledge, unclear procedures, and insufficient training—factors that can undermine the foundational ability to report incidents effectively.

This mapping again underscores the need for multi-level interventions. Strategies should prioritise enhancing psychological safety and motivation, improving system usability and social support, and ensuring adequate training and procedural clarity.

3.7. Consequences of IRB

The literature revealed a wide range of consequences associated with IRB. A distinction should be made between ‘consequences of reporting’ as it is defined in this section and as it is used when referring to an individual’s ‘fear of consequence of reporting.’ We define consequences based on this SLR as: ‘concepts that are linked to IRB in terms of being an outcome or a result of it.’ This category is intended to capture all outcomes, downstream effects, and ramifications of IRB. This wide range of

outcomes, however, are not what is typically meant with the term ‘fear of consequence,’ which tends to be more limited to negative repercussions that the individual in question is concerned they may face after reporting an incident.

There were 242 unique consequences listed related to IRB. The consequences were both positive and negative, reflecting the complex nature of organisational dynamics. More specifically, out of all 285 consequences mentioned (not only unique mentions), 165 were positive, 33 were negative, and 87 were neutral or unclear. An overview of positive outcomes is summarised in Table 5.

Approximately 20% (19 out of 106) of the articles included in this review made specific mention of the consequences of underreporting, as opposed to the consequences of IRB. Underreporting leads to missed opportunities for learning and improvement based on incidents, near misses, and systemic weaknesses (for an overview, see Table 6). Underreporting not only hinders organisational learning and system correction, but it also restricts the potential for robust, data-driven safety improvements. It compromises future safety by allowing risks and near misses to go unaddressed, thereby increasing the likelihood of future incidents. Operationally, underreporting leads to inefficiencies, diminished awareness, and distorted safety metrics, which in turn obstruct the development of effective prevention strategies. Culturally, it perpetuates a climate of silence, fear, and blame, reinforcing stagnation and resistance to safety initiatives. Psychologically, it lowers the perceived safety of reporting, discouraging open communication. Furthermore, underreporting can have serious legal and ethical consequences, as organisations may fail to adequately protect staff and lack the necessary data to inform policy and prevention planning.

The consequences impact distinct groups in diverse ways. Out of all 285 consequences, 126 were specific to the organisation, 18 were specific to the individual, and 141 were unclear. The consequences of IRB related to the organisation were resoundingly positive. In contrast to the strikingly positive consequences of reporting for the organisation, the consequences for the individual tended to be viewed as negative. They were often framed in terms of emotional strain, psychological burden, fear of blame or retaliation, stigmatisation, perceived futility, and potential strain on interprofessional relationships. Some positive consequences were also listed for individuals, including: professional competence enhancement, in-service education and enhanced professional development, psychological closure after reporting incidents, and satisfaction from contributing to safety.

The consequences of IRB fell roughly into five main themes, briefly discussed here in descending order in terms of mentions. The largest number of consequences were cultural in nature, relating to shared values, norms, and behaviours within the organisation.² Examples of consequences include improved patient safety, learning culture, and increased transparency. For instance, Cerrone et al. (2025) argue that cultural transformation is not a byproduct but a core consequence of effective reporting systems, aligning organisational behaviours with safety principles. The second most common consequence theme was organisational, relating to structural, procedural, and performance-related changes in the organisation. These consequences demonstrated a notably consistent message that IRB improves organisational learning and safety outcomes. Anderson et al. (2013) demonstrate that IRB not only help to identify risks but also drive organisational learning by informing policy changes, improving procedures, and strengthening safety management systems. The authors emphasise that reporting mechanisms create feedback loops that lead to structural improvements and measurable safety outcomes, demonstrating a consistent organisational benefit beyond individual IRB. Third, several consequences were technical in nature. These frame IRB as opportunities for system improvements, for example by integrating

² It is remarkable that this is the largest theme of consequences, as it is basically the description of a feedback loop (behaviour back to culture).

Table 5
Positive outcomes of IRB.

Organisational learning and system-level improvement
Enhanced safety culture and transparency
Better root cause analysis and incident response
Improved decision-making and risk mitigation
Enhanced cyber resilience and technical defences
Improved collaboration between safety and judicial authorities
Development of institutional protocols and policy refinement
Improved access to teams, tailored training, and awareness
Cultural transformation toward openness and shared responsibility
Improved trend analysis, resource allocation, and crime statistics
Faster detection, reduced incident impact, and organisational resilience

Table 6
Overview of negative consequences of underreporting for organisations.

Missed learning opportunities and systemic improvement gaps
Hindered development of effective prevention strategies
Perpetuation of a culture of silence, fear, or blame
Reduced organisational awareness of risks
Failure to develop or refine institutional protocols
Legal and organisational failure to protect staff
Cultural stagnation and resistance to safety initiatives
Limits on data-driven safety improvements and trend analysis
Reduced effectiveness of safety systems and incident investigations

IRB and associated data into technical workflow. For instance, [Ebert et al. \(2023\)](#) argue that reporting data can be leveraged for system optimization, including embedding feedback loops into technical workflows and aligning reporting mechanisms with cybersecurity and operational processes. The fourth theme was psychological and emotional. These consequences illustrate the emotional burden associated with underreporting, including fear of blame and stigma, while also highlighting a potential positive outcome in the form of psychological closure. [Winsvold Prang and Jelsness-Jørgensen \(2014\)](#) found that when reporting occurs, reporters often experience psychological relief and closure, as the act of reporting validates their concerns and contributes to a sense of resolution. These findings illustrate the dual nature of psychological consequences—negative when reporting is avoided and positive when it is embraced. The last theme to emerge was legal, related to the requirement to comply with legal obligations and to legal protection. The study by [Jausan et al. \(2017\)](#), for example, highlights that safety reporting systems are not only operational tools but also mechanisms for meeting regulatory requirements. It emphasises that compliance with legal obligations is a core driver for implementing reporting systems. Additionally, the authors note that robust reporting frameworks provide legal protection for both individuals and organisations by documenting safety-related actions and demonstrating adherence to mandated standards.

In conclusion, the consequences revealed by the SLR were wide-ranging. They had to do with organisational learning, technical improvements, organisational culture, and psychological or emotional strain. The multilevel and dual-natured landscape of consequences highlights the importance of fostering environments that amplify the positive outcomes of IRB while mitigating its potential downsides, particularly for individual reporters.

3.8. Definition of culture within the study

Several cultural models provide a theoretical foundation for analysing how CSC might shape IRB in organisational contexts. Hofstede's model ([Hofstede, 2011](#)), for instance, highlights how cultural dimensions such as power distance (i.e., the level of hierarchy), uncertainty avoidance (i.e., risk aversion), and individualism vs. collectivism can influence individual behaviour. Although often used to describe national cultures, these dimensions explicitly also pertain to organisational cultures. For example, in high power distance cultures, employees

may hesitate to report incidents due to fear of hierarchical repercussions. Similarly, in cultures with high uncertainty avoidance, the ambiguity surrounding incident classification may discourage reporting unless protocols are strictly defined.

Schein's model of organisational culture ([Schein, 2004](#)) further emphasises the role of underlying assumptions, espoused values, and artifacts in shaping behaviour. If an organisation implicitly values performance over transparency, employees may perceive incident reporting as a threat to their reputation or job security.

Our SLR shows that culture in the context of IRB is best understood as the behavioural manifestation of shared values, beliefs, norms, attitudes, and behavioural expectations that influence how individuals and groups perceive, interpret, and respond to safety-related events, including willingness to report incidents. It is deeply embedded within the organisational context shaped by internal policies, leadership styles, and communication practices and reflects how security becomes part of 'the way things are done.' Central to culture is a human-centric focus, recognising employees as both the first and last line of defence. Whether individuals report incidents, adhere to protocols, or engage in risky behaviour is influenced by the prevailing cultural climate.

A recurring theme in the literature is the importance of fostering a 'just culture,' a non-punitive, learning-oriented environment where mistakes are treated as opportunities for growth rather than grounds for punishment. Drawing on frameworks such as those by Schein and Hofstede, security culture is also seen as a system of often unwritten assumptions and expectations that guide behaviour. It is frequently conceptualised as a subculture within the broader organisational culture, with its own emphasis on security awareness, compliance, and behavioural norms. While some definitions are grounded in formal standards (e.g., ENISA, ISO), others are implicit, inferred through observable behaviours like openness, trust, and willingness to report.

Definitions of culture vary by entity level, reflecting the scope and focus of each context. Most definitions are situated at the organisational level (42 mentions), with fewer references to the individual (15), team (4), or national (1) levels. This suggests that culture is predominantly understood as a collective property of organisations, shaping and shaped by institutional norms, leadership practices, and systemic structures. At the organisational level, the most frequently referenced culture is typically defined as the aforementioned system of shared values, beliefs, and behavioural norms. At the team or departmental level, definitions are more implicit and focus on interpersonal dynamics, psychological safety, and communication practices that shape IRB. Macro-level (national or societal) perspectives are rare but introduce cultural traits like collectivism as background influences. Overall, the more localised the entity, the more definitions emphasise behavioural and relational aspects, while broader entities (e.g., organisations) incorporate structural, policy-driven, and leadership-related dimensions.

3.9. Towards a conceptual integrative model of IRB

Culture is not a peripheral factor in cyber resilience—it is a central determinant of how individuals perceive, interpret, and act upon security incidents. By understanding and leveraging cultural pathways, organisations can foster a more transparent, responsive, and cyber resilient posture. Based on our SLR and drawing on the Cybersecurity Culture-Behaviour (CSCB) framework developed by [Sutton and Thompson \(2024\)](#), we can identify several specific pathways through which culture influences IRB.

The CSCB framework conceptualises CSC through three interconnected components:

- Cultural Values – based on the Competing Values Framework (CVF);
- The Culture-to-Behaviour Link – informed by the Theory of Planned Behaviour (TPB) and the Awareness-Motivation-Capability (AMC) model;

- Cybersecurity-Related Behaviours – including both in-role and extra-role behaviours.

These components provide a structured lens through which to understand how culture influences the likelihood and quality of incident reporting.

To this framework, we add a component, namely the concepts that are linked to IRB in terms of being an outcome or a direct result of it. We feel that this component is essential in our understandings of IRB. From our SRL, we learned that the consequences vary by stakeholder and can be positive or negative. So, we included the positive and negative consequences of IRB at both the individual and the organisational level in the model.

Next, we decided to include a more updated behavioural model in the culture-behaviour link component of the framework to better organize the results of our analyses: the COM-factors of the COM-B framework. [Michie and colleagues \(2011\)](#) argue that their COM-B model (Capability, Opportunity, Motivation – Behaviour) serves as an integrative framework that encompasses and synthesises earlier behavioural theories. [Michie et al. \(2011\)](#) propose that behaviour occurs as an interaction between three necessary conditions:

- Capability: the individual's psychological and physical capacity to engage in the activity.
- Opportunity: external factors that make the behaviour possible or prompt it.
- Motivation: brain processes that energise and direct behaviour, including habitual processes, emotional responding, and analytical decision-making.

They argue that most existing behaviour change theories can be mapped onto this model, making it a meta-framework for understanding and designing behaviour change interventions.

The COM-B model developed by Michie et al. allows for a multi-level approach to behaviour, and the system context within this model can, in certain cases, overlap with—or even serve as an alternative to—cultural influences. Within this model, the concept of opportunity includes both physical and social environmental factors, such as organisational structures, policies, social norms, and access to resources. These elements closely align with what is often described in cultural models as ‘organisational culture’ or ‘shared values and norms.’ As such, the system context in the COM-B model can be seen as either overlapping with or, in some cases, providing a more operational alternative to traditional cultural constructs. Where cultural models often describe what influences behaviour in abstract terms, COM-B helps to explain how and why these influences translate into action, thereby unpacking the intricate concept of culture.

COM-B offers a more operational and behaviourally-oriented framework than many cultural models, which often remain somewhat abstract. Rather than measuring culture as a standalone construct, COM-B allows researchers to examine how cultural factors manifest in terms of opportunity, motivation, and capability. COM-B can also serve as a bridge between cultural models (such as Schein's model of organisational culture, 2004) and behavioural outcomes. For example, a culture characterised by high power distance (as described by Hofstede) may translate into low perceived behavioural control (in theory of planned behaviour (TPB) terms (see, [Ajzen, 1991](#)), or limited social opportunity (in COM-B terms)).

Moreover, COM-B is inherently suited to a multi-level analysis of behaviour. It can be applied at:

- the individual level (e.g., knowledge, skills, attitudes);
- the organisational level (e.g., leadership, policies, organisational culture);
- and the system level (e.g., regulation, sector-wide standards, nation culture).

This flexibility makes COM-B a powerful tool for analysing cybersecurity-related behaviours such as incident reporting. It allows researchers and practitioners to identify whether barriers to reporting lie in individual capability, motivational factors, or systemic opportunities, and how cultural factors might influence these mechanisms.

In this way, COM-B can function not only as a complement to cultural models but also as a pragmatic framework for designing interventions that address the behavioural determinants of cybersecurity practices. Hence, we decided to replace the Cultural Values component of the framework developed by [Sutton and Tompson \(2024\)](#) with an application of the COM-B model to the organisational and system levels, to provide a more operational alternative to traditional cultural constructs.

Furthermore, we added specific relationships between the component variables in the framework to show the more specific pathways of influence throughout the model. Emerging evidence and theoretical reasoning suggest that the relationship between antecedents of incident reporting—such as psychological safety, organisational justice, and fear of blame—and actual reporting behaviour may be significantly influenced by the type of incident involved. Incidents classified as severe—due to potential impacts on business continuity, legal compliance, or organisational reputation—are more likely to be reported promptly ([Edwards, 2024](#)). In the same manner, the nature of the incident (e.g., self-caused, or third-party) may function as a moderator, altering the strength or direction of these relationships. For instance, psychological safety may strongly predict reporting behaviour in the case of third-party incidents, where personal culpability is minimal, but may have a weaker effect for self-caused incidents, where fear of blame or shame is more salient ([Lantz-Deaton & Golubeva, 2020](#)). Alternatively, incident type may function as a mediator, shaping how individuals cognitively and emotionally process antecedents, thereby influencing their decision to report. This perspective aligns with attribution theory and organisational silence literature, which emphasise the role of perceived responsibility and social consequences in shaping disclosure behaviour. Recognising the roles of type of incident and reporters offers a more nuanced understanding of reporting dynamics and may inform more targeted interventions to promote transparent safety cultures.

3.10. Integrative multilevel model of cyber IRB

The proposed integrative and multilevel conceptual model of cyber IRB is depicted in [Fig. 2](#). It shows four main components: 1) societal influence, including cultural values at the national level; 2) the reciprocal culture-behaviour link, which resides at the level of the individual front-line workers and management within the organisation; 3) IRB, including a failure to report or selective reporting; and 4) consequences of IRB. We see the type and nature of incident and type of reporter as moderators or mediators of the relationship between the culture-to-behaviour link and IRB.

The integrative and multilevel model developed through this SLR offers a comprehensive framework for understanding how cultural, organisational, and individual factors influence cyber IRB. By structuring the model across four interrelated components—culture, the culture-to-behaviour link, behaviour (and non-behaviour), and consequences—it becomes possible to trace the pathways through which systemic and individual factors interact to shape reporting outcomes. This layered approach underscores the importance of aligning organisational systems and leadership practices with frontline realities to foster a culture conducive to transparent and proactive incident reporting.

At the top level, the model emphasises the role of system context and management as foundational to shaping organisational culture. This highlights the implication that interventions aimed at improving IRB must go beyond individual training or awareness campaigns. Instead, they should address broader structural and managerial factors, such as leadership commitment, resource allocation, and policy coherence.

Management that visibly prioritises safety and learning over blame is more likely to encourage reporting, especially when supported by consistent managerial behaviour, systemic reinforcement, and a congruent culture.

The second component—the culture-to-behaviour link—draws attention to the psychological and social mechanisms through which frontline workers internalise culture. This suggests that even in organisations with strong safety cultures, IRB may falter if individual workers do not perceive psychological safety, trust in management, or personal efficacy in reporting. Therefore, the model implies a need for targeted

strategies that bridge the gap between organisational values and individual perceptions, such as peer support systems, feedback loops, and recognition of reporting behaviour.

By explicitly including both behaviour and failure to behave (i.e., non-reporting), the model acknowledges that silence or inaction is itself a behavioural outcome with significant implications. This dual recognition invites a more nuanced understanding of IRB, where non-reporting is not merely the absence of action but a meaningful response to contextual cues. Consequently, organisations should consider not only how to promote reporting but also how to detect and

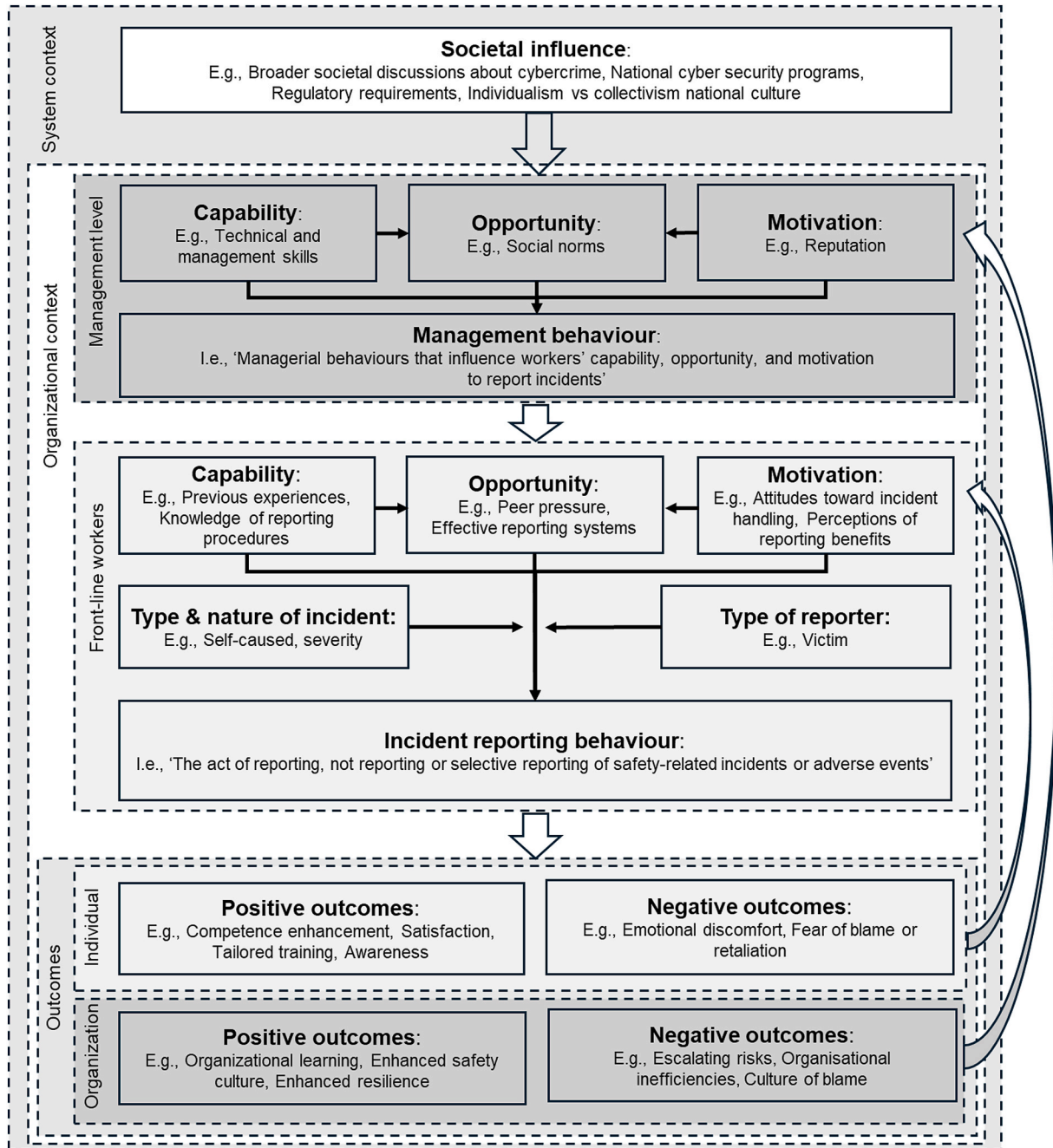


Fig. 2. Integrated multilevel model of cyber IRB. Rectangles represent key components of the model across different system levels (individual, organisational, and societal). Arrows indicate hypothesised relationships between components based on the literature. Bidirectional arrows represent reciprocal relationships, while feedback loops reflect how consequences of reporting influence future behaviour and contextual conditions. The model distinguishes between antecedent factors (organisational, psychological, technical, social, and motivational), incident reporting behaviour (IRB), and its consequences. IRB includes both reporting and non-reporting (underreporting) outcomes. The COM-B components (Capability, Opportunity, Motivation) structure the behavioural mechanisms linking cultural and organisational factors to reporting behaviour. Moderating factors, such as incident characteristics and reporter attributes, influence the strength and direction of these relationships.

address patterns of underreporting or selective reporting.

Finally, the inclusion of consequences and the moderating or mediating role of incident type adds a dynamic dimension to the model. It implies that the perceived or actual outcomes of reporting—such as disciplinary action, workload changes, or organisational learning—can reinforce or inhibit future behaviour. Moreover, the nature of the incident (e.g., severity, visibility, or attribution) may influence how cultural and individual factors interact. This suggests that interventions should be sensitive to incident typologies and tailored accordingly, recognising that a one-size-fits-all approach may be insufficient.

Our conceptual model builds upon and extends the CSCB framework developed by Sutton and Tompson (2024). While the CSCB framework outlines a three-part structure—cultural values, the culture-to-behaviour link, and cybersecurity-related behaviours—our model introduces two additional components that deepen the explanatory power of the framework in the context of IRB. First, by explicitly incorporating the outcomes of behaviour, the model captures the feedback loop through which outcomes of reporting (or underreporting) influence future behaviour, a dimension only implicitly addressed in the CSCB framework. Second, the model introduces incident type, nature, and who reports the incident, as potential moderators, or mediators, recognising that the incident, and therefore who reports it, may shape how cultural and individual factors interact to influence IRB. Furthermore, while the CSCB framework draws on the Theory of Planned Behaviour and the Awareness-Motivation-Capability model, our model integrates the well renowned COM-B model to offer a more granular behavioural lens. These additions not only align with the CSCB framework's emphasis on multilevel cultural influences but also enhance its applicability to safety-critical domains where reporting behaviour is both complex and consequential.

4. Discussion

This study set out to explore the multifaceted nature of IRB in organisational contexts, guided by five central research questions. Through an SLR and the development of an integrative, multilevel conceptual model, we provide a structured understanding of how cultural, organisational, and individual factors interact to shape IRB. The proposed model extends existing frameworks by incorporating not only cultural and behavioural dimensions, but also the outcomes of action or inaction (i.e., underreporting), as well as the moderating roles of incident characteristics and reporter attributes. In this final section, we discuss the implications of these findings in relation to the research questions, outlining how our model advances current theoretical and practical understandings of IRB and organisational cyber resilience. It is important to emphasise that the proposed model represents a theoretical synthesis derived from the literature rather than an empirically validated model. While grounded in a systematic review of existing studies, the relationships depicted have not been directly tested and should therefore be interpreted as a conceptual, theory-building framework that requires further empirical validation.

4.1. Definition and conceptual diversity of IRB

This systematic review reveals that IRB is a multifaceted construct with considerable variation in definitions across domains such as healthcare, cybersecurity, and aviation. This broad distribution underscores the relevance of IRB across domains and highlights the need for continued cross-sectoral research to address evolving challenges in safety and security. Among the 106 reviewed articles, only 41 provided explicit definitions, while 37 offered implicit ones, and 28 lacked a clear definition altogether. Despite this variability, several recurring elements emerged. IRB is most often framed as 'the act of reporting safety-related incidents or adverse events,' with frequent emphasis on its voluntary nature and its contribution to organisational learning and safety culture.

The definitional landscape reflects both individual and systemic

perspectives. Some definitions highlight personal motivation—such as willingness, intention, or responsibility—while others focus on procedural aspects like formal reporting mechanisms and compliance structures. This duality highlights the behavioural and institutional dimensions of IRB. Additionally, while some definitions include informal reporting (e.g., verbal disclosures), others restrict the concept to structured, system-based reporting.

Domain-specific emphases further illustrate the contextual nature of IRB. In healthcare, the focus is on patient safety and learning from clinical errors, often constrained by fear of blame and ambiguity about what constitutes a reportable event. In cybersecurity, IRB is framed within the 'human-as-a-sensor' paradigm, where employees report suspicious digital activity, yet face barriers such as credibility concerns and ethical dilemmas. Aviation literature emphasises voluntary reporting as a form of safety citizenship, embedded in mature safety cultures and formalised systems.

In sum, while no universal definition of IRB exists, the literature converges on core attributes: it is a behavioural act, often voluntary, aimed at disclosing safety-related events to enhance organisational learning, safety culture, and risk management. The definitional diversity reflects the interdisciplinary and context-sensitive nature of IRB, highlighting the need for conceptual clarity in both research and applied settings.

4.2. Conceptual relationship between IRB antecedents and barriers

The analysis of antecedents and barriers to IRB revealed a diverse and complex landscape of influencing factors. To facilitate interpretation and practical application, we first organised the antecedents into five overarching thematic clusters: organisational, psychological, technical, social, and motivational. Later, these were further clustered into the COM-factors (Capability, Opportunity, Motivation) of the COM-B framework. This structure provides a conceptual lens through which the interplay of individual, contextual, and systemic drivers can be better understood.

The analysis of barriers to IRB reveals a substantial conceptual overlap with antecedents, despite their distinct framing in the literature. Antecedents typically describe enabling conditions—such as psychological safety, leadership support, system usability, and perceived effectiveness—that foster a willingness to report. Barriers, conversely, often represent the absence or distortion of these same conditions, manifesting as fear of blame, lack of feedback, complexity of reporting systems, or distrust in organisational response. This duality suggests that antecedents and barriers are not mutually exclusive constructs, but rather interdependent dimensions of the same behavioural ecosystem. For example, while psychological safety is a known antecedent, its absence—expressed as fear of punishment—acts as a barrier. Similarly, leadership support enables reporting, whereas its absence contributes to underreporting. Therefore, a nuanced understanding of these constructs is essential for advancing both theoretical models and practical strategies aimed at improving incident reporting within organisations.

4.3. Impact of IRB and CSC on organisational cyber resilience

An important question that was posed at the beginning of this research was how CSC, through IRB, impacts the cyber resilience of organisations. At the organisational level, we found that IRB is overwhelmingly associated with positive consequences. These include enhanced learning and system-level improvements, improved decision-making, and increased cyber resilience. IRB also fosters better collaboration, policy refinement, and cultural transformation toward openness and shared responsibility.

Conversely, underreporting—highlighted in 18% of the articles reviewed—yields predominantly negative consequences (see, for example, Winsvold Prang & Jelsness-Jørgensen, 2014). These include missed learning opportunities, hindered prevention strategies, reduced

organisational awareness, and perpetuation of a culture of silence and blame. Underreporting also compromises data-driven safety improvements and may lead to legal and ethical failures.

The consequences also vary by stakeholder. While organisations benefit significantly from IRB, individuals often face negative repercussions such as fear of being punished by management for a late report, perceived ineffectiveness at defending the system, or a simple mistake due to fatigue. Nonetheless, some individual-level benefits were noted, including professional development, psychological closure, and a sense of contribution to safety.

4.4. Conceptual ambiguity of 'culture'

Culture, in the context of IRB, can be defined as: the shared values, beliefs, norms, attitudes, and behavioural expectations—shaped primarily at the organisational level—that influence how individuals and groups perceive, interpret, and respond to safety-related events, including willingness to report incidents. Across the reviewed studies in this SLR, the concept of culture emerged as one of the most frequently cited antecedents of IRB, appearing in 45 articles. The strong presence of culture highlights that reporting behaviour is not merely an individual decision but is deeply embedded in the broader cultural environment. A culture that values transparency, learning from errors, and psychological safety fosters conditions in which reporting is seen as constructive, rather than punitive. This reinforces the need for leadership to actively shape and sustain a 'just culture' that balances accountability with support. However, only a minority (approximately 20%) of the articles in our synthesis sample provided an explicit definition or detailed explanation of what culture entails in the context of reporting. In most cases, terms such as organisational culture (21 mentions), safety culture, or just culture were used without further conceptual clarification. This lack of definitional precision suggests that, while culture is widely acknowledged as a critical factor influencing IRB, it is often treated as a broad or implicit construct. The absence of consistent operationalisation limits comparability across studies and underscores the need for further investigations to define cultural dimensions relevant to IRB more rigorously.

While behavioural models such as the COM-B model primarily focus on the individual as the unit of analysis—explaining behaviour as a function of Capability, Opportunity, and Motivation—culture, as defined in this study, is predominantly situated at the organisational level. The SLR revealed that culture is most often described in terms of shared values, norms, beliefs, and practices that shape collective behaviour, particularly around safety and reporting. These cultural attributes—such as openness, psychological safety, and a practice of non-punitive responses—create the contextual environment in which individual behaviour occurs. In COM-B terms, culture can be understood as a meta-construct that influences both the Opportunity (e.g., social norms, leadership support) and Motivation (e.g., perceived consequences, trust) components. Moreover, culture can indirectly shape Capability by influencing access to training, clarity of procedures, and leadership modelling—factors that determine whether individuals feel competent and authorised to act. Thus, while COM-B provides a framework for understanding individual behaviour, culture provides the contextual scaffolding that enables or constrains those behaviours at scale. In this way, culture operates as a meta-construct that modulates all three COM-B components, not by replacing them, but by embedding them in a broader social and organisational context.

Integrating both perspectives allows for a more holistic understanding of IRB, bridging micro-level psychological mechanisms with macro-level organisational dynamics. It emphasises that interventions should not only target individual skills or attitudes, but also address the cultural conditions that enable or inhibit those behaviours. This alignment between micro-level behavioural mechanisms and macro-level cultural dynamics is essential for designing sustainable, system-wide improvements in safety reporting practices.

4.5. Multi-level influences on IRB

The findings of this study indicate that IRB is shaped by a constellation of factors that span multiple systemic levels. At the individual level, behavioural models such as COM-B highlight the importance of psychological capability, motivation, and perceived opportunity. These include personal attitudes, knowledge of reporting procedures, and confidence in the system. However, the SLR also reveals that many of the most influential antecedents—such as organisational culture, leadership support, and feedback mechanisms—are situated at the organisational level. These factors create the structural and normative environment in which individual behaviour is either enabled or constrained. Additionally, some studies reference national-level influences (e.g., societal norms, regulatory expectations), suggesting that IRB is embedded in a broader socio-cultural context (for example, see [Ebert et al., 2023](#)). This multi-level perspective underscores the need for integrated interventions that address not only individual behaviour change but also the organisational and systemic conditions that shape reporting practices.

4.6. Practical implications

Despite growing awareness, companies, government bodies, and institutions continue to face persistent cyber threats that severely impact an organisation's operations, finances, reputation, and its broader network of stakeholders. As the likelihood of cyber incidents increases, it is vital for organisations to build cyber resilience so that they can adapt swiftly and effectively to cyberattacks. This adaptive ability includes learning from cyber incidents, both from their own organisation as from others, and adjusting their systems and practices accordingly. Crucial to the organisation's adaptive capacity is the role of employee IRB, which remains inconsistent and infrequent.

The findings of this SLR offer several important implications for practice, particularly for organisations seeking to strengthen their incident reporting frameworks. While much of the existing literature has focused on identifying psychological antecedents to reporting, our synthesis highlights the importance of understanding how these factors interact and operate within broader organisational and societal systems. This perspective has direct consequences for how interventions should be designed, implemented, and evaluated.

As noted earlier in this section, there is a clear interdependency between antecedent factors and barriers to IRB: the absence of an antecedent factor often functions as a barrier. This insight is critical for designing multi-level interventions that not only promote enabling antecedents, but also actively dismantle obstacles. There is also evidence suggesting that antecedents should not be treated in isolation. Instead, they function as part of a dynamic system where the presence or absence of one factor can moderate the effect of another. This also has important implications for designing interventions: improving one area (e.g., system usability) may not yield results unless complementary factors (e.g., leadership support, feedback, or training) are also addressed.

A wide range of antecedents and barriers were identified that can either promote or hinder IRB. To determine which interventions should be prioritised, antecedent clusters and barriers were mapped onto the COM-B model, thereby informing the design of targeted strategies. The mapping revealed that Motivation-related barriers were the most prominent in the literature, suggesting that psychological and emotional factors are the primary inhibitors of reporting behaviour. These barriers include fear-based deterrents (e.g., fear of punishment, shame, guilt) and perceptions of futility (e.g., lack of feedback, absence of visible outcomes). Notably, both psychological and motivational antecedents also align with the Motivation component of the COM-B model. Psychological antecedents reflect an individual's sense of psychological safety and trust in the reporting process and its outcomes, which directly influences willingness to act. This reveals a duality: the absence of psychological safety (an antecedent) manifests as fear of repercussions

(a barrier). Similarly, motivational antecedents, such as perceived usefulness of reporting, attitudes toward reporting, and perceived behavioural control, further shape the intrinsic and extrinsic motivation to report. When the perceived usefulness is low, it becomes a barrier, as it can lead to a sense of futility, thereby discouraging reporting behaviour.

The mapping of the antecedents and barriers emphasises the need for multi-level interventions that prioritise the enhancement of psychological safety and motivation. Without addressing these foundational elements, efforts to improve capability or opportunity may fall short. Conversely, strengthening capability (e.g., through training) and opportunity (e.g., through user-friendly systems and supportive leadership) in alignment with motivational drivers, can reinforce psychological safety and intrinsic motivation. This reciprocal relationship highlights the need for integrated strategies that address all components of behaviour change.

4.6.1. Strategies for psychological safety

Cultivating a just CSC is essential for improving psychological safety within an organisation. A culture that is non-punitive, learning-oriented, and trust-based across department and organisation levels, can empower employees to report incidents without fear of blame or retaliation, and instead feel the opportunity to gain experience and grow. Organisations could nurture such a culture through a positively-framed security programme that is based on openness, trust, and empowerment and give the ownership, autonomy, and involvement to its employees (ENISA, 2017). Such a programme can help normalise reporting behaviour and reinforce the message that transparency is valued.

IRB can be further normalised with peer modelling and champion networks (Uchendu et al., 2021). The security champion role supports the security team in highlighting the security awareness messages, supporting the implementation of security policies, helping employees with adopting security behaviours, identifying their needs, and reporting back to the team. Moreover, as people are social creatures, peer influence and managerial expectations can encourage colleagues to conform to security norms (ENISA, 2017). To further instil confidence, organisations should align their practices with supportive legal frameworks and demonstrate consistent, non-punitive responses to past incidents. Ensuring job security and maintaining the credibility of individuals should send a powerful message, that reporting is not only safe, but respected and encouraged.

4.6.2. Strategies for motivation

To effectively motivate employees to report cybersecurity incidents, organisations must implement clear and responsive feedback mechanisms that demonstrate the value of reporting. When employees see that their input leads to meaningful action, they are more likely to engage and positively influence their colleagues to do the same. Providing constructive, non-judgmental feedback on what could have been done differently, helps employees to learn from their incidents (Pfeifer et al., 2023). This practical insight not only supports individual growth, but also contributes to collective learning across the organisation.

Equally important is closing the feedback loop. Informing employees about the operational impact of their reports, reinforces the perception that their action matters. This validation strengthens trust in the system, making future reporting more likely (Clarkson et al., 2017; Muthuswamy & Esakki, 2024). Additionally, creating space and time to openly discuss and share cybersecurity lessons with others, can encourage knowledge sharing and ensure that employees take individual and collective responsibility for their security behaviours (ENISA, 2017).

Consistent training plays an essential role in IRB. By providing managers and employees with the knowledge to recognize risks and understand when and how to respond to a cyber incident, training can enhance their sense of control and confidence in the reporting process, which are key components of perceived behavioural control. As such, training can help prevent cyber incidents or reduce its potential impact,

reducing the overall vulnerability of the organisation (ENISA, 2017; Trim & Upton, 2013).

4.6.3. Leadership support

Effective implementation of both psychological and motivational strategies for IRB requires leadership at all levels of the organisation. Leaders play a critical role in shaping a just CSC by setting clear norms, modelling desired behaviours, guiding, and supporting employees, and allocating the necessary resources to sustain these strategies (ENISA, 2017; Hu et al., 2012). In this context, establishing specific, realistic, and measurable goals, combined with clear communication about expectations, roles, and responsibilities, is essential for the success of any security programme.

Leadership may also more directly influence employees' willingness to report incidents. For instance, Yusuf and Irwan (2021) emphasise that transactional leadership, which focuses primarily on compliance, is less effective than transformational leadership, which builds trust and fosters collaboration toward shared goals. Their study found that nurses were more likely to report incidents when their lead nurse was supportive, demonstrated strong managerial skills, and maintained frequent, direct contact with staff. These findings illustrate how leadership behaviour may signal organisational commitment and build trust. Without visible and consistent leadership support, initiatives aimed at empowering and encouraging employees to report will likely fail.

4.6.4. Societal influence

Although societal influences are outside of an organisation's control, it is important for organisations to be aware of societal developments and their relevance for organisational and individual factors related to IRB. Societal discourse and national regulations play a significant role in shaping the norms, attitudes, and behaviours at both organisational and individual levels. (Inter)national public discussions about cybersecurity raise awareness and influence how people perceive cyber threats, which in turn affects internal conversations and awareness within organisations (ENISA, 2017). These internal dynamics can subsequently influence the development or refinement of organisational and national cybersecurity policies.

National regulations define the boundaries within which organisations operate and often serve as a catalyst for the implementation or tightening of cybersecurity measures. They also promote collaboration and alignment between organisations, encouraging knowledge sharing and mutual adaptation in response to evolving cyber threats.

As with the antecedents and barriers, the absence of such societal stimuli, including public discourse and national regulations, can function as barrier. Without these external drivers, awareness may remain low and cybersecurity may be vague or entirely lacking, increasing the vulnerability of organisations and society as whole to cyber threats. This highlights the dual role of societal influence: it can both enable and, when absent, hinder organisational preparedness.

While cyber threats often remain invisible to many, delaying or even fully preventing societal discussions, their consequences can be profound and undermine both social and physical infrastructures at every level. These impacts, whether direct or indirect, affect us all. To remain resilient, organisations must therefore adopt a proactive and continuously-updated approach to cyber incidents, independent of the pace of public debate or the evolution of national regulations.

4.7. Limitations and future research

The SLR identified a wide range of factors that influence IRB and are antecedent to or result of it, and revealed meaningful patterns of interaction among them. It is important, however, to acknowledge that the review does not provide insight into the relative strength or statistical significance of these relationships. The synthesis was qualitative in nature, included theoretical and conceptual articles, focusing on the presence and co-occurrence of factors across studies rather than on

effect sizes or predictive power. As such, although certain antecedents—such as system usability, psychological safety, and leadership support—appear frequently and in combination, this frequency should not be interpreted as evidence of causal weight. Future empirical research is needed to quantify the influence of these factors, assess their interactions statistically, and determine which combinations most strongly predict IRB in specific organisational contexts. This may include survey-based studies to operationalise key constructs and assess their relationships, longitudinal designs to examine feedback mechanisms over time, and experimental studies to evaluate the impact of targeted interventions on reporting behaviour. Finally, comparative studies across domains (e.g., healthcare, aviation, and cybersecurity) would help assess the generalisability of the model and identify context-specific mechanisms.

Further, it is important to acknowledge the heterogeneity of study contexts included in this review, which influences how the findings should be interpreted. The systematic review encompassed research from multiple domains—such as cybersecurity, healthcare, and aviation—each characterised by distinct operational environments, regulatory frameworks, and cultural norms. This diversity inevitably limits the feasibility of direct statistical comparisons between sectors. In addition, the use of a single database (Scopus) may have limited the inclusion of studies indexed in more specialised databases, which should also be considered when interpreting the scope and coverage of the findings.

Rather than attempting to aggregate or compare these contexts quantitatively, our synthesis emphasises patterns and conceptual themes that recur across studies. This approach aligns with the objectives of the review, which are to identify common factors influencing incident reporting behaviour and to develop a conceptual framework that integrates insights from different domains. By focusing on thematic convergence rather than numerical equivalence, we ensure that the conclusions drawn are both methodologically sound and relevant to the interdisciplinary nature of the research questions.

While tools such as ASReview and MS Copilot present promising opportunities for accelerating literature review processes, their limitations necessitate scrutiny. ASReview's stopping criteria are not always well-calibrated to the size of the dataset, which can result in the omission of a sizeable number of relevant papers, thereby compromising recall. MS Copilot, although capable of detecting implicit cues in some texts, operates as a black-box system whose heuristic-driven outputs often lack transparent justification. This raises concerns about the trustworthiness and reproducibility of its findings. While tools such as MS Copilot can support structured data extraction, their outputs may not be fully deterministic, as they can vary depending on model updates, prompt formulation, and system configurations. As a result, repeating the analysis using the same prompts may yield slight variations in extracted information, and the use of alternative LLMs could potentially lead to differences in interpretation or emphasis. To mitigate this risk, all AI-generated outputs in this study were systematically reviewed and validated by the researchers, and key coding decisions were guided by a predefined codebook. This human-in-the-loop approach ensured consistency and interpretative control, reducing reliance on any single model output. Nevertheless, the potential variability introduced by LLMs should be acknowledged as a limitation and an area for further methodological standardisation in future research. The absence of access to the Application Programming Interface (API) of these tools further restricts the ability to engage in iterative refinement. Moreover, privacy vulnerabilities such as the echo-leak issue³ identified in MS Copilot pose additional risks, particularly in sensitive research contexts. While performance can be enhanced through advanced prompt engineering and manual validation, this also fosters a growing dependence on LLMs, potentially undermining traditional academic skills and

critical engagement with source material. Finally, in the absence of benchmarking against alternative LLMs, it remains uncertain whether MS Copilot is the most suitable tool for this type of research task.

4.8. Conclusion

Cyber resilience requires, amongst other things, the capacity to adapt behaviours and systems using knowledge gained from previous incidents in one's own and each others' organisations. Harm to business operations, finances, or reputation can be reduced by IRB and by enabling CSC to support the collection, analysis, sharing, and use of incident reports to improve organisational cyber resilience. IRB is defined in the general literature as 'the act of reporting safety-related incidents or adverse events,' often emphasising its voluntary nature and its role in organisational learning often within a formal system. This SLR has shown that IRB is a complex, context-sensitive behaviour shaped by a constellation of psychological, organisational, technical, social, and motivational factors.

Barriers to IRB can be psychological, organisational, and cultural, with lack of feedback and the resulting perception that reporting does not lead to change mentioned most often. Another factor that is mentioned often is blame culture. Blame culture is characterised by fear of punishment, lack of psychological safety, and other organisational tendencies to assign fault rather than learn from mistakes. Employees may perceive incident reporting as a threat to their reputation or job security. Blame culture and peer pressure erodes trust in reporting systems, as employees doubt whether their reports will be used constructively or punitively. IRB can be encouraged, on the other hand, by providing feedback to reporters of incidents, reducing the time burden of reporting, and rewarding of incident reports. These factors do not operate in isolation; rather, they interact in ways that can amplify or inhibit reporting behaviour. For example, the positive impact of a user-friendly reporting system is contingent on the presence of psychological safety, while feedback mechanisms can enhance the perceived usefulness of reporting and sustain motivation over time.

To capture these dynamics, we developed an integrative, multilevel conceptual model of IRB that builds on and extends the Cybersecurity Culture-Behaviour (CSCB) framework developed by Sutton and Tompson (2024). Our model incorporates the COM-B framework to structure behavioural influences and explicitly includes the outcomes of reporting (or underreporting) as well as the moderating roles of incident and reporter. This layered approach allows for a more nuanced understanding of how system-level structures, culture, and individual perceptions converge to shape reporting outcomes.

Practically, this work underscores the need for multi-level interventions that go beyond individual training or awareness campaigns. Organisations must foster a just culture that prioritises learning over blame, implement feedback mechanisms that validate and reinforce reporting, and ensure that reporting systems are accessible, confidential, and easy to use. Leadership plays a pivotal role in modelling desired behaviours and allocating resources to sustain these efforts. Moreover, societal discourse and national regulations can serve as external drivers that shape internal norms and expectations around cybersecurity and reporting.

Finally, while this SLR provides a rich conceptual foundation, it does not quantify the relative strength of the relationships identified. Future research should employ empirical methods—such as longitudinal studies, multilevel modelling, and experimental designs—to assess the predictive power of specific concepts and interactions. Such work is essential to move from descriptive insight to actionable evidence and to enable organisations to prioritise interventions that most effectively enhance cyber resilience through improved IRB.

³ <https://www.aim.security/lp/aim-labs-echoleak-blogpost>.

Declaration of generative AI and AI-assisted technologies in the writing process

During the preparation of this work, the authors used ASReview and Microsoft Copilot to assist and accelerate certain steps in the literature review process, such as screening and structured data extraction. These tools were employed strictly as supportive aids under human supervision. After using these tools, the authors reviewed, verified, and edited all content as needed and take full responsibility for the final manuscript. Importantly, no consumer AI endpoints or public model-training pipelines received our data. ASReview was operated locally/offline, and MS Copilot was used within an enterprise MS 365 tenant under organisational data governance controls, ensuring compliance with security and confidentiality requirements. The authors affirm that all methodological decisions, interpretations, and conclusions presented in this paper were made by the research team and not by AI systems.

CRedit authorship contribution statement

Rick van der Kleij: Conceptualization, Formal analysis, Funding acquisition, Investigation, Methodology, Project administration, Supervision, Visualization, Writing – original draft, Writing – review & editing. **Olivier Spinnler:** Formal analysis, Methodology, Software, Writing

– original draft. **Julia Broderick-Hale:** Formal analysis, Writing – original draft. **Katie Hendriks:** Conceptualization, Funding acquisition, Methodology, Supervision. **Anthonie Drenth:** Conceptualization, Methodology, Writing – review & editing. **Joshua van Wijgerden:** Methodology, Validation, Writing – review & editing.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests. Rick van der Kleij reports financial support was provided by Netherlands Organisation for Applied Scientific Research. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This research was partly funded by the Dutch National Cyber Security Centre (NCSC). The authors would like to thank Dianne van Hemert, Kees van Dongen, Sander Ebberts, Esger ten Thij, Francien Baijanova and the participants of the validation workshop for their valuable contributions to this paper.

Appendix A. Synthesis sample

Table A1

Synthesis sample, including author(s), title, year, and domain, in alphabetical order.

#	Author(s)	Title	Year	Domain
1	AbuAlRub, R. F., Al-Akour, N. A., & Alatari, N. H.	Perceptions of reporting practices and barriers to reporting incidents among registered nurses and physicians in accredited and nonaccredited Jordanian hospitals	2015	Healthcare (nursing)
2	Adjekum, D. K., Keller, J., Walala, M., Christensen, C., DeMik, R. J., Young, J. P., & Northam, G. J.	An Examination of the Relationships between Safety Culture Perceptions and Safety Reporting Behavior among Non-Flight Collegiate Aviation Majors	2016	Aviation
3	Afolalu, O., Jordan, S., & Kyriacos, U.	Medical error reporting among doctors and nurses in a Nigerian hospital: A cross-sectional survey	2021	Healthcare (nursing)
4	Ahola, K., Butavicius, M., McCormac, A., & Sturman, D.	Hey “CSIRT”, should I report this? Investigating the factors that influence employees to report cyber security incidents in the workplace	2025	Cybersecurity
5	Ahola, K., Sturman, D., Scott, N., Pattinson, M., Reeves, A., Butavicius, M., & McCormac, A.	Improving the Human Firewall: Exploring the Factors that Influence Cyber-Security Incident Reporting	2025	Cybersecurity
6	Alshaikh, M.	Developing cybersecurity culture to influence employee behavior: A practice perspective	2020	Cybersecurity
7	Anderson, J., Kodate, N., Walters, R., & Dodds, A.	Can incident reporting improve safety? Healthcare practitioners' views of the effectiveness of incident reporting	2013	Healthcare (acute and mental health hospitals)
8	Atwal, A., Phillip, M., & Moorley, C.	Senior nurses' perceptions of junior nurses' incident reporting: A qualitative study	2020	Healthcare (nursing)
9	Aydeniz, E., & Intepeler, S.	Examining the Effectiveness of Strategies Developed to Create an Error Reporting Culture	2021	Healthcare (nursing)
10	Bagenal, J., Sahnan, K., & Shantikumar, S.	Comparing the Attitudes and Knowledge Toward Incident Reporting in Junior Physicians and Nurses in a District General Hospital	2016	Healthcare
11	Balcerzak, T.	“Just culture”? Conflicts of interest in the investigation of aviation accidents	2017	Aviation
12	Ballreich, F., Volkamer, M., Müllmann, D., Berens, B., Häußler, E., & Renaud, K.	Encouraging Organisational Information Security Incident Reporting	2023	Cybersecurity
13	Bhatti, M.A. & Jamil, S.	Factors Effecting Cyber Incident Occurrence: Mediating Role of Cyber Incident Reporting Mechanism	2023	Cybersecurity
14	Bidgoli, M., & Grossklags, J.	End user cybercrime reporting: what we know and what we can do to improve it	2016	Cybersecurity
15	Birkeli, G. H., Jacobsen, H. K., & Ballangrud, R.	Nurses' experience of incident reporting culture before and after implementing the Green Cross method: A quality improvement project	2022	Healthcare (nursing)
16	Briggs, P., Jeske, D., & Coventry, L.	The Design of Messages to Improve Cybersecurity Incident Reporting	2017	Cybersecurity
17	Cerrone, V., Andretta, V., Prendin, A., Ilardi, B., Bonetti, C., Capunzo, M., & Cascella, M.	Effectiveness of Incident Reporting Tools in Ensuring Patient Safety: A Systematic-Narrative Hybrid Review.	2025	Healthcare (nursing)
18	Chen, L. C., Wang, L. H., Redley, B., Hsieh, Y. H., Chu, T. L., & Han, C. Y.	A Study on the Reporting Intention of Medical Incidents: A Nursing Perspective	2018	Healthcare (nursing)
19	Chen, X., Doublet, S., Sergeeva, A., Lenzini, G., Koenig, V., & Distler, V.	What Motivates and Discourages Employees in Phishing Interventions: An Exploration of Expectancy-Value Theory	2024	Cybersecurity

(continued on next page)

Table A1 (continued)

#	Author(s)	Title	Year	Domain
20	Chiang, H. Y., Hsiao, Y. C., Lin, S. Y., & Lee, H. F.	Incident reporting culture: scale development with validation and reliability and assessment of hospital nurses in Taiwan	2011	Healthcare (nursing)
21	Chiang, H. Y., Lee, H. F., Lin, S. Y., & Ma, S. C.	Factors contributing to voluntariness of incident reporting among hospital nurses	2019	Healthcare (nursing)
22	Chiang, H.-Y., Lin, S.-Y., Hsu, S.-C., & Ma, S.-C.	Factors determining hospital nurses' failures in reporting medication errors in Taiwan	2010	Healthcare (nursing)
23	Clarkson, L., Naweed, A., & Whale, J.	The minority report: Hazard reporting in an Australian University	2017	Education
24	Da Silva da Paiva, M., Popim, R. C., Melleiro, M. M., Tronchim, D. M. R., Lima, S. A. M., & Juliani, C. M. C. M.	The reasons of the nursing staff to notify adverse events	2014	Healthcare
25	Da Veiga, A., & Eloff, J.	A framework and assessment instrument for information security culture	2010	Cybersecurity
26	Da Veiga, A., & Eloff, J.	An Information Security Governance Framework	2007	Cybersecurity
27	Dalky, A. A., Oweidat, I. A., Abuzaid, S. R., Khalifeh, A. H., & AlBashtawy, M.	Exploring the influence of nurses' demographics and hospital work environment on medical error reporting practices in Jordan: a cross-sectional study	2024	Healthcare (nursing)
28	Darveau, K., & Hannon, D.	Barriers and Facilitators to Voluntary Reporting and Their Impact on Safety Culture	2017	Aviation and railroad industries
29	Del Puerto, C.	Nurses' Medication Administration Error, Reporting Practices and Challenges in Tertiary Hospitals: Descriptive analysis	2024	Healthcare (nursing)
30	Dhamanti, I., Leggat, S., Barraclough, S., & Rachman, T.	Factors contributing to under-reporting of patient safety incidents in Indonesia: leaders' perspectives.	2022	Healthcare (hospital setting in Indonesia)
31	Ebert, N., Schaltegger, T., Ambuehl, B., Schöni, L., Zimmermann, V., & Knieps, M.	Learning from safety science: A way forward for studying cybersecurity incidents in organisations	2023	Cybersecurity
32	Fernandes, P., Pereira, R., & Wiedenhöft, G.	The Effect of Organisational Cultures on Relationships between IT Governance and Individual Behavior	2023	Cybersecurity
33	Filtiness, A., Goode, N., & Cook, R.	Incident Reporting Culture in Recreational Hot Air Ballooning	2015	Aviation (hot air ballooning)
34	Franz, A.	Why Do Employees Report Cyber Threats? Comparing Utilitarian and Hedonic Motivations to Use Incident Reporting Tools	2022	Cybersecurity
35	Gartmeier, M., Ottl, E., Bauer, J., & Berberat, P.	Learning from errors: critical incident reporting in nursing	2017	Healthcare (nursing)
36	Gcaza, N., & Thomson, K.	Factors contributing to the successful development of cyber safety education for foundation phase children: a systematic literature review	2025	Education
37	Gifford, M., & Anderson, J.	Barriers and Motivating Factors in Reporting Incidents of Assault in Mental Health Care	2010	Healthcare (nursing)
38	Gilbey, A., Tani, K., & Hong Kan Tsui, W.	Outcome Knowledge and Under-reporting of Safety Concerns in Aviation	2016	Aviation
39	Hamed, M., & Konstantinidis, S.	Barriers to Incident Reporting among Nurses: A Qualitative Systematic Review	2022	Healthcare (nursing)
40	Han, N., Jeong, S. H., Lee, M. H., & Kim, H. S.	Impacts of Just Culture on Perioperative Nurses' Attitudes and Behaviors With Regard to Patient Safety Incident Reporting: Cross-Sectional Nationwide Survey	2024	Healthcare (nursing)
41	Hewitt, T., Chreim, S., & Forster, A.	Sociocultural Factors Influencing Incident Reporting Among Physicians and Nurses: Understanding Frames Underlying Self- and Peer-Reporting Practices	2017	Healthcare
42	Hong, S., & Li, Q.	The reasons for Chinese nursing staff to report adverse events: a questionnaire survey	2017	Healthcare (nursing)
43	Hooper, P., Kocman, D., Carr, S., & Tarrant, C.	Junior doctors' views on reporting concerns about patient safety: a qualitative study	2015	Healthcare
44	Hutchinson, A., Young, T. A., Cooper, K. L., McIntosh, A., Karnon, J. D., Scobie, S., & Thomson, R. G.	Trends in healthcare incident reporting and relationship to safety and quality data in acute hospitals: results from the National Reporting and Learning System	2009	Healthcare – specifically acute hospitals in England
45	Jausan, M., Silva, J., & Sabatini, R.	A holistic approach to evaluating the effect of safety barriers on the performance of safety reporting systems in aviation organisations	2017	Aviation
46	Jennings, P., & Stella, J.	Barriers to incident notification in a regional prehospital setting	2011	Healthcare
47	Karlsson, M., Karlsson, F., Åström, J., & Denk, T.	The effect of perceived organisational culture on employees' information security compliance	2022	Cybersecurity
48	Kim, N., & Kwak, S.	Relationship between nurses' critical thinking disposition and patient safety incident reporting: The mediating role of patient safety culture in a comprehensive nursing service ward	2024	Healthcare (nursing)
49	Kioulepoglou, P., Nikolaidis, V., David, K. & Makris, I.	Investigating incident under-reporting in aviation: Qualitative insights among Greek pilots	2025	Aviation
50	Ko, E. S., & Kang, K. J.	Effects of Nurses' Incident Reporting Attitude, Perception of Importance on Patient Safety Management, and Patient Safety Culture on the Reporting of Patient Safety Events	2023	Healthcare (nursing)
51	Koning, L., Junger, M., & Veldkamp, B.	Reporting fraud victimization to the police: factors that affect whether victims report	2025	Cybersecurity
52	Kreckler, S., Catchpole, K., McCulloch, P., & Handa, A.	Factors influencing incident reporting in surgical care	2009	Healthcare – specifically surgical care in a UK teaching hospital
53	Kurihara, M., Nagao, Y., & Tokuda, Y.	Incident reporting among physicians-in-training in Japan: A national survey	2021	Healthcare
54	Kwak, Y., Lee, S., Damiano, A., & Vishwanath, A.	Why do users not report spear phishing emails?	2020	Cybersecurity
55	Lee, E.	Safety climate and attitude toward medication error reporting after hospital accreditation in South Korea	2016	Healthcare (nursing)
56	Lee, J., Havaei, F., Hirani, S., & Adhami, N.	Nurses' Workplace Violence Reporting Behaviours and Reasons for Not Formally Reporting: A Cross-Sectional Secondary Analysis	2024	Healthcare (nursing)
57	Lee, W., Kim, S. Y., Lee, S. I., Lee, S. G., Kim, H. C., & Kim, I.	Barriers to reporting of patient safety incidents in tertiary hospitals: A qualitative study of nurses and resident physicians in South Korea	2018	Healthcare (nursing)

(continued on next page)

Table A1 (continued)

#	Author(s)	Title	Year	Domain
58	Louis, M. Y., Hussain, L. R., Dhanraj, D. N., Khan, B. S., Jung, S. R., Quiles, W. R., ... & Klarquist, L. J.	Improving Patient Safety Event Reporting Among Residents and Teaching Faculty	2016	Healthcare
59	Martowirono, K., Jansma, J. D., van Luijk, S. J., Wagner, C., & Bijnen, A. B.	Possible solutions for barriers in incident reporting by residents	2012	Healthcare
60	McCoy, B., Stephens, G., & Stevens, K. J.	An Investigation of the Impact of Corporate Culture on Employee Information Systems Security Behaviour	2009	Cybersecurity
61	Mehanna, D., El Gerges, N., Chalhoub, M., & Daou, R.	Barriers to medication administration error reporting in a tertiary hospital in Lebanon	2024	Healthcare (nursing)
62	Moumtzoglou, A.	Factors impeding nurses from reporting adverse events: Adverse events in nursing	2010	Healthcare (nursing)
63	Mukherjee, S., Roy, S., & Era, N.	Safety incident reporting and barriers (SIRaB) study: Strategies and approaches for investigating patient safety events in a hospital set-up	2024	Healthcare
64	Munro, V.	Why do nurses neglect to report violent incidents?	2002	Healthcare (nursing)
65	Nasir, A., Arshah, R. A., Ab Hamid, M. R., & Fahmy, S.	An analysis on the dimensions of information security culture concept: A review	2019	Cybersecurity
66	Nurdin, D., & Wibowo, A.	Barriers to reporting patient safety incident in healthcare workers: Integrative literature review	2021	Healthcare (nursing)
67	Patterson, C., Nurse, J., & Franqueira, V.	"I don't think we're there yet": The practices and challenges of organisational learning from cyber security incidents	2024	Cybersecurity
68	Pfeifer, L., Vessey, J., Cazzell, M., Ponte, P. R., & Geyer, D.	Relationships among psychological safety, the principles of high reliability, and safety reporting intentions in pediatric nursing	2023	Healthcare (nursing)
69	Pfeiffer, Y., Briner, M., Wehner, T., & Manser, T.	Motivational antecedents of incident reporting: evidence from a survey of nurses and physicians	2013	Healthcare (nursing)
70	Pfeiffer, Y., Manser, T., & Wehner, T.	Conceptualising barriers to incident reporting: a psychological framework	2010	Healthcare (specifically hospitals and clinical settings)
71	Pilavakis, N., Jenkins, A., K��kcian, N., & Vaniea, K.	"I didn't click": What users say when reporting phishing	2023	Cybersecurity
72	Pollini, A., & Ciccone, A.	The Hidden Potential of an Incident. Designing for Cybersecurity Incident Reporting	2024	Cybersecurity
73	Prang, I. W., & Jelsness-J��rgensen, L. P.	Should I report? A qualitative study of barriers to incident reporting among nurses working in nursing homes	2014	Healthcare (nursing)
74	Pratama, G., & Caponecchia, C.	Examining the influence of national culture on aviation safety: A systematic review	2025	Aviation
75	Rahman, M. A., Carbutar, B., & Topkara, M.	Assessing the cyber-trustworthiness of human-as-a-sensor reports from mobile devices	2017	Cybersecurity
76	Rashed, A., & Hamdan, M.	Physicians' and Nurses' Perceptions of and Attitudes Toward Incident Reporting in Palestinian Hospitals	2019	Healthcare
77	Ruighaver, A. B., Maynard, S. B., & Chang, S.	Organisational security culture: Extending the end-user perspective	2007	Cybersecurity
78	Sato, K., Wakabayashi, T., Kiyoshi-Teo, H., & Fukahori, H.	Factors associated with nurses' reporting of patients' aggressive behavior: A cross-sectional survey	2013	Healthcare (nursing)
79	Schectman, J., & Plews-Ogan, M.	Physician Perception of Hospital Safety and Barriers to Incident Reporting	2006	Healthcare
80	Sieberichs, S., & Kluge, A.	How Just Culture and Personal Goals Moderate the Positive Relation between Commercial Pilots' Safety Citizenship Behavior and Voluntary Incident Reporting	2021	Aviation
81	Sieberichs, S., & Kluge, A.	Why Commercial Pilots Voluntarily Report Self-Inflicted Incidents: A Qualitative Study With Aviation Safety Experts	2021	Aviation
82	Smith, K. S., Harris, K. M., Potters, L., Sharma, R., Mutic, S., Gay, H. A., ... & Terezakis, S.	Physician Attitudes and Practices Related to Voluntary Error and Near-Miss Reporting	2014	Healthcare
83	Snijders, C., Kollen, B. J., van Ling, R. A., Fetter, W. P., Molendijk, H., & NEOSAFE Study Group.	Which aspects of safety culture predict incident reporting behavior in neonatal intensive care units? A multilevel analysis	2009	Healthcare – specifically neonatal intensive care units (NICUs)
84	Soleimani, F.	Learning from mistakes in New Zealand hospitals: what else do we need besides "no-fault"?	2006	Healthcare
85	Song, C., Wang, G., & Wu, H.	Frequency and barriers of reporting workplace violence in nurses: An online survey in China	2021	Healthcare (nursing)
86	Sutton A., & Tompson, L.	Towards a cybersecurity culture-behaviour framework: A rapid evidence review	2025	Cybersecurity
87	Szymusiak, J., Walk, T. J., Benson, M., Hamm, M., Zickmund, S., Gonzaga, A. M., & Bump, G. M.	A Qualitative Analysis of Resident Adverse Event Reporting: What's Holding Us Back	2019	Healthcare
88	Tabak, N., & Fleishman, S.	The intention to report medication error	2011	Healthcare (nursing)
89	Throckmorton, T., & Etchegaray, J.	Factors Affecting Incident Reporting by Registered Nurses: The Relationship of Perceptions of the Environment for Reporting Errors, Knowledge of the Nursing Practice Act, and Demographics on Intent to Report Errors	2007	Healthcare (nursing)
90	Tricarico, P., Castriotta, L., Battistella, C., Bellomo, F., Cattani, G., Grillone, L., ... & Brusaf��rro, S.	Professional attitudes toward incident reporting: can we measure and compare improvements in patient safety culture?	2017	Healthcare (hospital setting)
91	Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S.	Developing a cyber security culture: Current practices and future needs	2021	Cybersecurity
92	van Marum, S., Verhoeven, D., & de Rooy, D.	The Barriers and Enhancers to Trust in a Just Culture in Hospital Settings: A Systematic Review	2022	Healthcare
93	Van Steen, T., Del-Real, C., & Van den Berg, B.	What Works Well? A Safety-II Approach to Cybersecurity	2024	Cybersecurity
94	Varallo, F., Passos, A., De Nadai, T., & De Carvalho Mastroianni, P.	Incidents reporting: barriers and strategies to promote safety culture	2018	Healthcare
95	Vielberth, M., Englbrecht, L., & Pernul, G.	Improving data quality for human-as-a-security-sensor. A process driven quality improvement approach for user-provided incident information	2021	Cybersecurity

(continued on next page)

Table A1 (continued)

#	Author(s)	Title	Year	Domain
96	Vrbnjak, D., Denieffe, S., O'Gorman, C., & Pajnkihar, M.	Barriers to reporting medication errors and near misses among nurses: A systematic review	2016	Healthcare (nursing)
97	Walsh, K., Burns, C., & Antony, J.	Electronic adverse incident reporting in hospitals	2010	Healthcare
98	Waring, J.	A qualitative study of the intra-hospital variations in incident reporting	2004	Healthcare
99	Waring, J.	Beyond blame: cultural barriers to medical incident reporting	2005	Healthcare
100	Waters, N. F., Hall, W. A., Brown, H., Espezel, H., & Palmer, L.	Perceptions of Canadian labour and delivery nurses about incident reporting: A qualitative descriptive focus group study	2012	Healthcare (nursing)
101	Wawersik, D., & Palaganas, J.	Organisational Factors That Promote Error Reporting in Healthcare: A Scoping Review	2022	Healthcare (nursing)
102	Wiley, A., McCormac, A., & Calic, D.	More than the individual: Examining the relationship between culture and Information Security Awareness	2020	Cybersecurity
103	Williams, S., Phipps, D., & Ashcroft, D.	Examining the attitudes of hospital pharmacists to reporting medication safety incidents using the theory of planned behaviour	2015	Healthcare – specifically hospital pharmacy
104	Xu, Y., He, N., Lu, W., & Fluke, J.	Understanding factors associated with barefoot social workers' decision making in assessing and reporting child physical abuse in China	2021	Healthcare
105	Yusuf, Y., & Irwan, A.	The influence of nurse leadership style on the culture of patient safety incident reporting: a systematic review	2021	Healthcare (nursing)
106	Zhao, X., Zhao, S., Liu, N., & Liu, P.	Willingness to Report Medical Incidents in Healthcare: a Psychological Model Based on Organisational Trust and Benefit/Risk Perceptions	2021	Healthcare

Data availability

Data will be made available on request.

References

Adamse, I., Eichelsheim, V., Blokland, A., & Schoonmade, L. (2024). The risk and protective factors for entering organized crime groups and their association with different entering mechanisms: A systematic review using ASReview. *European Journal of Criminology*, 21(6), 859–886. <https://doi.org/10.1177/14773708241250278>

Adjekum, D. K., Keller, J., Walala, M., Christensen, C., DeMik, R. J., Young, J. P., & Northam, G. J. (2016). An examination of the relationships between safety culture perceptions and safety reporting behavior among non-flight collegiate aviation majors. *International Journal of Aviation, Aeronautics, and Aerospace*, 3(3). <https://doi.org/10.15394/ijaaa.2016.1134>. Article 4.

Ahmed, M. F., Molla, A. H., Uddin, M. R., & Chowdhury, T. R. (2023). Advancing cyber resilience: Bridging the divide between cyber security and cyber defense. *International Journal for Multidisciplinary Research*, 5(6).

Ahola, K., Butavicius, M., McCormac, A., & Sturman, D. (2025). "Hey CSIRI, should I report this?" investigating the factors that influence employees to report cyber security incidents in the workplace. *Information & Computer Security*, 33(2), 242–266. <https://doi.org/10.1108/ICS-11-2023-0214>

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, 98, Article 102003. <https://doi.org/10.1016/j.cose.2020.102003>

Anderson, J. E., Kodate, N., Walters, R., & Dodds, A. (2013). Can incident reporting improve safety? Healthcare practitioners' views of the effectiveness of incident reporting. *International Journal for Quality in Health Care*, 25(2), 141–150. <https://doi.org/10.1093/intqhc/mzt009>

Araujo, M. S. D., Machado, B. A. S., & Passos, F. U. (2024). Resilience in the context of cyber security: A review of the fundamental concepts and relevance. *Applied Sciences*, 14(5), 2116. <https://doi.org/10.3390/app14052116>

Atkinson, C. F. (2024). Cheap, quick, and rigorous: Artificial intelligence and the systematic literature review. *Social Science Computer Review*, 42(2), 376–393. <https://doi.org/10.1177/08944393221118958>

Ballreich, F. L., Volkamer, M., Müllmann, D., Berens, B. M., Häußler, E. M., & Renaud, K. V. (2023). Encouraging organisational information security incident reporting. In *Proceedings of the European symposium on useable security* (pp. 224–236).

Basnyat, S., Chozos, N., & Palanque, P. (2006). Multidisciplinary perspective on accident investigation. *Reliability Engineering & System Safety*, 91(12), 1502–1520. <https://doi.org/10.1016/j.res.2005.11.039>

Bernard, N., Sagawa, J. Y., Bier, N., Lihoreau, T., Pazard, L., & Tannou, T. (2025). Using artificial intelligence for systematic review: The example of elicitor. *BMC Medical Research Methodology*, 25. <https://doi.org/10.1186/s12874-025-02528-y>. Article 75.

Boheemen, P. van, Munnichs, G., Kool, L., Diercks, G., Hamer, J., & Vos, A. (2020). *Cyberweerbaar met nieuwe technologie – Kans en noodzaak van digitale innovatie*. Rathenau Instituut. Den Haag.

Bolaños, F., Salatino, A., Osborne, F., & Motta, E. (2024). Artificial intelligence for literature reviews: Opportunities and challenges. *Artificial Intelligence Review*, 57. <https://doi.org/10.1007/s10462-024-10902-3>. Article 259.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp0630a>

Briggs, P., Jeske, D., & Coventry, L. (2017). The design of messages to improve cybersecurity incident reporting. In *Human aspects of information security, privacy and trust* (pp. 3–13). ^{*} Springer International Publishing.

Brown, S. A., Upchurch, S. L., & Acton, G. J. (2003). A framework for developing a coding scheme for meta-analysis. *Western Journal of Nursing Research*, 25(2), 205–222. <https://doi.org/10.1177/0193945902250038>

Callaghan, M., Müller-Hansen, F., Bond, M., Hamel, C., Devane, D., Kusa, W., O'Mara-Eves, A., Spijker, R., Stevenson, M., Stansfield, C., Thomas, J., & Minx, J. C. (2024). Computer-assisted screening in systematic evidence synthesis requires robust and well-evaluated stopping criteria. *Systematic Reviews*, 13(284). <https://doi.org/10.1186/s13643-024-02699-7>

Callaghan, M. W., & Müller-Hansen, F. (2020). Statistical stopping criteria for automated screening in systematic reviews. *Systematic Reviews*, 9(273). <https://doi.org/10.1186/s13643-020-01521-4>

Campos, D. G., Fütterer, T., Gfrörer, T., Lavelle-Hill, R., Murayama, K., König, L., Hecht, M., Zitzmann, S., & Scherer, R. (2024). Screening smarter, not harder: A comparative analysis of machine learning screening algorithms and heuristic stopping criteria. *Educational Psychology Review*, 36(1). Article 19.

Cerrone, V., Andretta, V., Prendin, A., Ilardi, B., Bonetti, C., Capunzo, M., & Cascella, M. (2025). Effectiveness of incident reporting tools in ensuring patient safety: A systematic-narrative hybrid review. *Patient Experience Journal*, 12(1), 83–92. <https://doi.org/10.35680/2372-0247.2001>

Chai, K. E. K., Lines, R. L. J., Gucciardi, D. F., & Ng, L. (2021). Research screener: A machine learning tool to semi-automate abstract screening for systematic reviews. *Systematic Reviews*, 10(93). <https://doi.org/10.1186/s13643-021-01635-3>

Clarkson, L., Naweed, A., & Whale, J. J. (2017). The minority report: Hazard reporting in an Australian university. *Work*, 56(1), 91–97. <https://doi.org/10.3233/WOR-162470>

Crayon. (2025). Onderzoek: Veel nederlandse medewerkers onvoorbereid op cyberaanvallen. Crayon. Retrieved from <https://www.crayon.com/nl/resources/inzichten/nederlandse-medewerker-onvoorbereid-cyberaanvallen/>.

Ebberts, S., Jansen, J., & Stol, W. P. (2025). Beyond phishing: A human-centered exploration of cyber incident reporting. In *Proceedings of the international symposium on human aspects of information security and assurance* (pp. 335–348). Nature Switzerland: Springer.

Ebberts, S., Jansen, J., & Stol, W. P. (2026). Predictors of employees' cyber incident reporting intention: A vignette study on TPB, psychological safety, and organisational citizenship behaviour. *Computers & Security*, 167. <https://doi.org/10.1016/j.cose.2026.104920>

Ebert, N., Schaltegger, T., Ambuehl, B., Schöni, L., Zimmermann, V., & Knieps, M. (2023). Learning from safety science: A way forward for studying cybersecurity incidents in organizations. *Computers & Security*, 134, Article 103435. <https://doi.org/10.1016/j.cose.2023.103435>

Edwards, D. J. (2024). Incident response. In D. J. Edwards (Ed.), *Mastering cybersecurity: Strategies, technologies, and best practices* (pp. 677–711). Apress. https://doi.org/10.1007/978-8-8688-0297-3_18

Eken, M., Lucas, R., Hoorens, S., & Nederveen, F. (2024). Strengthening societal resilience: A perspective on strategic priorities for the Netherlands amidst geopolitical tensions. *RAND Europe*.

Elsevier. (n.d.). Scopus content coverage guide. Elsevier. Retrieved from https://assets.ctfassets.net/o78em1y1w4i4/EX1iy8VxBeQKf8aN2XzOp/c36f79db25484cb38a5972ad9a5472ec/Scopus_ContentCoverage_Guide_WEB.pdf.

ENISA. (2017). *Cyber security culture in organisations*. European Union Agency for Cybersecurity. <https://doi.org/10.2824/10543>

Estay, D. A. S., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). A systematic review of cyber-resilience assessment frameworks. *Computers & Security*, 97, Article 101996. <https://doi.org/10.1016/j.cose.2020.101996>

- Franz, A. (2022). Why do employees report cyber threats? Comparing utilitarian and hedonic motivations to use incident reporting tools. In *Proceedings of the international conference on information systems (ICIS 2022)*.
- Furnell, S., Heyburn, H., Whitehead, A., & Shah, J. N. (2020). Understanding the full cost of cyber security breaches. *Computer Fraud & Security*, 2020(12), 6–12. [https://doi.org/10.1016/S1361-3723\(20\)30127-5](https://doi.org/10.1016/S1361-3723(20)30127-5)
- Gisladdottir, V., Ganin, A., Keisler, J., Kepner, J., & Linkov, I. (2017). Resilience of cyber systems with over- and underregulation. *Risk Analysis*, 37(9), 1644–1651. <https://doi.org/10.1111/risa.12729>
- Graddol, D. (2006). *English next* (Vol. 62). British Council.
- Guan, X., Feng, X., & Islam, A. Y. M. A. (2023). The dilemma and countermeasures of educational data ethics in the age of intelligence. *Humanities and Social Sciences Communications*, 10(1), 1–14.
- Hofstede, G. (2011). Dimensionalizing cultures: The Hofstede model in context. *Online Readings in Psychology and Culture*, 2(1), 8.
- Hollnagel, E. (2022). Systemic potentials for resilient performance. In F. Matos, P. M. Selig, & E. Henriksen (Eds.), *Resilience in a digital Age: Global challenges in organisations and Society* (pp. 7–17). Springer International Publishing.
- Häring, I., Ebenhöch, S., & Stolz, A. (2016). Quantifying resilience for resilience engineering of socio-technical systems. *European Journal of Scientific Research*, 1, 21–58. <https://doi.org/10.1007/s41125-015-0001-x>
- Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies. *Decision Sciences*, 43(4), 615–660.
- Huang, Y., Procházková, M., Lu, J., Riad, A., & Macek, P. (2022). Family-related variables' influences on adolescents' health. *Frontiers in Psychology*, 13. <https://doi.org/10.3389/fpsyg.2022.871795>
- Jausan, M., Silva, J., & Sabatini, R. (2017). A holistic approach to evaluating the effect of safety barriers on the performance of safety reporting systems in aviation organisations. *Journal of Air Transport Management*, 63, 95–107. <https://doi.org/10.1016/j.jairtraman.2017.06.004>
- Kamath, U., Keenan, K., Somers, G., & Sorenson, S. (2024). *Large language models: A deep dive*. Springer. <https://doi.org/10.1007/978-3-031-65647-7>
- Khan, R. A., Khan, S. U., Khan, H. U., & Ilyas, M. (2022). Systematic literature review on security risks and practices in secure software development. *IEEE Access*, 10, 5456–5481.
- Khiat, N., Zeghmi, L., & Perrault, L. (2024). HTA121 improving literature review efficiency: Evaluating the impact of the open-source ASReview tool. *Value in Health*, 27(12), Article S377.
- Kong, A., Zhao, S., Chen, H., Li, Q., Qin, Y., Sun, R., Zhou, X., Wang, E., & Dong, X. (2023). Better zero-shot reasoning with role-play prompting. *arXiv, arXiv:2308.07702*.
- Kott, A., & Linkov, I. (2021). To improve cyber resilience, measure it. *Computer*, 54(2), 80–85. <https://doi.org/10.1109/MC.2020.3038411>
- Kwak, Y., Lee, S., Damiano, A., & Vishwanath, A. (2020). Why do users not report spear phishing emails? *Telematics and Informatics*, 48, Article 101343.
- Lantz-Deaton, C., & Golubeva, I. (2020). What are critical incidents and how can we get the most out of them?. In *Intercultural competence for college and university students* (pp. 197–222). Springer. https://doi.org/10.1007/978-3-030-57446-8_6
- Li, Z., Xu, S., Mei, K., Hua, W., Rama, B., Raheja, O., Wang, H., & Zhang, Y. (2024). Autoflow: Automated workflow generation for large language model agents. *arXiv, arXiv:2407.12821*.
- Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. In *Cyber resilience of systems and networks* (pp. 1–25). Springer.
- Marotta, A., & Madnick, S. E. (2023). Regulating cyber incidents: A review of recent reporting requirements. In *Proceedings of the 20th international conference on security and cryptography (SECRYPT)* (pp. 410–416). <https://doi.org/10.5220/0012086000003555>
- Michie, S., van Stralen, M. M., & West, R. (2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implementation Science*, 6(42). <https://doi.org/10.1186/1748-5908-6-42>
- Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *Annals of Internal Medicine*, 151(4), 264–269.
- Muthuswamy, V., & Esakki, S. (2024). Impact of cybersecurity- and AI-related factors on incident reporting and employee stress. *International Journal of Cyber Criminology*, 18 (1).
- Naeem, M., Ozuem, W., Howell, K., & Ranfagni, S. (2023). A step-by-step process of thematic analysis to develop a conceptual model. *International Journal of Qualitative Methods*, 22, Article 16094069231205789.
- Nationaal Coördinator Terrorismedebijding en Veiligheid. (2023). De veiligheidsstrategie voor het Koninkrijk der Nederlanden. *Ministerie van Justitie en Veiligheid*. <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/publicaties/2023/04/03/veiligheidsstrategie-voor-het-koninkrijk-der-nederlanden/Veilighedsstrategie+voor+het+Koninkrijk+der+Nederlanden.pdf>
- National Research Council. (2012). *Disaster resilience: A national imperative*. The National Academies Press.
- Patterson, C. M., Nurse, J. R., & Franqueira, V. N. (2023). Learning from cyber security incidents. *Computers & Security*, 132. <https://doi.org/10.1016/j.cose.2023.103309>
- Patterson, C. M., Nurse, J. R., & Franqueira, V. N. (2024). 'I don't think we're there yet': Organisational learning from cyber security incidents. *Computers & Security*, 139. <https://doi.org/10.1016/j.cose.2024.103699>
- Pfeifer, L., Vessey, J., Cazzell, M., Reid Ponte, P., & Geyer, D. (2023). Relationships among psychological safety and safety reporting intentions. *Journal of Pediatric Nursing*, 73, 130–136.
- Prancutė, R. (2021). Web of science (WoS) and scopus: The titans of bibliographic information in today's academic world. *Publications*, 9(1), 12. <https://doi.org/10.3390/publications9010012>
- Ravitch, S. M., & Riggan, M. (2016). *Reason & rigor: How conceptual frameworks guide research*. SAGE Publications.
- Sabiri, B., Khtira, A., El Asri, B., & Rhanoui, M. (2025). Hybrid quality-based recommender systems: A systematic literature review. *Journal of Imaging*, 11(1), 12. <https://doi.org/10.3390/jimaging11010012>
- Salewski, L., Alaniz, S., Rio-Torto, I., Schulz, E., & Akata, Z. (2023). In-context impersonation reveals large language models' strengths and biases. *Advances in Neural Information Processing Systems*, 36, 72044–72057.
- Schein, E. H. (2004). *Organizational culture and leadership* (3rd ed. Jossey-Bass.
- Serrat, O. (2017). The critical incident technique. In O. Serrat (Ed.), *Knowledge solutions* (pp. 211–222). Springer. https://doi.org/10.1007/978-981-10-0983-9_123
- Shemilt, I., Khan, N., Park, S., & Thomas, J. (2016). Use of cost-effectiveness analysis to compare the efficiency of study identification methods in systematic reviews. *Systematic Reviews*, 5, 1–13.
- Smith, V., Devane, D., Begley, C. M., & Clarke, M. (2011). Methodology in conducting a systematic review of systematic reviews of healthcare interventions. *BMC Medical Research Methodology*, 11, 1–6.
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339. <https://doi.org/10.1016/j.jbusres.2019.07.039>
- Springer. (2025). *How peer reviewing is conducted*. Springer. Retrieved from <https://www.springer.com/gp/authors-editors/editors/peer-review>
- Sutton, A., & Tompson, L. (2024). Towards a cybersecurity culture-behaviour framework: A rapid evidence review. *Computers & Security*, Article 104110.
- Trim, P., & Upton, D. (2013). *Cyber security culture: Counteracting cyber threats through organizational learning and training*. Routledge. <https://doi.org/10.4324/9781315575681>
- Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture. *Computers & Security*, 109. <https://doi.org/10.1016/j.cose.2021.102387>
- Van de Schoot, R., de Bruin, J., Schram, R., Zahedi, P., de Boer, J., Weijdem, F., et al. (2021). An open source machine learning framework for efficient and transparent systematic reviews. *Nature Machine Intelligence*, 3(2), 125–133.
- Van der Kleij, R. (2025). Een groot digitaal dilemma. *IB Informatiebeveiliging Magazine*, 25 (4), 4–11.
- Van Steen, T., Del-Real, C., & Van den Berg, B. (2024). What works well? A safety-II approach to cybersecurity. In *International conference on human-computer interaction* (pp. 250–262). Nature Switzerland. : Springer.
- Verweijen, B. (2022). Leren van cyberincidenten: Een meta-analyse van evaluatierapporten. *Tijdschrift voor Veiligheid*, 21(3–4), 89–108. <https://doi.org/10.5553/TvV.000046>
- Vrbnjak, D., Denieffe, S., O'Gorman, C., & Pajnikar, M. (2016). Barriers to reporting medication errors and near misses among nurses: A systematic review. *International Journal of Nursing Studies*, 63, 162–178. <https://doi.org/10.1016/j.ijnurstu.2016.08.019>
- Wawersik, D., & Palaganas, J. (2022). Organizational factors that promote error reporting in healthcare. *Journal of Healthcare Management*, 67(4), 283–301.
- Winsvold Prang, I., & Jelsness-Jørgensen, L.-P. (2014). Should I report? A qualitative study of barriers to incident reporting among nurses working in nursing homes. *Geriatric Nursing*, 35(6), 441–447. <https://doi.org/10.1016/j.gerinurse.2014.07.003>
- World Economic Forum. (2024). *Unpacking cyber resilience (White paper)*. World Economic Forum. Retrieved from https://www3.weforum.org/docs/WEF_Unpacking_Cyber_Resilience_2024.pdf
- Yusuf, Y., & Irwan, A. M. (2021). The influence of nurse leadership style on patient safety incident reporting. *British Journal of Healthcare Management*, 27(6), 1–7. <https://doi.org/10.12968/bjhc.2020.0083>
- Zeng, Z., Watson, W., Cho, N., Rahimi, S., Reynolds, S., Balch, T., & Veloso, M. (2023). FlowMind: Automatic workflow generation with large language models. In *Proceedings of the ACM international conference on AI in finance* (pp. 73–81).
- Zhang, Q., Wang, J., & Neitzel, A. (2023). School-based mental health interventions targeting depression or anxiety: A meta-analysis of Rigorous randomized controlled trials for School-aged children and adolescents. *Journal of Youth and Adolescence*, 52 (1), 195–217. <https://doi.org/10.1007/s10964-022-01684-4>

Systematic literature

- AbuAlRub, R. F., Al-Akour, N. A., & Alatari, N. H. (2015). Perceptions of reporting practices and barriers to reporting incidents among registered nurses and physicians in accredited and nonaccredited Jordanian hospitals. *Journal of Clinical Nursing*, 24 (19–20), 2973–2982. <https://doi.org/10.1111/jocn.12934>
- Afolalu, O. O., Jordan, S., & Kyriacos, U. (2021). Medical error reporting among doctors and nurses in a Nigerian hospital: A cross-sectional survey. *Journal of Nursing Management*, 29(5), 1007–1015. <https://doi.org/10.1111/jonm.13238>
- Ahola, K., Sturman, D., Scott, N., Pattinson, M., Reeves, A., Butavicius, M., & McCormac, A. (2024). Improving the human firewall: Exploring the factors that influence cyber-security incident reporting. In *Proceedings of the international symposium on human aspects of information security and assurance* (pp. 116–129). : Springer Nature Switzerland.
- Atwal, A., Phillip, M., & Moorley, C. (2020). Senior nurses' perceptions of junior nurses' incident reporting: A qualitative study. *Journal of Nursing Management*, 28(6), 1215–1222. <https://doi.org/10.1111/jonm.13065>

- Aydeniz, E., & Intepeler, S. S. (2021). Examining the effectiveness of strategies developed to create an error reporting culture. *Clinical Nurse Specialist*, 35(5), 253–263. <https://doi.org/10.1097/NUR.0000000000000636>
- Bagenal, J., Sahnan, K., & Shantikumar, S. (2016). Comparing the attitudes and knowledge toward incident reporting in junior physicians and nurses in a district general hospital. *Journal of Patient Safety*, 12(1), 51–53. <https://doi.org/10.1097/PTS.0000000000000077>
- Balcerzak, T. A. (2017). “just culture”? Conflicts of interest in the investigation of aviation accidents. *Zeszyty Naukowe. Transport/Politechnika Śląska*, (94), 5–17.
- Bhatti, M. A., & Jamil, S. (2023). Factors effecting cyber incident occurrence: Mediating role of cyber incident reporting mechanism. *International Journal of Cyber Criminology*, 17(2), 112–132.
- Chen, L. C., Wang, L. H., Redley, B., Hsieh, Y. H., Chu, T. L., & Han, C. Y. (2018). A study on the reporting intention of medical incidents: A nursing perspective. *Clinical Nursing Research*, 27(5), 560–578. <https://doi.org/10.1177/1054773817692179>
- Chen, X., Doublet, S., Sergeeva, A., Lenzini, G., Koenig, V., & Distler, V. (2024). What motivates and discourages employees in phishing interventions: An exploration of expectancy-value theory. In *Proceedings of the symposium on useable privacy and security (SOUPS 2024)* (pp. 487–506).
- Chiang, H. Y., Hsiao, Y. C., Lin, S. Y., & Lee, H. F. (2011). Incident reporting culture: Scale development with validation and reliability and assessment of hospital nurses in Taiwan. *International Journal for Quality in Health Care*, 23(4), 429–436. <https://doi.org/10.1093/intqhc/mzr031>
- Chiang, H. Y., Lee, H. F., Lin, S. Y., & Ma, S. C. (2019). Factors contributing to voluntariness of incident reporting among hospital nurses. *Journal of Nursing Management*, 27(4), 806–814.
- Chiang, H. Y., Lin, S. Y., Hsu, S. C., & Ma, S. C. (2010). Factors determining hospital nurses' failures in reporting medication errors in Taiwan. *Nursing Outlook*, 58(1), 17–25. <https://doi.org/10.1016/j.outlook.2009.06.001>
- Da Silva da Paiva, M., Popim, R. C., Melleiro, M. M., Tronchim, D. M. R., Lima, S. A. M., & Juliani, C. M. C. M. (2014). The reasons of the nursing staff to notify adverse events. *Revista Latino-Americana de Enfermagem*, 22(5), 747–754. <https://doi.org/10.1590/0104-1169.35556.2476>
- Da Veiga, A., & Eloff, J. H. (2007). An information security governance framework. *Information Systems Management*, 24(4), 361–372. <https://doi.org/10.1080/10580530701586136>
- Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), 196–207. <https://doi.org/10.1016/j.cose.2009.10.006>
- Dalky, A. A., Oweidat, I. A., Abuzaid, S. R., Khalifeh, A. H., & AlBashtawy, M. (2024). Exploring the influence of nurses' demographics and hospital work environment on medical error reporting practices in Jordan: A cross-sectional study. *BMJ Open*, 14(11), Article e087057.
- Darveau, K., & Hannon, D. (2017). Barriers and facilitators to voluntary reporting and their impact on safety culture. *The International Journal of Aerospace Psychology*, 27(3–4), 92–108. <https://doi.org/10.1080/24721840.2018.1442221>
- Del Puerto, C. J. C. (2024). Nurses' medication administration error, reporting practices and challenges in tertiary hospitals: Descriptive analysis. *Philippine Journal of Nursing*, 94(2).
- Dhamanti, I., Leggat, S., Barraclough, S., & Rachman, T. (2022). Factors contributing to under-reporting of patient safety incidents in Indonesia: Leaders' perspectives. *F1000Research*, 10, 367. <https://doi.org/10.12688/f1000research.51912.2>
- Fernandes, P., Pereira, R., & Wiedenhöft, G. (2023). The effect of organizational cultures on relationships between IT governance and individual behavior. *Emerging Science Journal*, 7(5), 1602–1635. <https://doi.org/10.28991/ESJ-2023-07-05-010>
- Filtness, A. J., Goode, N., & Cook, R. (2015). Incident reporting culture in recreational hot air ballooning. *Procedia Manufacturing*, 3, 1165–1172. <https://doi.org/10.1016/j.promfg.2015.07.194>
- Gartmeier, M., Ottl, E., Bauer, J., & Berberat, P. O. (2017). Learning from errors: Critical incident reporting in nursing. *Journal of Workplace Learning*, 29(5), 343–356. <https://doi.org/10.1108/JWL-01-2017-0011>
- Gcaza, N., & Thomson, K. L. (2025). Factors contributing to the successful development of cyber safety education for foundation phase children: A systematic literature review. *Information & Computer Security*, 33(4), 499–519.
- Gifford, M. L., & Anderson, J. E. (2010). Barriers and motivating factors in reporting incidents of assault in mental health care. *Journal of the American Psychiatric Nurses Association*, 16(5), 288–298.
- Gilbey, A., Tani, K., & Tsui, W. H. K. (2016). Outcome knowledge and under-reporting of safety concerns in aviation. *Applied Cognitive Psychology*, 30(2), 141–151. <https://doi.org/10.1002/acp.3179>
- Hamed, M. M. M., & Konstantinidis, S. (2022). Barriers to incident reporting among nurses: A qualitative systematic review. *Western Journal of Nursing Research*, 44(5), 506–523. <https://doi.org/10.1177/0193945921999449>
- Han, N., Jeong, S. H., Lee, M. H., & Kim, H. S. (2024). Impacts of just culture on perioperative nurses' attitudes and behaviors with regard to patient safety incident reporting. *Asian Nursing Research*, 18(4), 323–330.
- Hewitt, T., Chreim, S., & Forster, A. (2017). Sociocultural factors influencing incident reporting among physicians and nurses. *Journal of Patient Safety*, 13(3), 129–137.
- Hong, S., & Li, Q. (2017). The reasons for Chinese nursing staff to report adverse events. *Journal of Nursing Management*, 25(3), 231–239.
- Hooper, P., Kocman, D., Carr, S., & Tarrant, C. (2015). Junior doctors' views on reporting concerns about patient safety. *Postgraduate Medical Journal*, 91(1075), 251–256.
- Hutchinson, A., Young, T. A., Cooper, K. L., McIntosh, A., Karnon, J. D., Scobie, S., & Thomson, R. G. (2009). Trends in healthcare incident reporting. *BMJ Quality and Safety*, 18(1), 5–10.
- ISO/IEC/IEEE. (2023). *Systems and software engineering — System life cycle processes (ISO/IEC/IEEE 15288:2023)*. ISO/IEC/IEEE Standards.
- Jennings, P. A., & Stella, J. (2011). Barriers to incident notification in a regional prehospital setting. *Emergency Medicine Journal*, 28(6), 526–529.
- Karlsson, M., Karlsson, F., Åström, J., & Denk, T. (2022). The effect of perceived organizational culture on employees' information security compliance. *Information & Computer Security*, 30(3), 382–401. <https://doi.org/10.1108/ICS-06-2021-0073>
- Kim, N. Y., & Kwak, S. J. (2024). Relationship between nurses' critical thinking disposition and patient safety incident reporting: The mediating role of patient safety culture. *PLoS One*, 19(12), Article e0315679.
- Kioulapoglou, P., Nikolaidis, V., David, K. M., & Makris, I. (2025). Investigating incident under-reporting in aviation: Qualitative insights among Greek pilots. *Research in Transportation Business & Management*, 59, Article 101309.
- Ko, E. S., & Kang, K. J. (2023). Effects of nurses' incident reporting attitude and patient safety culture on reporting patient safety events. *Journal of Korean Academy of Nursing Administration*, 29(3), 309–319.
- Koning, L., Junger, M., & Veldkamp, B. (2025). Reporting fraud victimization to the police: Factors that affect whether victims report. *Psychology, Crime and Law*, 1–29.
- Kreckler, S., Catchpole, K., McCulloch, P., & Handa, A. (2009). Factors influencing incident reporting in surgical care. *BMJ Quality and Safety*, 18(2), 116–120.
- Kurihara, M., Nagao, Y., & Tokuda, Y. (2021). Incident reporting among physicians-in-training in Japan: A national survey. *Journal of General and Family Medicine*, 22(6), 356–358.
- Lee, E. (2016). Safety climate and attitude toward medication error reporting after hospital accreditation in South Korea. *International Journal for Quality in Health Care*, 28(4), 508–514.
- Lee, J., Havaei, F., Hirani, S., & Adhami, N. (2025). Nurses' workplace violence reporting behaviours and reasons for not formally reporting. *Journal of Clinical Nursing*, 34(10), 4235–4245.
- Lee, W., Kim, S. Y., Lee, S. I., Lee, S. G., Kim, H. C., & Kim, I. (2018). Barriers to reporting of patient safety incidents in tertiary hospitals. *The International Journal of Health Planning and Management*, 33(4), 1178–1188.
- Liu, N. F., Lin, K., Hewitt, J., Paranjape, A., Bevilacqua, M., Petroni, F., & Liang, P. (2023). Lost in the middle: How language models use long contexts. *arXiv*, arXiv:2307.03172.
- Louis, M. Y., Hussain, L. R., Dhanraj, D. N., Khan, B. S., Jung, S. R., Quiles, W. R., et al. (2016). Improving patient safety event reporting among residents and teaching faculty. *The Ochsner Journal*, 16(1), 73–80.
- Martowirono, K., Jansma, J. D., van Luijk, S. J., Wagner, C., & Bijnen, A. B. (2012). Possible solutions for barriers in incident reporting by residents. *Journal of Evaluation in Clinical Practice*, 18(1), 76–81.
- McCoy, B., Stephens, G., & Stevens, K. J. (2009). An investigation of the impact of corporate culture on employee information systems security behaviour. In *Proceedings of ACIS 2009* (p. 58). <https://aisel.laisnet.org/acis2009/58>.
- Mehanna, D., El Gerges, N., Chalhoub, M., & Daou, R. (2024). Barriers to medication administration error reporting in a tertiary hospital in Lebanon. *BMJ Open Quality*, 13(4).
- Mountzoglou, A. (2010). Factors impeding nurses from reporting adverse events. *Journal of Nursing Management*, 18(5), 542–547. <https://doi.org/10.1111/j.1365-2834.2010.01049>
- Mukherjee, S., Roy, S., & Era, N. (2024). Safety incident reporting and barriers (SIRaB) study. *Journal of Evaluation in Clinical Practice*, 30(4), 651–659. <https://doi.org/10.1111/jep.13990>
- Munro, V. (2002). Why do nurses neglect to report violent incidents? *Nursing Times*, 98(17), 38–39.
- Nasir, A., Arshah, R. A., Ab Hamid, M. R., & Fahmy, S. (2019). An analysis on the dimensions of information security culture. *Journal of Information Security and Applications*, 44, 12–22. <https://doi.org/10.1016/j.jisa.2018.11.003>
- Nurdin, D. A., & Wibowo, A. (2021). Barriers to reporting patient safety incidents. *Indonesian Journal of Health Administration*, 9(2), 210–217. <https://doi.org/10.20473/jaki.v9i2.2021.210-217>
- Pfeiffer, Y., Briner, M., Wehner, T., & Manser, T. (2013). Motivational antecedents of incident reporting: Evidence from a survey of nurses and physicians. *Swiss Medical Weekly*, 143, Article w13881. <https://doi.org/10.4414/smw.2013.13881>
- Pfeiffer, Y., Manser, T., & Wehner, T. (2010). Conceptualising barriers to incident reporting: a psychological framework. *Quality and Safety in Health Care*, 19(6), e60. <https://doi.org/10.1136/qshc.2008.030445>
- Pilavakis, N., Jenkins, A., Kokciyan, N., & Vaniea, K. E. (2023). ‘I didn't click’: What users say when reporting phishing. In *Proceedings of the Symposium on Useable Security and Privacy (USEC 2023)* *.
- Pollini, A., & Ciccone, A. (2024). The hidden potential of an incident: Designing for cybersecurity incident reporting. In *Damocles – First international workshop on detection and mitigation of cyber attacks That exploit human vulnerabilities* (pp. 21–36).
- Prang, I. W., & Jelsness-Jørgensen, L.-P. (2014). Should I report? A qualitative study of barriers to incident reporting among nurses working in nursing homes. *Geriatric Nursing*, 35(6), 441–447.
- Pratama, G. B., & Caponecchia, C. (2025). Examining the influence of national culture on aviation safety: A systematic review. *Journal of Safety Research*, 92, 317–330.
- Rahman, S. S., Heartfield, R., Oliff, W., Loukas, G., & Filippoupolitis, A. (2017). Assessing the cyber-trustworthiness of human-as-a-sensor reports from Mobile devices. In *2017 IEEE 15th international conference on software engineering research, management and applications (SERA)* (pp. 387–394). IEEE.
- Rashed, A., & Hamdan, M. (2019). Physicians' and nurses' perceptions of and attitudes toward incident reporting in Palestinian hospitals. *Journal of Patient Safety*, 15(3), 212–217.

- Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security*, 26(1), 56–62. <https://doi.org/10.1016/j.cose.2006.10.008>
- Sato, K., Wakabayashi, T., Kiyoshi-Teo, H., & Fukahori, H. (2013). Factors associated with nurses' reporting of patients' aggressive behavior: A cross-sectional survey. *International Journal of Nursing Studies*, 50(10), 1368–1376. <https://doi.org/10.1016/j.ijnurstu.2012.12.011>
- Schectman, J. M., & Plews-Ogan, M. L. (2006). Physician perception of hospital safety and barriers to incident reporting. *Joint Commission Journal on Quality and Patient Safety*, 32(6), 337–343.
- Sieberichs, S., & Kluge, A. (2021a). How just culture and personal goals moderate the relation between pilots' safety citizenship behavior and voluntary incident reporting. *Safety Now*, 7(3), 59. <https://doi.org/10.3390/safety7030059>
- Sieberichs, S., & Kluge, A. (2021b). Why commercial pilots voluntarily report self-inflicted incidents. *Aviation Psychology and Applied Human Factors*, 11(2), 98–111. <https://doi.org/10.1027/2192-0923/a000216>
- Smith, K. S., Harris, K. M., Potters, L., Sharma, R., Mutic, S., Gay, H. A., et al. (2014). Physician attitudes and practices related to voluntary error and near-miss reporting. *Journal of Oncology Practice*, 10(5), e350–e357.
- Snijders, C., Kollen, B. J., van Ling, R. A., Fetter, W. P., Molendijk, H., & NEOSAFE Study Group. (2009). Which aspects of safety culture predict incident reporting behavior in neonatal intensive care units? *Critical Care Medicine*, 37(1), 61–67.
- Soleimani, F. (2006). Learning from mistakes in New Zealand hospitals: What else do we need besides 'no-fault'. *New Zealand Medical Journal*, 119(1239).
- Solomon, G., & Brown, I. (2021). The influence of organisational culture and information security culture on employee compliance behaviour. *Journal of Enterprise Information Management*, 34(4), 1203–1228.
- Song, C., Wang, G., & Wu, H. (2021). Frequency and barriers of reporting workplace violence in nurses: An online survey in China. *International Journal of Nursing Science*, 8(1), 65–70.
- Szymusiak, J., Walk, T. J., Benson, M., Hamm, M., Zickmund, S., Gonzaga, A. M., & Bump, G. M. (2020). A qualitative analysis of resident adverse event reporting. *American Journal of Medical Quality*, 35(2), 155–162.
- Tabak, N., & Fleishman, S. (2011). The intention to report medication error. *Medicine & Law*, 30(3), 363–370.
- Throckmorton, T., & Etchegaray, J. (2007). Factors affecting incident reporting by registered nurses. *Journal of PeriAnesthesia Nursing*, 22(6), 400–412.
- Tricarico, P., Castriotta, L., Battistella, C., Bellomo, F., Cattani, G., Grillone, L., et al. (2017). Professional attitudes toward incident reporting. *International Journal for Quality in Health Care*, 29(2), 243–249.
- Van der Kleij, R., Van Hemert, D., te Paske, B. J., & Rooijakkers, T. (2024). Human-centric security engineering: Towards a research agenda. In *Proceedings of the AHFE international conference*.
- Van Marum, S., Verhoeven, D., & de Rooy, D. (2022). The barriers and enhancers to trust in a just culture in hospital settings. *Journal of Patient Safety*, 18(7), e1067–e1075.
- Varallo, F. R., Passos, A. C., Nadai, T. R. D., & Mastroianni, P. D. C. (2018). Incidents reporting: Barriers and strategies to promote safety culture. *Revista da Escola de Enfermagem da USP*, 52. <https://doi.org/10.1590/S1980-220X2017026403346>
- Vielberth, M., Englbrecht, L., & Pernul, G. (2021). Improving data quality for human-as-a-security-sensor. *Information & Computer Security*, 29(2), 332–349.
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102. <https://doi.org/10.1016/j.cose.2013.04.004>
- Walsh, K., Burns, C., & Antony, J. (2010). Electronic adverse incident reporting in hospitals. *Leadership in Health Services*, 23(4), 292–303. <https://doi.org/10.1108/17511871011079047>
- Waring, J. J. (2004). A qualitative study of the intra-hospital variations in incident reporting. *International Journal for Quality in Health Care*, 16(5), 347–352. <https://doi.org/10.1093/intqhc/mzh068>
- Waring, J. J. (2005). Beyond blame: Cultural barriers to medical incident reporting. *Social Science & Medicine*, 60(9), 1927–1935. <https://doi.org/10.1016/j.socscimed.2004.08.055>
- Waters, N. F., Hall, W. A., Brown, H., Espezel, H., & Palmer, L. (2012). Perceptions of Canadian labour and delivery nurses about incident reporting. *International Journal of Nursing Studies*, 49(7), 811–821.
- Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and information security awareness. *Computers & Security*, Article 101640. <https://doi.org/10.1016/j.cose.2019.101640>, 88.
- Williams, S. D., Phipps, D. L., & Ashcroft, D. (2015). Examining the attitudes of hospital pharmacists to reporting medication safety incidents. *International Journal for Quality in Health Care*, 27(4), 297–304.
- Xu, Y., He, N., Lu, W., & Fluke, J. (2021). Understanding factors associated with social workers' decision making in reporting child physical abuse in China. *Child Abuse & Neglect*, 120, Article 105177. <https://doi.org/10.1016/j.chiabu.2021.105177>
- Zhao, X., Zhao, S., Liu, N., & Liu, P. (2021). Willingness to report medical incidents in healthcare: a psychological model based on organizational trust and benefit/risk perceptions. *The Journal of Behavioral Health Services & Research*, 48(4), 583–596. <https://doi.org/10.1007/s11414-021-09753-5>