

Frontline perceptions of middle management as a bottleneck in cybersecurity escalation and risk communication

Brian Scavotto

Eastern Oregon University, La Grande, Oregon, USA

Organizational
Cybersecurity
Journal: Practice,
Process and
People

Received 4 February 2026

Revised 4 June 2026

22 July 2026

Accepted 27 August 2026

Abstract

Purpose – This study examines how frontline cybersecurity professionals perceive middle management's role in the escalation and communication of cyber risk within large organizations, and identifies the communication failures they associate with delayed or incomplete reporting of critical security issues to senior leadership.

Design/methodology/approach – Semi-structured interviews were conducted with 20 frontline cybersecurity professionals across multiple industries. Thematic analysis identified patterns in how participants perceived middle management's handling of security information to shape the reporting and resolution of security threats.

Findings – Participants perceived three interconnected failure modes: structural barriers that delay escalation, procedural gaps that limit tracking and accountability, and behavioral dynamics in which the severity of security issues was perceived to be minimized or suppressed before reaching senior leadership. Participants attributed these patterns variously to impression management and controllability concerns and to resource constraints, competing priorities, immature escalation processes, unclear ownership and misunderstanding of technical severity. Where these dynamics occur, organizations risk exposure to preventable threats and senior leaders may lack the accurate information needed for risk-based decisions.

Originality/value – While prior work has examined organizational communication, governance and coordination failures in cybersecurity incidents, relatively little research has examined middle-management communication dynamics in the escalation of cyber risk. This study addresses that gap from the frontline perspective and proposes interventions including direct reporting mechanisms, interdisciplinary technical advisory councils and targeted middle-management training.

Keywords Middle management, Cybersecurity, Cyber risk, Security communications, Incident response, Vulnerability management

Paper type Research article

1. Introduction

Effective communication is the bedrock of a well-designed cybersecurity defense strategy. The flow of information regarding cyber threats, risks and vulnerabilities experienced by a large organization must travel through many levels and dimensions of corporate structure to be adequately addressed. Large-scale breaches continue to occur despite healthy cybersecurity budgets, mature organizations and a sea of cybersecurity technologies. Many studies have attempted to determine the root causes of why seemingly well-protected and well-funded organizations experience significant security incidents. These studies have examined security breaches and how they relate to managerial factors (Doherty and Fulford, 2005; Angst *et al.*, 2017), technological factors (Ransbotham and Mitra, 2009; Cavusoglu *et al.*, 2005) and human factors (Liginlal *et al.*, 2009; Kamoun and Nicho, 2014). While prior work has examined

© Brian Scavotto. Published in *Organizational Cybersecurity Journal: Practice, Process and People*. Published by Emerald Publishing Limited. This article is published under the Creative Commons Attribution (CC BY 4.0) license. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this license may be seen at <http://creativecommons.org/licenses/by/4.0/>

Funding: This research received no external funding.

Conflict of interest: The author declares no conflict of interest.



Organizational Cybersecurity Journal:
Practice, Process and People
Emerald Publishing Limited
e-ISSN: 2635-0289
p-ISSN: 2635-0270
DOI 10.1108/OJ-02-2026-0006

organizational communication, governance and coordination failures in cybersecurity incidents, including top management's attention to cybersecurity following breaches (Shaikh and Siponen, 2023) and corporate communication after incidents (Knight and Nurse, 2020), relatively little research has specifically examined middle-management communication dynamics in the escalation of cyber risk. The literature makes it clear that there is no singular reason why these incidents occur. Still, each case presents many complicated reasons highly dependent on technical and human-related factors (Schlackl *et al.*, 2022).

Large-scale breaches frequently prove preventable in hindsight (Internet Society, 2019; Verizon, 2022). Well-resourced organizations with mature programs, including Equifax in 2017, Target in 2013 and repeat victims such as Yahoo and T-Mobile, have nonetheless suffered major incidents (US House of Representatives, 2018; Plachkinova and Maurer, 2018; Bederna *et al.*, 2021; Newman, 2023).

Why such mature organizations succumb to preventable incidents is often obscured by legal protections around disclosure (Stephenson, 2003). What is consistently reported, however, is that most incidents involve some form of human error (Verizon, 2022).

In most organizations, the frontline cyber defenders are the most aware of the vulnerabilities, susceptibilities and threats that the company faces. Frontline cyber defenders are often well removed from leadership and decision-makers, especially at large organizations, only to find their reporting brokered by various middle management levels. While there has been extensive research around the technical aspects of information security, unfortunately, little research has been done on the challenges of internal communications to cybersecurity programs. More research needs to be presented on how the potential failures of middle management may contribute to significant cybersecurity breaches. Previous work in these areas focused on effective communications with the business (Nurse *et al.*, 2011; Hayes-Munson, 2022; Hamburg and Groch, 2018), communicating incidents with customers, third parties and regulators (D'Arcy and Basoglu, 2022; Pacella, 2016; Wolfff, 2014) and the importance of communication and collaboration after a security incident (Hawkins, 2017; Tatu *et al.*, 2018; Patterson *et al.*, 2023), but there is a lack of research that comprehensively studies the connection between internal cybersecurity communications issues, particularly involving middle management and their impact on an organization's susceptibility to security incidents.

This study contributes an account of how frontline cybersecurity professionals perceive middle management as a bottleneck in the escalation and communication of cyber risk. Rather than asserting that middle managers intentionally suppress information, it identifies three perceived failure modes, structural, procedural and behavioral, and considers competing explanations for each, ranging from impression management and controllability concerns to resource constraints, competing priorities, immature escalation systems, unclear ownership and misunderstanding of technical severity. It maps these perceived mechanisms to established theory and derives governance interventions tied to each failure mode.

This article conducted a qualitative study to explore whether internal communications breakdowns and middle management failures prevent frontline employees from successfully mitigating critical cybersecurity issues. In contrast to quantitative research, qualitative research focuses on meanings, concepts, definitions, characteristics, metaphors, symbols and descriptions of things (Berg, 2001). The qualitative methodology aligns with discovering the issues within internal security team communications and those in the broader business. Within the above context, these research questions will be addressed in this study:

- RQ1. Do frontline information security professionals perceive that the critical security issues they report are urgently received, properly handled and fully understood by decision-makers?
- RQ2. What cross-team challenges do frontline information security professionals experience when reporting critical security issues?

RQ3. Do frontline information security professionals perceive that the details or severity of critical security issues they report are altered or suppressed before reaching decision-makers?

2. Background

2.1 Organizational overview

Information security is the protection of information and systems to preserve confidentiality, integrity and availability (NIST, 2015), and the terms cybersecurity and information security are used interchangeably here. In large organizations, the security program is typically led by a Chief Information Security Officer (CISO), who reports to a senior executive such as the CIO, CTO or CEO (Aiello *et al.*, 2023) and whose direct reports constitute the program’s senior leadership.

Security program structures vary across industries but typically include security engineering, operations, incident management and governance (Shayo and Lin, 2019), with multiple management layers between frontline staff and executive leadership. This study treats levels two and three in Figure 1 as middle management and levels three and four as senior leadership.

Frontline employees at level one typically hold the deepest technical expertise, which tends to decrease at higher levels as leadership focuses on strategy, people management and reporting (Espinoza, 2023). Senior leaders therefore lack the frontline’s detailed read on security posture, while frontline staff lack leadership’s strategic view. Middle management becomes the information broker between them, placing it in a pivotal position to report security issues, vulnerabilities and incidents accurately to senior leadership, which is responsible for governance, remediation and reducing cyber risk.

2.2 Cybersecurity governance

Cybersecurity governance is a subset of corporate governance focused on information security strategy, policies and procedures, and is shaped by each organization’s security culture (AlGhamdi *et al.*, 2020; Al-Izki and Weir, 2016). Effective programs depend on success factors that include clear communication, risk and threat assessment, and the timely reporting of security issues (Gashgari *et al.*, 2017), and organizations increasingly recognize cybersecurity as a business problem rather than a purely technical one (Posthumus and von

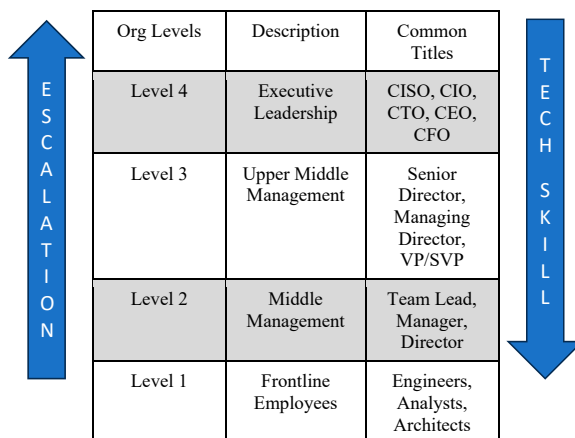


Figure 1. Typical large organization security hierarchy

[Solms, 2005](#)). Internal communication, in particular the reporting of cyber risk upward, is among the highest-weighted governance practices ([Bobbert and Mulder, 2015](#)).

Cybersecurity governance is typically top-down, with executives relying on middle management to report upward and implement decisions ([Boehm et al., 2020](#)). Yet executives often lack the complete, consistent and reliable information needed for genuinely risk-based decisions ([Boehm et al., 2020](#)).

2.3 *The pivotal role of middle management*

Middle managers are widely recognized as critical to organizational change ([Harding et al., 2014](#); [Rydland, 2020](#)) and act as information and resource brokers across teams ([Shi et al., 2009](#)), helping to formulate strategy with the experts beneath them while implementing decisions from above ([Vaz and Bulgacov, 2018](#)). In this sense, they are the “linking pins” between decision-makers and frontline employees ([Bryant and Stensaker, 2011](#)). Operating as a buffer between leadership and the frontline, however, can introduce vulnerability, as managers face competing pressures to satisfy leadership while meeting frontline expectations ([Harding et al., 2014](#)). These competing pressures can be read through several theoretical lenses that recur throughout this study. Impression management concerns how managers curate the information they pass upward ([Goffman, 1959](#); [DuBrin, 2010](#)); controllability bias, related to the illusion of control, concerns a manager’s belief that an issue can be resolved before it needs to be escalated ([Langer, 1975](#); [Goerke et al., 2004](#)); and agency theory concerns the divergence between a manager’s incentives and the organization’s risk interest ([Eisenhardt, 1989](#); [Lopes, 2016](#); [Stone et al., 2019](#)). The urgency with which escalated issues are then treated, and whether nonescalation carries any consequence, can be read through deterrence theory and protection motivation theory, both of which address what motivates a timely protective response ([Straub, 1990](#); [D’Arcy et al., 2009](#); [Rogers, 1975](#)).

Middle management is not always viewed positively. [Balogun \(2003\)](#) notes a reputation for being obstructive and resistant to change, and [Scarborough and Burrell \(1996\)](#) observe that middle managers can block communication in both directions, since they filter information through their own appraisals and interpretations before passing it upward; these problems worsen when managers feel excluded from strategic decisions ([Wooldridge et al., 2008](#)).

2.4 *Motivations for middle management misconduct*

The literature offers several reasons middle managers may obstruct or distort information flow. [Stone et al. \(2019\)](#) identify a fear of reporting adverse information and appearing incompetent, prompting managers to save face while attempting to resolve issues themselves. [Hiekkataipale and Lamsa \(2016\)](#) find that some managers withhold or manipulate information to serve hidden agendas. Organizational culture strongly shapes what employees are willing to report or conceal ([Bennejen and Tropp, 2019](#)), and some structures insulate senior leadership from unethical behavior occurring below them ([White, 2019](#)). [Stone et al. \(2019\)](#) further find that managers misreport or falsify information to improve short-term metrics tied to bonuses and to ease competitive pressure among peers.

Comparable dynamics appear in corporate scandals outside cybersecurity, where middle management suppressed or distorted unfavorable information, as in the Volkswagen emissions scandal ([Leggett, 2018](#)), the collapse of Lehman Brothers ([Valukas, 2010](#)) and an ethnographic study of coerced deception in a telecommunications sales unit ([Den Nieuwenboer et al., 2017](#)).

Three constructs frame how these motivations could shape what frontline staff observe. Controllability bias, an expression of the illusion of control, leads managers to believe they can resolve an issue themselves, prompting them to withhold or delay escalation while attempting a fix ([Langer, 1975](#); [Goerke et al., 2004](#)); this anticipates the delayed-escalation pattern examined under RQ1. Impression management explains how managers may curate or soften information to maintain a positive image or avoid blame ([Goffman, 1959](#); [DuBrin, 2010](#)); this anticipates the minimization and watering-down examined under RQ3. Agency theory holds

that agents may act in their own interest rather than the organization's, particularly when performance is evaluated (Eisenhardt, 1989; Lopes, 2016; Stone *et al.*, 2019); this anticipates misreporting tied to image or to metrics.

A second dimension concerns the urgency of response once an issue reaches decision-makers and the consequences attached to escalating, or failing to escalate, a serious issue. Deterrence theory holds that the perceived certainty and severity of consequences shape whether individuals act in line with security expectations (Straub, 1990; D'Arcy *et al.*, 2009), and recent work extends this to how formal sanctions interact with social norms in security behavior (Prabhu *et al.*, 2025; Merhi and Ahluwalia, 2024). Protection motivation theory explains protective responses in terms of perceived severity, vulnerability and the efficacy of acting (Rogers, 1975; Johnston and Warkentin, 2010). These literatures concern individual policy compliance and insider intentions rather than middle-management suppression specifically, so they are drawn on here as construct sources for interpreting the perceived lack of urgency and accountability reported by participants, not as direct precedent.

2.5 Real-world consequences in cybersecurity

Survey evidence suggests such suppression is not rare: in Bitdefender's (2023) assessment of 400 IT professionals, 42% reported being told to keep a breach confidential rather than report it, although the data do not specify whether this pressure originated with middle management or concerned external disclosure.

3. Methodology

Twenty semi-structured interviews were conducted with frontline information security professionals, such as security engineers, analysts and architects, from 15 organizations. Although the study concerns middle management, frontline employees were chosen because they are directly affected by managers' decisions and are well positioned to observe how their reporting is handled, providing an indirect but valuable lens on middle management. As the staff closest to security issues, they are also uniquely able to judge how effectively their reports are acted upon and where communication breaks down.

This study adopted a purposeful maximum variation sampling approach (Patton, 2015) to collect various views and experiences across factors such as geography, industry vertical, interviewee experience and role. Other participant dimensions could have been employed; however, those chosen here will still allow the study to avoid distortions due to a limited breadth of sampling (Patton, 1990). Participants were restricted to only organizations based in the United States with a minimum headcount of 5,000 employees. This decision was made to ensure the focus remained on large organizations. Since cybersecurity is approached differently based on industry, ensuring that the participant sample was across several industries was important. The participants' positions ranged from Incident Response Analysts (5 participants) and Vulnerability Management Analysts (5 participants) to Security Engineers (6 participants), Security Operations Analysts (2 participants) and two Security Architects. A pseudonym (P1-P20) was assigned to each participant to ensure the confidentiality of their identities. Questions were geared toward the participants' entire security career at large organizations, not just their current employer. Various organizations employed several participants over their careers, providing them with many differing perspectives and experiences from which to draw. Table 1 below provides an overview of participant details.

Participants were recruited through LinkedIn searches and local cybersecurity professional groups, with snowball sampling for additional referrals. Eligibility was assessed against three inclusion criteria: current or prior employment as a frontline cybersecurity professional (security engineer, analyst or architect); employment at a United States organization; and an employer headcount of at least 5,000. These criteria were verified in two steps. During recruitment, candidates' roles and employer size were checked against their LinkedIn profiles,

Table 1. Participant job descriptions

Participant	Job title	Industry	Years of experience in information security	Total years of experience in technology	Number of unique organizations employed by
P1	Incident Response Analyst	Telecom	8	17	1
P2	Incident Response Analyst	Commercial Real Estate	13	30	13
P3	Incident Response Analyst	Telecom	7	25	1
P4	Incident Response Analyst	Technology	25	25	9
P5	Vulnerability Management Analyst	Technology	3	5	7
P6	Security Operations Analyst	Commercial Real Estate	9	9	3
P7	Security Architect	Healthcare	12	17	6
P8	Vulnerability Management Analyst	Healthcare	4	6	2
P9	Security Engineer	Financial Services	12	12	5
P10	Security Engineer	Energy	8	10	3
P11	Security Operations Analyst	Healthcare	4	4	1
P12	Incident Response Analyst	Financial Services	10	15	7
P13	Security Engineer	Higher Education	6	6	3
P14	Vulnerability Management Analyst	Manufacturing	4	4	2
P15	Security Engineer	Construction	7	12	5
P16	Vulnerability Management Analyst	Retail	5	5	2
P17	Vulnerability Management Analyst	Financial Services	3	3	2
P18	Security Engineer	Retail	5	7	2
P19	Security Engineer	Retail	7	9	2
P20	Security Architect	Healthcare	15	19	4

and eligibility was then confirmed through a short set of pre-interview screening questions covering role, employer size and geography. Candidates who did not meet all three criteria were not interviewed. The total number of interviews was determined based on data saturation, which is said to be achieved when no new information emerges from the data analysis (Camic *et al.*, 2003). This study reached saturation after 16 interviews when no new themes or relevant information was uncovered. Four subsequent interviews were conducted beyond saturation to ensure no new or novel themes were identified. All interviews were conducted between September 2023 and September 2024 via video conference. The diversity of roles and responsibilities resulted in interesting variations in perception around internal cybersecurity communications. Fifteen participants were male, and five participants were female. This ratio of 25% female participants matches recent industry reporting of the percentage of women within cybersecurity as 25–30% (Gates, 2024). Interviews lasted an average of 52 min, ranging from 27 min to one hour and 17 min. All interviews utilized a semi-structured approach commonly used in exploratory phenomenological projects (Billups, 2021). All participants were asked the same questions in the same order found in Appendix A. A variance in follow-up

questions may change during separate interviews and is based on the responses from each participant. All interviews were transcribed using the online machine-learning transcription service Otter.ai. Each transcription was reviewed for accuracy prior to being introduced into the study.

3.1 Interview question design

Interview questions were tailored to participants' roles. Interviews opened with each participant's role and responsibilities, then, because terminology and hierarchy vary across organizations, established who the decision-makers were, how many management levels separated the participant from the senior-most security leader (typically a CISO), and how they defined a critical or high-severity issue. Subsequent questions addressed how often such issues arose, how and by what means they were reported upward, whether reporting was altered, what hindered reporting and participants' perceptions of how the CISO responded. Every question was optional. The semi-structured format allowed both question order and follow-ups to vary to draw out clarifying detail (Billups, 2021).

3.2 Data analysis

The thematic analysis method was chosen to process the collected data and turn it into insights and interpretations of internal communications challenges within cybersecurity programs (Braun and Clarke, 2006). Within qualitative research, thematic analysis is ubiquitous and well-recognized. The systematic method allows for a coherent reporting of coding, analytical and interpretative processes (Miles and Huberman, 1984). Using inductive coding driven by the research questions allows patterns to be identified from participants' accounts rather than imposed from a predetermined framework. The aim is exploratory and interpretive: to surface and organize how frontline professionals perceive middle management's role in escalation and risk communication, and to relate those patterns to established theory, rather than to generate a new formal theory. Braun and Clarke (2012) developed six phases of thematic analysis used in this study. The six phases are as follows: (1) development of the initial codes, (2) transcription of the interviews (using a third-party transcription service), (3) initial theme generation and connection to research questions, (4) comprehensive review of the themes concerning the entire dataset, (5) defining and naming the themes and (6) report production from the thematic analysis. I performed manual coding with the help of an open-source software tool known as Taguette. Textual transcriptions from Otter.ai were loaded into Taguette, allowing the ability to mark and tag text sections.

Because the interview questions addressed participants' experiences across their entire cybersecurity careers rather than only their current employer, many accounts spanned multiple organizations and the findings draw on a mixture of current-employer and prior-employer experiences. To track this during analysis, each coded account was labeled in the coding software by employer context (current employer, prior employer or unspecified), so that the source of each theme could be distinguished during interpretation. The findings are therefore reported as career-spanning perceptions of how middle management functions in large security programs rather than as claims about any single named organization, and participants were asked to anchor each theme in specific remembered incidents rather than general impressions.

I performed all coding as the sole coder. This study follows Braun and Clarke's reflexive thematic analysis, in which coding is treated as an interpretive act rather than a measurement to be replicated; under this approach, inter-rater reliability statistics are not regarded as a meaningful or appropriate quality criterion, and none were computed. Analytic quality was instead pursued through several measures. An audit trail was maintained in the coding software, recording how initial codes were generated and how they were collated into the reported themes. Preliminary interpretations and themes were shared with five of the 20 participants for confirmation (member checking). Three confirmed the interpretations as

written and recommended no changes. The remaining two suggested small amendments to how particular statements had been interpreted; both amendments were incorporated, and neither altered the substance of the accounts or the themes derived from them. Rich verbatim quotations are used throughout the findings to ground each theme in participants' own words, and the saturation procedure described above, in which four interviews were conducted beyond the point of apparent saturation, provided a further check that the themes were stable.

Because the data capture frontline professionals' accounts rather than directly observed managerial behavior, findings are reported at the level of participant experience. To avoid overstating what the interviews can support, each reported pattern is graded by the directness of the underlying account: (1) a direct instruction not to report or to withhold an issue, which the participant personally received or witnessed; (2) direct observation of reported information being altered or minimized; (3) loss of visibility into an issue after it was escalated and (4) a general perception that decision-makers did not receive, understand or act on an issue. Categories (1) and (2) rest on concrete events the participant experienced firsthand, whereas category (4) reflects inference about others' knowledge or intent. Where a finding rests only on category (3) or (4) evidence, it is presented as a perception and is not treated as an established organizational outcome.

A full data structure mapping first-order codes to themes and the three failure modes is provided as [Supplementary Table S1](#).

4. Results

This section analyzes the results of speaking with frontline information security professionals about internal communications, issues with middle management and how they perceive reporting of critical security issues handled by executive leadership. [Section 4.1](#) is dedicated to addressing [RQ1](#) by revealing the perception of information security professionals when reporting critical security concerns up their chain of command. [Section 4.2](#) addresses [RQ2](#) by revealing what internal communications challenges frontline information security professionals experience when reporting critical security issues. [Section 4.3](#) addresses [RQ3](#) by revealing if frontline information security professionals perceive the details or severity of critical security issues they report are altered or suppressed before reaching decision-makers. Each section, respectively, will report on the themes that emerged from the participant interviews. Participants will be referred to by their assigned pseudonyms, such as P1-P20. When referring to a range of participants, for example, P6-P10 indicates that participants six through ten reported the theme.

4.1 Reporting and communicating critical security concerns

The main themes that emerged from the qualitative analysis of interviews about [RQ1](#) *Do frontline information security professionals perceive the critical security issues they report are received and properly handled by decision-makers?* are as follows: First, participants were concerned that what they were reporting to their management chain was not being rapidly escalated with urgency and a lack of follow-up. Concerns in this area gravitated toward needing a formal reporting process and a shared sense of urgency. Second, participants needed more formal methods for reporting critical security concerns to governance groups outside of information security (risk, audit and legal). Lastly, participants reflected on a high amount of skepticism that (1) decision-makers understood the nature of the problem being reported, (2) the severity and potential risk of financial loss to the company if not quickly remedied and (3) the accuracy and integrity of the information as reported to several levels above them.

The aggregated responses show that 16 out of 20 participants (P1-12, P14, P16, P18-P19) did not feel a sense of urgency when reporting significant security issues to their management chain in the past. The majority of the 16 responses (P2-P4, P6-P14, P19) indicated that they could report these issues to their immediate supervisor; however, they had no reasonable levels

of confidence that those issues were being addressed above their immediate supervisor. These concerns centered around the fact that there was no formal method to report issues so that the reporter could follow up on them and monitor their resolution status. Participants often continued uncovering the same significant security issues for long periods despite reporting them to their supervisors.

When I report a critical security finding to my management, it's extremely informal and usually in the form of an e-mail or teams message. There is no centralized platform to report these types of issues. We have a ticketing system, but that is not used at all for security issues. It would be nice if I could track what I've reported to make sure it's being dealt with. Instead, I feel like our reports sometimes fall into the void. (P11).

The observation of P15 regarding not knowing what happens to critical issue reporting after they tell their immediate supervisor existed across several other participants (P1, P3, P7-P10, P13-P17, P20). These participants reflected on how impactful the rank and position within an organization is in influencing whether or not concerns are heard, believed and appropriately addressed. Outside of a security incident, frontline participants were rarely brought into further discussions, meetings or strategy sessions regarding the critical security issues they reported.

All 20 participants doubted that decision-makers fully understood the technical nature of what they were reporting up their management chain, and all agreed that the higher the management chain, the lower the likelihood that significant security concerns are understood from a technical and risk perspective.

Once you hit the VP-level at our company, which is two levels below the CISO, the amount of technical knowhow you encounter is near zero. Nobody at that level likes admitting they don't understand an issue and they certainly don't want to seem incompetent to their bosses. (P4).

Within that broader doubt, a narrower group of nine participants (P3, P7, P8-P10, P12-P13, P15-P16) specifically raised their executive leadership team's grasp of the severity or potential impact that a significant security concern could have on the organization; it is this group of nine, rather than the full sample, that is recorded for this finding in [Table 2](#). All nine participants blamed middle management as the primary cause for this, explicitly calling out (1) the practice of downgrading or minimizing what is being reported as it rises through the organizational levels, (2) not understanding the nature of the issue correctly and (3) avoiding the perception of incompetence of superiors. These were participants' attributions. The interviews do not establish whether reduced severity at higher levels reflected deliberate downgrading, genuine misunderstanding of technical detail or competing organizational priorities, and the finding is therefore reported as a frontline perception of how information was received rather than as a verified account of managerial intent.

One time I saw a PowerPoint presentation that I was not supposed to see regarding a briefing given by senior security leaders to the CISO. Most of the information in the PowerPoint was not accurate. It seemed significantly watered down and stretched the truth in several areas. No wonder we can't actually get anything done sometimes if this is how they report what we find. (P15).

Middle management wants to make it appear to senior leaders that things are in control within the teams below them. I think this is a major factor in watering down what we identify as a major security issue. Nobody wants to make it appear that they're not doing their job properly. (P2).

4.2 Difficulties in cross-team communications

The main themes that emerged from the qualitative analysis of interviews about [RQ2 What cross-team challenges do frontline information security professionals experience when reporting critical security issues?](#) are as follows: First, participants identified the lack of capability or purview of the information security program to fix critical security issues without significant cross-team assistance. Second, participants expressed frustration around

Table 2. Evidence grading of main findings

Finding	RQ	Strongest evidence category	Basis in the interviews	Participants
Reports not received with urgency; no ability to track or follow up on escalated issues	RQ1	(c) loss of visibility; (d) perception	Participants could report to an immediate supervisor but had no confidence that issues progressed above that level, and no formal mechanism to track resolution	16 of 20 (P1-12, P14, P16, P18-P19)
Executive leadership was perceived not to grasp the severity or potential impact of reported issues	RQ1	(d) general perception/inference	Participants inferred limited technical understanding at higher levels and attributed it in part to minimization as information rose	9 of 20 (P3, P7, P8-P10, P12-P13, P15-P16)
Reliance on middle management to broker cross-team remediation; competing priorities	RQ2	Description/perception of coordination	Structural and procedural accounts of how remediation depends on other teams; perceived deprioritization of security work	14 of 20 (P3-P6, P9-P13, P15, P16, P18-P20); 11 of 20 (P1, P4-P6, P9-P13, P15, P20)
Explicit instruction or pressure not to report, or to withhold an issue	RQ3	(a) direct instruction	Participants personally instructed, cautioned, or threatened against reporting (for example, P3 and P12). P14's account describes an instruction given to a colleague rather than one received personally, and is therefore recorded under direct observation below	7 of 20 (P1, P3-P4, P10, P12-P13, P19)
Reported information altered, minimized or watered down	RQ3	(b) direct observation in several accounts; (d) inference in others	Several participants directly observed the alteration or knew a prior report was inaccurate: P15 saw an inaccurate, watered-down briefing; P14 knew a prior report was false; P8 saw a reported vulnerability's severity reduced. The remaining accounts rest on inference from how the issue was subsequently handled	11 of 20 (P2, P4, P6, P7-P9, P12, P14-15, P18, P20)

competing cross-team priorities and a general misunderstanding of the organization's security objectives. Similar to what was reported by the participants, the literature makes it clear that cross-team communications are often more challenging than internal team communications (Van Hoek and Mitchell, 2006).

The aggregated responses show that 14 out of 20 participants (P3-P6, P9-P13, P15, P16, P18-P20) explained that the information security program at their respective companies did not oversee efforts to fix identified security issues. The information security team is rarely responsible for directly remediating acute situations involving a significant security issue. Information security teams often need the help of other internal technology teams to fix problems, patch systems and deploy security controls. All 14 participants reflected on their

frustration around getting other technology teams and the business to resolve issues, resulting in a heavy reliance on middle management to address these issues.

The reality of the job is that there is often little we can actually do beyond finding and reporting things while hoping they're taken care of. Management needs to be involved in the process of explaining the issues and negotiating a fix. There's a big separation of duties approach at my company so technical responsibilities are often spread out over several teams, many of which are resistant to what we are trying to accomplish (P15).

All participants identified a general reliance on middle management to convey their concerns and ideas up the information security management chain and intervene when other teams became resistant to taking action on a significant concern. The reasons behind this difficulty are mainly aversion to business downtime, impact on profits or a general misunderstanding of the problem.

Eleven out of 20 participants (P1, P4-P6, P9-P13, P15, P20) discussed how competing priorities of technology teams and the business often result in security concerns not being appropriately prioritized. Participants P6, P12, P15 and P20 specifically identified management failures to adequately explain security concerns to their peers on nonsecurity teams.

There's a huge divide about what's important to the security program versus what's important to other internal teams. It takes leadership buy-in to push security efforts forward, and many times, I don't feel we have that buy-in. Senior leadership is responsible for that, but unless they're well-informed and understand the risks, changes won't happen. (P6).

4.3 Alteration and suppression of information

The main themes that emerged from the qualitative analysis of interviews about [RQ3](#) *Do frontline information security professionals perceive the details or severity of critical security issues they report are altered or suppressed before reaching decision-makers?* are as follows: First, participants identified many times when critical or significant security concerns were either minimized, watered down or suppressed by their management chain. Second, several participants conveyed times when they were instructed not to report critical findings or reveal certain essential issues to specific levels of management.

The aggregated responses show that eleven out of 20 participants (P2, P4, P6, P7-P9, P12, P14-15, P18, P20) reflected on times when they reported significant security issues to their management chain where details were eventually minimized, watered down, or suppressed. These eleven accounts differ in the directness of the underlying evidence. Some describe directly observing the alteration, or knowing that a prior report was inaccurate, as in the accounts of P15, P14 and P8; others rest on inference from how an issue was subsequently handled. [Table 2](#) therefore records the strongest evidence category represented in this finding rather than implying that all eleven accounts are direct observations.

One time that comes to mind involved a particularly nasty web application vulnerability my team urgently reported. This particular vulnerability was definitely impacting some of our critical internet facing applications. It was going to cost a lot of money and time to fix, so the severity of it was suppressed, which prevented decision-makers from tackling the issue quickly. This activity eventually led to a breach and rather large cybersecurity incident. (P8).

In my first job I worked on a data security team. Our team was responsible for encryption and tokenization of the company's sensitive data. We happened to find an error having to do with tokenization of data that resulted in a large portion of the effort failing. The problem was our division director already reported that we hit 100% saturation for tokenized data. When my boss reported the error and the much lower percentage, he was told in no uncertain terms to not say anything and fix the problem ourselves. The issue was never reported upward and it took us several months to fix the issue. (P14).

Seven out of 20 participants (P1, P3-P4, P10, P12-P13, P19) reported episodes where they were explicitly prevented or cautioned against reporting urgent security concerns. These

episodes were often situations where something was initially misreported to senior leadership, and the restriction was to preserve that initial incorrect reporting. Two participants, P3 and P12, mentioned that their jobs were in jeopardy if they proactively reported the identified issues to anyone outside their team or group.

Once, I attended a meeting with executives regarding a security incident we were in the middle of. Things were not going well and our team had made several mistakes during the initial response to the incident. My boss's boss was aware of these mistakes but conveyed only positive reporting and obviously left out information that made his organization look bad on purpose. I think it was to maintain his image and reputation. I was later told to keep the details left out strictly confidential. (P3).

I had one incident at a former employer that involved uncovering an executive's bad behavior. I can't really say any more details other than this person was trying to go around our security controls, but I felt threatened by management that if I reported this issue, then my career at that company would be hugely impacted. (P12).

These accounts rest largely on direct evidence: participants who personally received instructions not to report (category a) or who directly observed reported information being altered or minimized (category b), such as P15's account of an inaccurate, watered-down briefing, P14's knowledge that a prior report was false and P8's account of a reported vulnerability's severity being reduced. Where, by contrast, a perceived gap rests on inference about whether decision-makers received, understood, or acted on an issue, the data cannot exclude alternative explanations such as resource constraints, competing priorities, risk acceptance, deprioritization or the issue being addressed through another channel.

5. Discussion

This study has uncovered some of how the actions, or lack thereof, regarding middle management in cybersecurity programs impact the overall cybersecurity posture of large organizations. This section will discuss the interpretation of the findings and connect them to existing literature to see how they align or contradict.

5.1 Middle management as an obstacle

While middle management is critical to organizational success ([Harding et al., 2014](#)), this research reveals how it can simultaneously become a roadblock. The roadblocks fall into three categories: structural barriers, procedural inefficiencies and behavioral dynamics. Each category reinforces the others.

Hierarchical structures mean multiple levels separate frontline experts from senior leadership, with technical acumen decreasing at higher levels ([Espinoza, 2023](#)). Behavioral dynamics further complicate matters: participants reported middle management diluting, suppressing or downgrading unfavorable information to avoid appearing incompetent. This aligns with [Stone et al.'s \(2019\)](#) findings regarding underreporting to avoid negative repercussions and [Balogun's \(2003\)](#) observation that middle managers resist escalation due to reputation concerns. Because these dynamics are observed only through frontline accounts, the same patterns may also reflect resource constraints, competing priorities, immature escalation processes, unclear ownership or genuine misunderstanding of technical severity rather than deliberate suppression. The interpretation offered here is therefore one plausible reading of the perceived behavior, not a verified account of managerial motive. When escalation fails, organizations remain exposed to threats for extended periods while senior leadership makes strategic decisions based on incomplete information.

5.2 Challenges in cross-team communications

Effective cross-team communication is essential in large organizations, where teams must collaborate to resolve complex security issues ([Kato et al., 2023](#); [Kim and Lee, 2023](#)), and middle management often brokers these communications when frontline efforts must be

escalated. This study, however, reveals significant cross-team communication challenges that can delay the resolution of critical concerns.

5.3 *Suppression and minimization of critical issues*

One particularly troubling theme that emerged in the study is participants' perception that middle management minimized or suppressed critical security issues. The data capture how frontline professionals experienced and interpreted reporting outcomes; they do not directly observe managerial intent, so this pattern is presented as a perceived dynamic rather than a verified organizational behavior. For organizations where this behavior is prevalent, it presents a unique security threat to their overall security posture. It degrades the integrity of information flow from the frontline to senior decision-makers.

Middle management faces significant pressure to meet performance targets and maintain operational stability (McCann *et al.*, 2008; Sliwka, 2020). Admitting to security vulnerabilities can appear as failure, creating pressure to minimize or alter information. This pressure is one explanation consistent with the frontline accounts; others, such as limited capacity to act on every reported issue or competing business priorities, may produce the same perceived outcome without intentional minimization. This approach delays rapid resolution and deprives senior leadership of accurate information needed for resource allocation and strategic planning (Astakhova, 2017).

5.4 *Implications for cybersecurity governance*

A well-structured cybersecurity governance program depends on the accurate, timely and complete flow of information from frontline employees to senior leaders. The communication breakdowns identified here, and the role of middle management as a perceived bottleneck, point to the need to rethink governance structures around transparency, accountability and proactivity (Greco, 2019).

These findings point to three interventions, each tied to one of the failure modes identified above and each carrying operational tradeoffs that organizations should weigh. To address the behavioral failure mode, the perceived minimization of bad news, middle managers could receive scenario-based training built on documented breaches such as Equifax and Yahoo, paired with anonymous, retaliation-protected reporting channels. Anonymous channels can surface concerns that hierarchy would otherwise suppress, but they can also reduce accountability and generate unverifiable reports, so they are best positioned to supplement rather than replace named escalation. To address the procedural failure mode, the absence of tracking and follow-up, organizations could adopt a formal escalation platform rather than email, with timestamps, severity ratings and required acknowledgment. This improves auditability and lets reporters confirm that an issue progressed, but it adds process overhead and can degrade into a compliance checkbox if it is not resourced and actively monitored. To address the structural failure mode, the distance between frontline experts and decision-makers, organizations could convene an interdisciplinary technical advisory council spanning senior technical staff, legal, risk and audit, and, where warranted, establish direct reporting pathways to senior leadership and watchdog functions. Direct pathways improve leadership visibility, but they can create information overload at the top and bypass legitimate managerial accountability, so they should be reserved for defined severity thresholds rather than used as a routine channel. Table 3 maps each of these findings to its corresponding practical and research implications.

5.5 *Linking findings to theory and research questions*

The findings map onto the theoretical constructs introduced in Section 2, summarized in Table 4. The minimization and watering down reported under RQ3, including P15's account of an inaccurate, watered-down briefing, are consistent with impression management, in which

Table 3. Mapping of findings to practical and research implications

Finding (perceived)	RQ/failure mode	Evidence grade	Practical implication	Research implication
Reports not urgently received, tracked or understood	RQ1/structural	(c) loss of visibility; (d) perception	Direct reporting pathways; interdisciplinary technical advisory council	Escalation latency and the effect of direct channels on response time
Cross-team coordination breakdowns; competing priorities	RQ2/procedural	Description/ perception of coordination	Formal escalation and tracking platform with required acknowledgment	Whether tracking and acknowledgment measurably improve accountability and resolution
Severity perceived as minimized or suppressed	RQ3/behavioral	(a) direct instruction; (b) direct observation (11 of 20)	Scenario-based training; anonymous, retaliation-protected reporting channels	Manager-side and dyadic studies of escalation and suppression decisions

Table 4. Mapping of theoretical constructs to perceived findings

Theoretical construct	Source	Perceived behavior in this study	Manuscript anchor
Impression management	Goffman (1959), DuBrin (2010)	Watering down or minimizing bad news before it reaches senior leadership	§4.3 (RQ3); §4.1
Controllability bias/ illusion of control	Langer (1975), Goerke <i>et al.</i> (2004)	Withholding or delaying escalation while attempting to fix the issue first	§4.3 (e.g. P14)
Agency misalignment	Eisenhardt (1989), Lopes (2016), Stone <i>et al.</i> (2019)	Manager incentives diverging from the organization’s risk interest; misreporting tied to image or metrics	§4.3 (e.g. P3, P15)
Deterrence	Straub (1990), D’Arcy <i>et al.</i> (2009)	Perceived absence of consequences for nonescalation; reports unacknowledged and untracked	§4.1
Organizational sanctions (perceived misalignment)	Prabhu <i>et al.</i> (2025), Merhi and Ahluwalia (2024)	No consequence for suppression, while attempts to escalate drew perceived career risk; sanctions appear to deter reporting rather than suppression	§4.1; §4.3 (e.g. P3, P12)
Protection motivation	Rogers (1975), Johnston and Warkentin (2010)	Perceived lack of urgency where severity, vulnerability, or the efficacy of acting is underappreciated up the chain	§4.1 (RQ1)

Note(s): The deterrence, sanctions and protection-motivation rows draw on construct sources from the compliance and insider-intention literatures, not on direct precedent for middle-management suppression

managers curate information to preserve image or avoid blame (Goffman, 1959; DuBrin, 2010). Accounts of issues being held back while a manager attempted a fix, as in P14’s case, are consistent with controllability bias and the illusion of control (Langer, 1975; Goerke *et al.*, 2004). Misreporting tied to a manager’s image or to performance metrics, as several participants perceived, is consistent with agency theory (Eisenhardt, 1989; Lopes, 2016; Stone *et al.*, 2019).

The urgency theme that runs through RQ1 invites a second set of lenses. The perceived lack of urgency once issues were escalated, and the perception that decision-makers neither grasped the severity nor were held to account for acting, are consistent with deterrence theory, under

which the absence of perceived consequences weakens compliance with security expectations (Straub, 1990; D'Arcy *et al.*, 2009). Protection motivation theory offers a complementary reading: where the severity of a reported issue, the organization's vulnerability to it and the efficacy of acting are underappreciated as information rises, the motivation to respond with urgency weakens (Rogers, 1975; Johnston and Warkentin, 2010).

Organizational sanctions warrant particular attention, because the frontline accounts suggest the structure of consequences may be inverted relative to what deterrence theory would prescribe. Deterrence and sanctions research holds that behavior tracks the perceived certainty and severity of consequences, and that formal sanctions interact with social norms to shape security behavior (Straub, 1990; Prabhu *et al.*, 2025; Merhi and Ahluwalia, 2024). In this study, participants perceived no consequence for failing to escalate or for minimizing a serious issue: reports went unacknowledged, were untracked and carried no follow-up (RQ1). At the same time, several participants who did attempt to surface bad news perceived consequences directed at them, including explicit instructions not to report and, for P3 and P12, a sense that their jobs were at risk (RQ3). Read through a sanctions lens, this is a perceived misalignment: the informal sanction structure appears to deter the desired behavior, escalation, rather than the undesired behavior, suppression. This reading is an interpretation of frontline perceptions rather than a measured account of how any organization actually applied consequences, and the sanctions literature it draws on concerns policy compliance and insider intentions rather than middle-management escalation; it is offered as a construct-level explanation and a direction for manager-side research, not as established fact.

As above, these are construct-level interpretations of frontline perceptions, not verified accounts of managerial motive and the compliance and insider-intention origins of the deterrence and protection-motivation literatures should be kept in view.

RQ1. Do frontline information security professionals perceive that the critical security issues they report are urgently received, properly handled and fully understood by decision-makers?

Sixteen of 20 participants expressed concerns about the lack of urgency and follow-through when they reported significant security issues.

RQ2. What cross-team challenges do frontline information security professionals experience when reporting critical security issues?

The study surfaced significant challenges in cross-team communications, with participants frequently identifying difficulties in coordinating efforts with other departments.

RQ3. Do frontline information security professionals perceive that the details or severity of critical security issues they report are altered or suppressed before reaching decision-makers?

Among the more concerning findings, 11 of 20 participants perceived that the severity of security issues they raised was minimized or suppressed before reaching senior leadership. These perceived patterns are consistent with impression management and controllability concerns, in which managers may seek to avoid blame or the appearance of incompetence. The data cannot, however, exclude alternative explanations such as resource constraints, competing priorities, immature escalation processes or misunderstanding of technical severity, and the findings are therefore presented as frontline perceptions rather than confirmed managerial intent.

6. Conclusion

This study examined how frontline cybersecurity professionals perceive middle management's role in cybersecurity governance in large organizations. Interviews with 20 frontline cybersecurity professionals indicate that, from the frontline perspective, middle

management functions simultaneously as the primary communication channel and, at times, its most significant perceived bottleneck. Three systemic issues emerged: perceived information suppression or minimization associated with impression management concerns, lack of formal mechanisms to track escalated issues and insufficient technical acumen to convey severity accurately to decision-makers. These failures delay rapid response and leave organizations exposed to preventable threats.

This study addressed three research questions. Regarding [RQ1](#), participants perceived that critical security issues were not urgently received or fully understood by decision-makers, with information frequently watered down, underreported or lost as it moved up the hierarchy. For [RQ2](#), significant cross-team communication challenges emerged; the dependency on middle management to broker communications led to delays and miscommunications, and the lack of direct pathways between frontline staff and senior leadership or internal watchdog groups (audit, risk, legal) left decisions made without adequate understanding or urgency. For [RQ3](#), 11 of 20 participants perceived that the severity of security issues was minimized or suppressed before reaching senior leadership, a pattern consistent with impression management and controllability concerns but also open to alternative explanations such as resource constraints, competing priorities and misunderstanding of technical severity.

The findings should prompt large organizations to reexamine rigid hierarchies and cybersecurity governance structures. As developed in the discussion, three interventions, each tied to a specific failure mode and each carrying operational tradeoffs, follow from these findings: scenario-based middle-management training paired with protected reporting channels for the behavioral failure mode; a formal escalation platform with timestamps, severity ratings and required acknowledgment for the procedural failure mode; and an interdisciplinary technical advisory council with bounded, severity-gated direct-reporting pathways for the structural failure mode.

Several limitations apply. The sample of 20 U.S.-based participants may limit generalizability to other national and regulatory contexts; the data are self-reported and drawn only from frontline employees, without middle-manager or senior-leadership perspectives; and because participants reflected on experiences across their careers rather than a single organization, some recall bias is possible.

Future research should develop and test these interventions across organizations to identify industry-specific factors, and examine how different governance structures affect responsiveness to critical issues and whether direct reporting mechanisms measurably reduce information suppression.

Ethics

This study was conducted in accordance with ethical standards for human subjects research and approved by EOU's IRB. Participants provided informed consent prior to interviews.

Data availability

Interview transcripts are not publicly available to protect participant confidentiality.

Supplementary material

The supplementary material for this article can be found online.

References

- Aiello, M., Thompson, S., Raventlow, C., Shaul, G., Randria, M. and Vaughan, A. (2023), *2023 Global Chief Information Security Officer (CISO) Survey*, available at: <https://www.heidrick.com/-/media/heidrickcom/publications-and-reports/2023-global-chief-information-security-officer-survey.pdf>

- Al-Izki, F. and Weir, G.R. (2016), "Management attitudes toward information security in Omani public sector organisations", *2016 Cybersecurity and Cyberforensics Conference (CCC)*, IEEE, pp. 107-112.
- AlGhamdi, S., Win, K.T. and Vlahu-Gjorgievska, E. (2020), "Information security governance challenges and critical success factors: systematic review", *Computers and Security*, Vol. 99, 102030, doi: [10.1016/j.cose.2020.102030](https://doi.org/10.1016/j.cose.2020.102030).
- Angst, C.M., Block, E.S., D'Arcy, J. and Kelley, K. (2017), "When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches", *MIS Quarterly*, Vol. 41 No. 3, pp. 893-A8, doi: [10.25300/misq/2017/41.3.10](https://doi.org/10.25300/misq/2017/41.3.10).
- Astakhova, L.V. (2017), "About informing the leadership in an organization: problems in the context of information security", *Scientific and Technical Information Processing*, Vol. 44 No. 2, pp. 134-140, doi: [10.3103/S0147688217020113](https://doi.org/10.3103/S0147688217020113).
- Balogun, J. (2003), "From blaming the middle to harnessing its potential: creating change intermediaries", *British Journal of Management*, Vol. 14 No. 1, pp. 69-83, doi: [10.1111/1467-8551.00266](https://doi.org/10.1111/1467-8551.00266).
- Bederna, Z., Rajnai, Z. and Szadeczy, T. (2021), "Further strategy analysis of cybersecurity incidents", *Land Forces Academy Review*, Vol. 26 No. 3, pp. 251-260, doi: [10.2478/raft-2021-0032](https://doi.org/10.2478/raft-2021-0032).
- Benneqren, J. and Tropp, A. (2019), "Ethical leadership on the horizontal scene: a case study on middle managers in the tech industry", available at: <https://urn.kb.se/resolve?urn=urn:nbn:se:uu:diva-388865>
- Berg, B.L. (2001), *Qualitative Research Methods for the Social Sciences*, Pearson Education Company.
- Billups, F.D. (2021), *Qualitative Data Collection Tools*, Sage Publications.
- Bitdefender (2023), *Bitdefender 2023 Cybersecurity Assessment*, available at: <https://businessresources.bitdefender.com/bitdefender-2023-cybersecurity-assessment>
- Bobbert, Y. and Mulder, H. (2015), "Governance practices and critical success factors suitable for business information security", in *2015 International Conference on Computational Intelligence and Communication Networks (CICN)*, IEEE, pp. 1097-1104, doi: [10.1109/CICN.2015.216](https://doi.org/10.1109/CICN.2015.216).
- Boehm, J., Kaplan, J.M., Merrath, P., Poppensieker, T. and Stähle, T. (2020), "Enhanced cyberrisk reporting: opening doors to risk-based cybersecurity", *McKinsey on Risk*, Vol. 9, pp. 1-10.
- Braun, V. and Clarke, V. (2006), "Using thematic analysis in psychology", *Qualitative Research in Psychology*, Vol. 3 No. 2, pp. 77-101, doi: [10.1191/1478088706qp063oa](https://doi.org/10.1191/1478088706qp063oa).
- Braun, V. and Clarke, V. (2012), "Thematic analysis", in Cooper, H., Camic, P.M., Long, D.L., Panter, A.T., Rindskopf, D. and Sher, K.J. (Eds), *APA Handbook of Research Methods in Psychology, Research Designs*, American Psychological Association, Vol. 2, pp. 57-71, doi: [10.1037/13620-004](https://doi.org/10.1037/13620-004).
- Bryant, M. and Stensaker, I. (2011), "The competing roles of middle management: negotiated order in the context of change", *Journal of Change Management*, Vol. 11 No. 3, pp. 353-373, doi: [10.1080/14697017.2011.586951](https://doi.org/10.1080/14697017.2011.586951).
- Camic, P.M., Rhodes, J.E. and Yardley, L.E. (2003), *Qualitative Research in Psychology: Expanding Perspectives in Methodology and Design*, American Psychological Association.
- Cavusoglu, H., Mishra, B. and Raghunathan, S. (2005), "The value of intrusion detection systems in information technology security architecture", *Information Systems Research*, Vol. 16 No. 1, pp. 28-46, doi: [10.1287/isre.1050.0041](https://doi.org/10.1287/isre.1050.0041).
- Den Nieuwenboer, N.A., Cunha, J.V.D. and Treviño, L.K. (2017), "Middle managers and corruptive routine translation: the social production of deceptive performance", *Organization Science*, Vol. 28 No. 5, pp. 781-803, doi: [10.1287/orsc.2017.1153](https://doi.org/10.1287/orsc.2017.1153).
- Doherty, N.F. and Fulford, H. (2005), "Do information security policies reduce the incidence of security breaches: an exploratory analysis", *Information Resources Management Journal*, Vol. 18 No. 4, pp. 21-39.
- DuBrin, A.J. (2010), *Impression Management in the Workplace: Research, Theory and Practice*, Routledge, doi: [10.4324/9780203865712](https://doi.org/10.4324/9780203865712).

- D'Arcy, J. and Basoglu, A. (2022), "The influences of public and institutional pressure on firms' cybersecurity disclosures", *Journal of the Association for Information Systems*, Vol. 23 No. 3, pp. 779-805, doi: [10.17705/1jais.00740](https://doi.org/10.17705/1jais.00740).
- D'Arcy, J., Hovav, A. and Galletta, D. (2009), "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach", *Information Systems Research*, Vol. 20 No. 1, pp. 79-98, doi: [10.1287/isre.1070.0160](https://doi.org/10.1287/isre.1070.0160).
- Eisenhardt, K.M. (1989), "Agency theory: an assessment and review", *Academy of Management Review*, Vol. 14 No. 1, pp. 57-74, doi: [10.2307/258191](https://doi.org/10.2307/258191).
- Espinoza, C. (2023), "A CISO isn't a technical role", available at: <https://christianespinoza.com/blog/a-ciso-isnt-a-technical-role/>
- Gashgari, G., Walters, R.J. and Wills, G.B. (2017), "A proposed best-practice framework for information security governance", *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDs)*, pp. 295-301.
- Gates, M. (2024), *ISC2 Report: The Number of Women in Cybersecurity Remains Stagnant, Despite Ongoing Workforce Gap*, ASIS, available at: <https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2024/april/The-Number-of-Women-in-Cyber/>
- Goerke, M., Möller, J., Schulz-Hardt, S., Napiersky, U. and Frey, D. (2004), "'It's not my fault-but only I can change it': counterfactual and prefactual thoughts of managers", *Journal of Applied Psychology*, Vol. 89 No. 2, pp. 279-292, doi: [10.1037/0021-9010.89.2.279](https://doi.org/10.1037/0021-9010.89.2.279).
- Goffman, E. (1959), *The Presentation of Self in Everyday Life*, Doubleday.
- Greco, F. (2019), "Communication in corporate governance behavioral and distortion: a cognitive approach to the management of the company", *New Challenges in Corporate Governance: Theory and Practice, Conference Proceedings*, available at: <https://virtusinterpress.org/Communication-in-corporate-governance-behavioral-and-distortion-A-cognitive.html>
- Hamburg, I. and Grosch, K.R. (2018), "Aligning a cybersecurity strategy with communication management in organizations", in *Digital Communication Management*, IntechOpen, doi: [10.5772/intechopen.75952](https://doi.org/10.5772/intechopen.75952).
- Harding, N., Lee, H. and Ford, J. (2014), "Who is 'the middle manager'", *Human Relations*, Vol. 67 No. 10, pp. 1213-1237, doi: [10.1177/0018726713516654](https://doi.org/10.1177/0018726713516654).
- Hawkins, N. (2017), "Why communication is vital during a cyber-attack", *Network Security*, Vol. 2017 No. 3, pp. 12-14, doi: [10.1016/S1353-4858\(17\)30028-4](https://doi.org/10.1016/S1353-4858(17)30028-4).
- Hayes Munson, K.A. (2022), "Considerations for a successful cybersecurity program", in *Routledge Handbook of Risk Management and the Law*, Routledge.
- Hiekkataipale, M.-M. and Lamsa, A.-M. (2016), "The ethical problems of middle managers and their perceived organizational consequences", *Transformations in Business & Economics*, Vol. 15 No. 3, pp. 36-52.
- Internet Society (2019), "2018 cyber incident & breach trends report", available at: <https://www.internetsociety.org/resources/ota/2019/2018-cyber-incident-breach-trends-report/>
- Johnston, A.C. and Warkentin, M. (2010), "Fear appeals and information security behaviors: an empirical study", *MIS Quarterly*, Vol. 34 No. 3, pp. 549-566, doi: [10.2307/25750691](https://doi.org/10.2307/25750691).
- Kamoun, F. and Nicho, M. (2014), "Human and organizational factors of healthcare data breaches: the swiss cheese model of data breach causation and prevention", *International Journal of Healthcare Information Systems and Informatics*, Vol. 9 No. 1, pp. 42-60.
- Kato, H., Aoyama, T. and Watanabe, K. (2023), "Modeling the hierarchical structure of effective communication factors for cyberattack responses", *Critical Information Infrastructures Security: 17th International Conference, CRITIS 2022*, pp. 197-211, doi: [10.1007/978-3-031-35190-7_14](https://doi.org/10.1007/978-3-031-35190-7_14).
- Kim, S. and Lee, J.J. (2023), *Management of Cybersecurity through Internal Communication, Internal Communication and Employee Engagement*, Routledge.
- Knight, R. and Nurse, J.R.C. (2020), "A framework for effective corporate communication after cyber security incidents", *Computers and Security*, Vol. 99, 102036, doi: [10.1016/j.cose.2020.102036](https://doi.org/10.1016/j.cose.2020.102036).

- Langer, E.J. (1975), "The illusion of control", *Journal of Personality and Social Psychology*, Vol. 32 No. 2, pp. 311-328, doi: [10.1037/0022-3514.32.2.311](https://doi.org/10.1037/0022-3514.32.2.311).
- Leggett, T. (2018), *How VW Tried to Cover up the Emissions Scandal*, BBC, available at: <https://www.bbc.co.uk/news/business-44005844>
- Liginlal, D., Sim, I. and Khansa, L. (2009), "How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management", *Computers and Security*, Vol. 28 Nos 3-4, pp. 215-228, doi: [10.1016/j.cose.2008.11.003](https://doi.org/10.1016/j.cose.2008.11.003).
- Lopes, H. (2016), "Agency theory and social interactions at work", *Review of Social Economy*, Vol. 74 No. 4, pp. 349-368, doi: [10.1080/00346764.2016.1171381](https://doi.org/10.1080/00346764.2016.1171381).
- McCann, L., Morris, J. and Hassard, J. (2008), "Normalized intensity: the new labour process of middle management", *Journal of Management Studies*, Vol. 45 No. 2, pp. 343-371, doi: [10.1111/j.1467-6486.2007.00762.x](https://doi.org/10.1111/j.1467-6486.2007.00762.x).
- Merhi, M.I. and Ahluwalia, P. (2024), "Predicting compliance of security policies: norms and sanctions", *Journal of Computer Information Systems*, Vol. 64 No. 5, pp. 683-697, doi: [10.1080/08874417.2023.2241413](https://doi.org/10.1080/08874417.2023.2241413).
- Miles, M.B. and Huberman, A.M. (1984), "Drawing valid meaning from qualitative data: toward a shared craft", *Educational Researcher*, Vol. 13 No. 5, pp. 20-30, doi: [10.3102/0013189x013005020](https://doi.org/10.3102/0013189x013005020).
- National Institute of Science & Technology (NIST) (2015), "Glossary of the term 'Infosec'", available at: <https://csrc.nist.gov/glossary/term/infosec>
- Newman, L. (2023), "T-Mobile's \$150 million security plan isn't cutting it", *Wired*, available at: <https://www.wired.com/story/tmobile-data-breach-again/>
- Nurse, J.R.C., Creese, S., Goldsmith, M. and Lamberts, K. (2011), "Trustworthy and effective communication of cybersecurity risks: a review", *2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST)*, pp. 60-68, doi: [10.1109/STAST.2011.6059257](https://doi.org/10.1109/STAST.2011.6059257).
- Pacella, J.M. (2016), "The cybersecurity threat: compliance and the role of whistleblowers", *SSRN Scholarly Paper 2803995*, doi: [10.2139/ssrn.2803995](https://doi.org/10.2139/ssrn.2803995).
- Patterson, C.M., Nurse, J.R.C. and Franqueira, V.N.L. (2023), "Learning from cyber security incidents: a systematic review and future research agenda", *Computers and Security*, Vol. 132, 103309, doi: [10.1016/j.cose.2023.103309](https://doi.org/10.1016/j.cose.2023.103309).
- Patton, M.Q. (1990), *Qualitative Evaluation and Research Methods*, 2nd ed., Sage Publications, Newbury Park, CA.
- Patton, M.Q. (2015), "Sampling, qualitative (purposeful)", in *The Blackwell Encyclopedia of Sociology*, doi: [10.1002/9781405165518.wbeoss012.pub2](https://doi.org/10.1002/9781405165518.wbeoss012.pub2).
- Plachkinova, M. and Maurer, C. (2018), "Teaching case: security breach at target", *Journal of Information Systems Education*, Vol. 29 No. 1, p. 11.
- Posthumus, S. and von Solms, R. (2005), "A responsibility framework for information security", in *Security Management, Integrity, and Internal Control in Information Systems*, Springer US, pp. 205-221.
- Prabhu, S., Kocsis, D. and Lew, T.Y. (2025), "Beyond the direct impact of sanctions and subjective norms in cybersecurity", *Information and Computer Security*, Vol. 33 No. 5, pp. 807-825, doi: [10.1108/ICS-04-2025-0148](https://doi.org/10.1108/ICS-04-2025-0148).
- Ransbotham, S. and Mitra, S. (2009), "Choice and chance: a conceptual model of paths to information security compromise", *Information Systems Research*, Vol. 20 No. 1, pp. 121-139, doi: [10.1287/isre.1080.0174](https://doi.org/10.1287/isre.1080.0174).
- Rogers, R.W. (1975), "A protection motivation theory of fear appeals and attitude change", *The Journal of Psychology*, Vol. 91 No. 1, pp. 93-114, doi: [10.1080/00223980.1975.9915803](https://doi.org/10.1080/00223980.1975.9915803).
- Rydland, M. (2020), "Middle managers' role during strategic change: one size does not fit all", *Beta*, Vol. 34 No. 1, pp. 5-22, doi: [10.18261/issn.1504-3134-2020-01-01](https://doi.org/10.18261/issn.1504-3134-2020-01-01).
- Scarborough, H. and Burrell, G. (1996), "The axeman cometh: the changing role and knowledge of middle managers", in Clegg, S. and Palmer, G. (Eds), *The Politics of Management Knowledge*, Sage, Thousand Oaks, CA.

- Schlackl, F., Link, N. and Hoehle, H. (2022), "Antecedents and consequences of data breaches: a systematic review", *Information & Management*, Vol. 59 No. 4, 103638, doi: [10.1016/j.im.2022.103638](https://doi.org/10.1016/j.im.2022.103638).
- Shaikh, F.A. and Siponen, M. (2023), "Information security risk assessments following cybersecurity breaches: the mediating role of top management attention to cybersecurity", *Computers and Security*, Vol. 124, 102974, doi: [10.1016/j.cose.2022.102974](https://doi.org/10.1016/j.cose.2022.102974).
- Shayo, C. and Lin, F. (2019), "An exploration of the evolving reporting organizational structure for the chief information security officer (CISO) function", *Journal of Computer Science*, Vol. 7 No. 1, pp. 1-20, doi: [10.15640/jcsit.v7n1a1](https://doi.org/10.15640/jcsit.v7n1a1).
- Shi, W., Markoczy, L. and Dess, G.G. (2009), "The role of middle management in the strategy process: group affiliation, structural holes, and tertius iungens", *Journal of Management*, Vol. 35 No. 6, pp. 1453-1480, doi: [10.1177/0149206309346338](https://doi.org/10.1177/0149206309346338).
- Sliwka, D. (2020), *Bonuses and Performance Evaluations*, IZA World of Labor, doi: [10.15185/izawol.478](https://doi.org/10.15185/izawol.478).
- Stephenson, P. (2003), "Modeling of post-incident root cause analysis", *International Journal of Digital Evidence*, Vol. 2, available at: https://www.researchgate.net/publication/220542511_Modeling_of_Post-Incident_Root_Cause_Analysis
- Stone, M., Aravopoulou, E., Evans, G., Aldhaen, E. and Parnell, B.D. (2019), "From information mismanagement to misinformation: the dark side of information management", *The Bottom Line*, Vol. 32 No. 1, pp. 47-70, doi: [10.1108/BL-09-2018-0043](https://doi.org/10.1108/BL-09-2018-0043).
- Straub, D.W. (1990), "Effective IS security: an empirical study", *Information Systems Research*, Vol. 1 No. 3, pp. 255-276, doi: [10.1287/isre.1.3.255](https://doi.org/10.1287/isre.1.3.255).
- Tatu, T., Ament, C. and Jaeger, L. (2018), "Lessons learned from an information security incident: a practical recommendation to involve employees in information security", *Proceedings of the 51st Hawaii International Conference on System Sciences*, pp. 3736-3745, doi: [10.24251/HICSS.2018.471](https://doi.org/10.24251/HICSS.2018.471).
- U.S. House of Representatives (2018), *The Equifax Data Breach*, available at: <https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf>
- Valukas, A.R. (2010), *Report of Anton R. Valukas, Examiner: Lehman Brothers Holdings Inc*, United States Bankruptcy Court Southern District of New York, Chapter 11 Case No. 08-13555 (JMP).
- Van Hoek, R.I. and Mitchell, A.J. (2006), "The challenge of internal misalignment", *International Journal of Logistics Research and Applications*, Vol. 9 No. 3, pp. 269-281, doi: [10.1080/13675560600859342](https://doi.org/10.1080/13675560600859342).
- Vaz, S.L. and Bulgacov, S. (2018), "Middle managers' involvement in strategy: analyzing the past and projecting the future", *RAC*, Vol. 22 No. 3, pp. 380-402, doi: [10.1590/1982-7849rac2018170191](https://doi.org/10.1590/1982-7849rac2018170191).
- Verizon (2022), "2022 data breach investigations report (DBIR)", available at: <https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf>
- White, M.J. (2019), "What I've learned about white-collar crime", *Harvard Business Review*, available at: <https://hbr.org/2019/07/what-ive-learned-about-white-collar-crime>
- Wolff, J. (2014), "Models for cybersecurity incident information sharing and reporting policies", *SSRN Scholarly Paper 2587398*, doi: [10.2139/ssrn.2587398](https://doi.org/10.2139/ssrn.2587398).
- Wooldridge, B., Schmid, T. and Floyd, S.W. (2008), "The middle management perspective on strategy process: contributions, synthesis, and future research", *Journal of Management*, Vol. 34 No. 6, pp. 1190-1221, doi: [10.1177/0149206308324326](https://doi.org/10.1177/0149206308324326).

Further reading

- Badhwar, R. (2021), "Cyber program turnaround by new CISO", in Badhwar, R. (Ed.), *The CISO's Transformation: Security Leadership in a High Threat Landscape*, Springer International Publishing, pp. 15-19, doi: [10.1007/978-3-030-81412-0_3](https://doi.org/10.1007/978-3-030-81412-0_3).

- Ford, A., Al-Nemrat, A., Ghorashi, S.A. and Davidson, J. (2022), "The impact of CISO appointment announcements on the market value of firms", *International Conference on Cyber Warfare and Security*, Vol. 17 No. 1, doi: [10.34190/iccws.17.1.49](https://doi.org/10.34190/iccws.17.1.49).
- Karanja, E. and Rosso, M.A. (2017), "The chief information security officer: an exploratory study", *Journal of International Technology and Information Management*, Vol. 26 No. 2, pp. 23-47, doi: [10.58729/1941-6679.1299](https://doi.org/10.58729/1941-6679.1299).
- Melaku, H.M. (2023), "A dynamic and adaptive cybersecurity governance framework", *Journal of Cybersecurity and Privacy*, Vol. 3 No. 3, pp. 327-350, doi: [10.3390/jcp3030017](https://doi.org/10.3390/jcp3030017).

Corresponding author

Brian Scavotto can be contacted at: bscavotto@eou.edu