Asian Journal of Current Research

Volume 11, Issue 3, Page 233-248, 2026; Article no.AJOCR.15330
ISSN: 2456-804X

From Risk Reporting to Resilience: A Narrative Integrative Review of Cybersecurity Governance Practices in Organizations

William Asare Yirenkyi [a*], Apaflo Godson Teye [b], Matilda Konotey [a] and Yeboah Mary Magdalene [c]

[a] Temple University, Fox School of Business, Philadelphia, PA, United States.
[b] University of Energy and Natural Resources, Sunyani, Ghana.
[c] University of Ghana, Accra, Ghana.

Authors' contributions

This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.

Article Information

DOI: https://doi.org/10.56557/ajocr/2026/v11i310877

Open Peer Review History:
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: https://prh.ikprress.org/review-history/15330

Review Article

Received: 20/05/2026
Accepted: 16/07/2026
Published: 20/07/2026

Abstract

Cybersecurity has moved from a peripheral technical function to a core pillar of organizational governance, driven by the escalating frequency and cost of digital intrusions, tightening disclosure regulation, and growing recognition that technical controls alone cannot guarantee continuity of operations. This narrative integrative review synthesises contemporary academic literature on cybersecurity governance, tracing its evolution from a compliance-oriented, risk-reporting paradigm toward an integrated model of organizational cyber resilience. The review examines governance structures and board oversight arrangements, the integration of

**Corresponding author: E-mail: asarewilliam0@gmail.com;*

Cite as: *Yirenkyi, W. A., Teye, A. G., Konotey, M., & Magdalene, Y. M. (2026). From Risk Reporting to Resilience: A Narrative Integrative Review of Cybersecurity Governance Practices in Organizations. Asian Journal of Current Research, 11(3), 233–248. https://doi.org/10.56557/ajocr/2026/v11i310877*

cybersecurity into enterprise risk management, the conceptual architecture of organizational cyber resilience, the human and cultural determinants of governance effectiveness, sector-specific and supply-chain vulnerabilities, financial and insurance mechanisms for risk transfer, the regulatory and standards landscape, and approaches to measuring governance maturity. Findings indicate that although disclosure obligations and formal oversight structures have proliferated, substantive board-level expertise remains scarce, enterprise risk management integration is uneven, and resilience-building efforts are frequently undermined by fragmented accountability and inconsistent measurement practices. The review argues that a durable shift from reactive risk reporting to genuine organizational resilience requires coherent alignment across governance structures, cultural investment, supply-chain oversight and outcome-based metrics. Directions for future research and the practical implications of these findings for boards, risk officers and regulators are discussed.

Keywords: Cybersecurity governance; organizational resilience; enterprise risk management; board oversight; cyber risk disclosure.

1. Introduction

1.1 The Rising Salience of Cybersecurity Governance

Digital transformation has embedded information systems into nearly every operational, financial and strategic process of contemporary organizations, extending the attack surface available to malicious actors and elevating cybersecurity from a specialist information-technology concern to a matter of enterprise-wide governance (Dalal et al., 2022). Cloud computing, remote working and interconnected supply chains have each opened new vectors through which adversaries can compromise organizational assets (Kuzior et al., 2024). Cybersecurity was once treated as a discrete technical discipline sitting within the information-technology function; it is now widely regarded instead as a strategic risk that intersects with financial reporting, legal compliance, operational continuity and reputational management (Schinagl & Shahim, 2020). Recent evidence further indicates that boards frequently delegate information-technology governance rather than integrate it fully into corporate governance, despite the increasing importance of board-level information-technology competence (Caluwe et al., 2024).

1.2 Governance as a Response to Escalating Risk

This reframing has been reinforced by regulation that requires boards and senior executives to demonstrate active oversight of cybersecurity risk rather than delegate it wholesale to technical specialists. Disclosure regimes in major jurisdictions increasingly compel organizations to report on governance arrangements, board expertise and material incidents, turning cybersecurity governance from an internal operational matter into a subject of external scrutiny by investors, regulators and the public (Elsayed et al., 2024). Yet the expansion of formal oversight structures has not been matched by a comparable growth in substantive board-level expertise, which raises a genuine question: are governance reforms achieving their intended protective effect, or largely satisfying symbolic compliance expectations (Lowry et al., 2026). Empirical evidence indicates that board oversight and cybersecurity expertise are associated with clearer and more specific risk disclosures, although these benefits are weaker where oversight remains largely symbolic (Gao & Calderon, 2025).

1.3 From Reporting to Resilience

Alongside the growth of disclosure-oriented governance, a distinct and increasingly influential strand of scholarship argues that risk reporting, while necessary, is not sufficient on its own to protect organizations against the consequences of cyber incidents. This literature advances the concept of organizational cyber resilience — the capacity of an organization to anticipate, withstand, adapt to and recover from cyber disruptions while continuing to deliver its core objectives (Neri, Niccolini, & Virili, 2026). Resilience thinking reframes cybersecurity governance away from a narrow focus on preventing breaches and toward a broader concern with sustaining organizational function under conditions of persistent, evolving threat (Dupont, Shearing, Bernier, & Leukfeldt, 2023). The tension between compliance-driven reporting and capability-driven resilience forms the central thematic axis of this review. Field evidence on accountability configurations further suggests that effective cybersecurity governance depends not only on the formal separation of responsibilities but also on sustained engagement across control functions, executive management and boards (Slapničar et al., 2023).

1.4 Scope, Research Gap and Objectives

Recent firm-level evidence shows that cyber risk can be incorporated into enterprise risk management processes, although the sophistication and framing of that integration vary considerably across organizations (Romanosky & Petrun Sayers, 2024). Despite a substantial and rapidly growing body of scholarship addressing individual facets of cybersecurity governance — board oversight, enterprise risk management integration, organizational culture, sector-specific vulnerabilities — comparatively few contributions attempt to synthesise these strands into a coherent account of how organizations move from reactive, disclosure-oriented practices toward embedded, resilience-oriented governance. Existing systematic reviews tend to be narrowly bounded, addressing single dimensions such as board composition, insurance markets or supply-chain exposure in isolation, leaving practitioners and scholars without an integrated view of how these elements interact across the governance life cycle. This review addresses that gap by drawing together evidence from accounting, management, information systems and risk research to construct a cross-disciplinary account of how cybersecurity governance has developed over the past decade. Its scope is confined to organizational-level governance practices in private and public sector entities; it does not extend to national cyber-defence policy or military cyber operations, which follow different institutional logics and are treated as a distinct domain. The review pursues three objectives: first, to characterise the principal governance structures and disclosure practices that have emerged under regulatory and market pressure; second, to examine how — and how far — cybersecurity risk has been integrated into broader enterprise risk management systems; and third, to evaluate the conceptual and practical mechanisms through which organizations attempt to build genuine cyber resilience beyond compliance-oriented reporting.

2. Methods for Literature Selection

2.1 Databases and Indexing Sources Searched

The literature underpinning this review was identified through structured searches of Web of Science, Scopus and Google Scholar, supplemented by six field-specific indexing sources chosen for their relevance to the intersecting disciplines of information systems, accounting and risk management: the Association for Information Systems electronic library, Business Source, EconLit, ACM Digital Library indexing records, IEEE Xplore indexing records, and the RePEc bibliographic database. PubMed was consulted but returned negligible relevant material given the organizational, rather than clinical, focus of the topic, and was therefore not drawn upon for the final reference set.

2.2 Search Strings and Date Range

Search strings combined core concept clusters using Boolean operators, for example ("cybersecurity governance" OR "information security governance") AND ("board oversight" OR "risk disclosure" OR "enterprise risk management"), and ("cyber resilience" OR "organizational resilience") AND ("cybersecurity" OR "information security"). Further strings targeted subordinate themes, including cybersecurity culture, third-party and supply-chain cyber risk, cyber insurance, and regulatory frameworks such as the NIST Cybersecurity Framework and the European Union Network and Information Security Directive. The search covered material published between January 2015 and 2 April 2026, a window chosen to capture the period during which cybersecurity governance emerged as a distinct scholarly and regulatory concern; foundational conceptual works published earlier were retained where they remain the primary theoretical reference point for later empirical studies.

2.3 Inclusion and Exclusion Criteria

Studies were included where they were published in peer-reviewed academic journals, addressed organizational-level cybersecurity governance, risk management or resilience, and were available in English. Studies were excluded where they consisted of grey literature, conference proceedings without subsequent journal publication, preprints, patents, trade or vendor publications, or where their empirical focus was confined to purely technical security engineering without a governance, management or organizational dimension. Institutional reports from bodies such as the National Institute of Standards and Technology were consulted for definitional and regulatory context but treated as background material rather than counted among the peer-reviewed evidence base.

2.4 Rationale for a Narrative Rather Than Systematic Review Approach

A narrative integrative review was chosen over a systematic review because the aim here is to synthesise conceptually diverse literatures — accounting disclosure research, management theories of organizational resilience, information systems scholarship on security culture — into a coherent thematic account, rather than to answer a single, narrowly defined empirical question through a predefined protocol. Narrative reviews are recognised as better suited to tracing the development of a field, identifying cross-cutting themes and surfacing conceptual tension, since their flexibility permits integration across heterogeneous methodologies and disciplinary traditions that a systematic protocol would otherwise exclude (Ferrari, 2015). This is a deliberate trade-off: systematic reviews offer greater reproducibility for narrowly bounded questions, but they are less suited to mapping an emerging, multidisciplinary field such as cybersecurity governance, where relevant evidence is scattered across accounting, management science, information systems and risk journals that follow markedly different methodological conventions.

2.5 Screening Workflow, Duplicate Handling and Selection of Influential Studies

Records retrieved from each database were screened first by title and abstract against the inclusion criteria, with full-text review conducted for studies passing this initial filter. Duplicate records arising from overlapping database coverage were identified by comparing author names, titles and publication years, and removed before full-text assessment. Where several studies addressed closely related questions, preference went to more recent publications, to studies in higher-impact journals within the relevant subfield, and to studies already cited within subsequent systematic or integrative reviews — taken as a marker of field-level influence. English-language restriction applied throughout; no restriction was placed on geographic origin, reflecting the global character of cybersecurity governance research. This process yielded the set of studies synthesised below.

3. Theoretical Foundations of Cybersecurity Governance

Cybersecurity governance research draws on several overlapping theoretical traditions, most prominently agency theory and institutional theory, to explain how boards and executives approach oversight of a risk domain in which technical expertise is unevenly distributed. Agency theory frames cybersecurity governance as a problem of aligning the interests and information of executives, who possess operational knowledge of cyber risk, with those of boards and shareholders, who typically lack such expertise yet bear ultimate responsibility for oversight (Lowry et al., 2026). This asymmetry has practical consequences: field research on board oversight has found that although directors consistently identify cybersecurity as a top strategic priority, their oversight activity often lacks the independence and depth associated with well-established areas of board responsibility such as financial reporting, simply because few directors have the technical background to interrogate management assertions critically (Lowry et al., 2026).

Institutional theory offers a complementary explanation. It proposes that governance structures are adopted not solely, or even primarily, for their functional effectiveness, but to secure legitimacy with external stakeholders — regulators, investors, business partners — who expect visible evidence of oversight (Schinagl & Shahim, 2020). Under this view, the proliferation of board-level cybersecurity committees, named cyber-risk officers and disclosure statements may reflect an institutionalised script for demonstrating conformity with expected governance norms, independent of whether such structures materially reduce organizational vulnerability. Schinagl and Shahim (2020) argue that information security governance research has historically been dominated by narrowly technical, compliance-based conceptions situated at the operational level, and that a more mature perspective requires locating governance decisions within the strategic apparatus of the organization — extending, as they put it, from the technical basement to the executive boardroom.

A further theoretical strand draws on organizational resilience theory, which treats resilience not as a static attribute but as a dynamic capability comprising anticipatory, absorptive, adaptive and restorative dimensions unfolding across time (Neri, Niccolini, & Virili, 2026). This perspective diverges from the risk-management tradition, which tends to emphasise the identification and mitigation of discrete threats, by treating disruption instead as an inevitable feature of organizational life and directing attention toward the capacity to sustain core functions despite it. Integration of resilience theory with governance scholarship has been comparatively recent, and much of the literature reviewed below reflects an ongoing effort to reconcile these traditions — moving from a governance model preoccupied with reporting and compliance toward one oriented around organizational capability and adaptive capacity.

4. Governance Structures, Board Oversight and Risk Disclosure

4.1 The Expansion of Formal Oversight Structures

Regulatory intervention has been a principal driver of change in cybersecurity governance structures over the past decade. In the United States, disclosure rules introduced by securities regulators now require publicly traded companies to report material cybersecurity incidents and describe their governance processes for assessing and managing cyber risk, prompting a marked increase in the proportion of firms disclosing board-level oversight arrangements (Elsayed et al., 2024). Comparable developments have occurred in the European Union, where network and information security directives have obliged covered entities to strengthen governance accountability and incident-reporting obligations. Comparative analyses of cybersecurity risk disclosure between United States and non-United States firms find that the regulatory environment substantially shapes the extent and specificity of disclosed risk information, with firms operating under more prescriptive regimes disclosing more granular detail on governance processes and risk exposure (Calderon & Gao, 2022).

4.2 The Gap between Formal Structures and Substantive Oversight

Despite this expansion of formal disclosure, evidence consistently points to a persistent gap between the existence of governance structures and their substantive effectiveness. Field-based qualitative research with corporate directors finds that oversight practices frequently take the form of periodic briefings and question-and-answer sessions with cybersecurity executives — a format that gives limited scope for independent verification of the information presented, and may substitute the appearance of diligence for genuine scrutiny (Lowry et al., 2026). This is consistent with the broader institutional account of governance as partly symbolic in character, whereby boards adopt legitimacy-conferring practices under conditions of information asymmetry without necessarily transforming the organization's underlying risk profile.

4.3 Disclosure as a Governance and Accountability Mechanism

Risk disclosure research has examined not only the extent of reporting but its downstream consequences for organizational behaviour and stakeholder confidence. Evidence from the banking sector shows that cybersecurity disclosure is associated with improved financial performance, and that this relationship is moderated by the strength of underlying corporate governance mechanisms — suggesting disclosure works best as an accountability device when embedded within a broader governance apparatus, rather than treated as a standalone compliance exercise (Elsayed et al., 2024). This aligns with a wider argument that disclosure regulation, while valuable for improving market transparency, does not on its own guarantee improved security posture; translating disclosed commitments into operational practice depends on the depth of board engagement and the resources allocated to cybersecurity functions.

Table 1 summarises key empirical findings concerning governance structures, board expertise and risk disclosure drawn from the reviewed literature.

Table 1. Governance structures, board oversight and cybersecurity risk disclosure

Theme	Key finding	Implication for organizations	Source
Board oversight depth	Directors prioritise cybersecurity but often lack independent verification capacity	Formal committees may provide symbolic rather than substantive assurance	Lowry et al. (2026)
Regulatory disclosure	Mandatory incident and governance disclosure has expanded sharply since 2023	Disclosure quality is uneven and shaped by jurisdictional stringency	Elsayed et al. (2024)
Cross-jurisdictional variation	United States and non-United States firms differ in disclosure specificity	Harmonisation of disclosure standards would aid comparability	Calderon & Gao (2022)
Governance maturity model	Governance research has historically been technically bounded rather than strategic	A "basement-to-boardroom" reconceptualisation is required	Schinagl & Shahim (2020)
Disclosure–performance link	Cybersecurity disclosure correlates with improved bank performance, moderated by governance strength	Disclosure is most effective when integrated with strong governance	Elsayed et al. (2024)

The pattern in Table 1 is that regulatory pressure has succeeded in expanding the visibility of cybersecurity governance to external stakeholders, but has been markedly less successful in closing the expertise gap that underlies much of the substantive weakness identified by field researchers. This tension between visible compliance and underlying capability recurs throughout the review and motivates the shift in emphasis, in the sections that follow, toward enterprise risk management integration and organizational resilience as complements to disclosure-based governance.

5. Integrating Cybersecurity into Enterprise Risk Management

5.1 The Case for Integration

A recurring theme in the literature is that cybersecurity risk should not be managed as an isolated technical concern, but integrated into the organization's broader enterprise risk management architecture alongside financial, operational, legal and reputational risk categories. Proponents argue that treating cybersecurity as a siloed information-technology function weakens organizational risk visibility, delays incident response and obscures the interdependencies between cyber events and other business risks, such as supply disruption or regulatory penalty exposure. Embedding cybersecurity within enterprise risk management is said to enable more proactive identification, prioritisation and mitigation of cyber risk by aligning it with the same governance cadence, escalation pathways and reporting language used for other categories of enterprise risk.

5.2 Persistent Barriers to Integration

Despite the conceptual appeal of integration, empirical studies find its implementation remains inconsistent across organizations. A frequently cited barrier is the communication gap between technical cybersecurity teams and senior leadership, whose risk vocabularies and analytical frameworks often diverge, complicating the translation of technical vulnerability data into terms meaningful for strategic decision-making. The absence of standardised cyber-risk metrics compounds the difficulty: financial and operational risk categories benefit from decades of actuarial and accounting convention, whereas cybersecurity risk quantification remains comparatively immature and contested. Organizations that have attempted integrated metrics, such as expected loss from cyber incidents or risk-adjusted control effectiveness measures, report that implementation requires a cultural shift extending well beyond new reporting templates, since risk owners across business units must be persuaded to treat cyber exposure with the same rigour historically reserved for financial risk.

5.3 Governance Roles within Integrated Risk Frameworks

Effective integration depends on clearly delineated accountability spanning operational management, oversight functions and independent assurance. The "three lines" model widely used in enterprise risk management assigns operational risk ownership to business units, risk oversight to dedicated risk and compliance functions, and independent assurance to internal audit; extending this model to cybersecurity requires each line to possess sufficient cyber-specific competence to discharge its distinct role. Evidence on layered accountability models suggests that internal audit functions face particular structural constraints in providing timely assurance, since traditional audit cycles spanning several years sit poorly with the pace at which cyber threats and organizational technology environments evolve, creating a persistent lag between assurance activity and the current risk landscape.

Emerging supply-chain and enterprise risk research illustrates the practical stakes of this integration challenge. Studies of cyber risk management in logistics and supply-chain contexts find that the strategies organizations adopt to manage cyber risk have measurable consequences for the degree of cybersecurity integration achieved with suppliers, customers and internal functions, and that stronger integration is in turn associated with greater supply-chain cyber resilience and robustness (Jazairy, Brho, Manuj, & Goldsby, 2024). This supports the broader proposition that enterprise risk management integration is not merely an internal administrative exercise, but a determinant of an organization's capacity to withstand disruption propagating through its extended business network.

6. Organizational Cyber Resilience: Concepts and Frameworks

6.1 Conceptual Development

The concept of organizational cyber resilience has developed rapidly over the past decade as scholars have sought to reconcile the information-security tradition — which emphasises preventing and detecting specific

threats — with the organizational resilience tradition from management science, which emphasises the capacity to absorb, adapt to and recover from disruption more broadly. A recent integrative conceptual framework synthesising both literatures identifies temporal dimensions spanning anticipatory action before disruption, absorptive and adaptive response during disruption, and restorative action after disruption, and proposes that organizational cyber resilience be understood as the intersection of these capabilities applied specifically to cyber-related disruption (Neri, Niccolini, & Virili, 2026). This framework builds on earlier historical and conceptual reviews tracing the resilience concept from its origins in ecological and engineering systems theory to its contemporary application in digital and organizational contexts, and notes that definitional inconsistency across the literature has historically hampered comparability of empirical findings (Tzavara & Vassiliadis, 2024). Complementary conceptual work outside the cyber domain has argued for redefining the broader organizational resilience construct through a frame-based, ecology-inspired methodology, underscoring that resilience thinking itself remains an actively contested and evolving construct even before it is applied to the cyber context specifically (Khan, Ozkan, Deligonul, & Cavusgil, 2024).

The anticipatory dimension of resilience has itself attracted growing empirical attention, particularly through the lens of cyber threat intelligence. A systematic review of cyber threat intelligence practice finds that the systematic gathering, processing and dissemination of information on emerging threats materially strengthens an organization's anticipatory posture, and proposes a framework combining a shared knowledge base, detection models and visualisation tools to operationalise this capability (Saeed, Suayyid, Al-Ghamdi, Al-Muhaisen, & Almuhaideb, 2023). This body of work situates threat intelligence not as a purely technical function but as an organizational capability integral to the anticipatory phase of the resilience life cycle described above.

6.2 Resilience as a Socio-Technical Capability

A significant strand of resilience scholarship argues against purely technological conceptions of cyber resilience, contending that resilience is fundamentally a socio-technical property arising from the interaction of technical controls with organizational structures, decision-making processes and human behaviour. Research examining the tensions inherent in cyber-resilience practice finds that the sensemaking processes through which organizations interpret and respond to cyber incidents are frequently as consequential for resilience outcomes as the underlying technical architecture, and that resilience efforts risk failure where they neglect these social and organizational dimensions in favour of narrowly technical fixes (Dupont, Shearing, Bernier, & Leukfeldt, 2023). A related argument, examining the addition of social considerations to technological resilience measures, finds that resilience-enhancing interventions prove more durable when they account for organizational learning, communication patterns and the distribution of decision authority during crisis conditions, rather than relying solely on redundancy and technical hardening (Dunn Cavelty, Eriksen, & Scharte, 2023).

6.3 Sector-Specific Resilience Frameworks

Resilience frameworks have been developed and empirically examined across a range of sectors, reflecting differences in threat exposure, regulatory obligation and operational tolerance for disruption. In financial services, cyber resilience is theorised as both particularly significant and particularly hard to operationalise, given the sector's role as critical infrastructure for the broader economy and the systemic consequences a major incident could generate beyond the organization itself (Dupont, 2019). In healthcare, resilience research emphasises the interaction between cybersecurity and digital transformation, finding that organizations pursuing rapid digitalisation of clinical and administrative systems face compounded resilience challenges as new digital dependencies arrive faster than the security and continuity controls needed to match them (Garcia-Perez, Cegarra-Navarro, Sallos, Martinez-Caro, & Chinnaswamy, 2023). Studies of critical infrastructure organizations more broadly have examined cybersecurity performance and crisis response through an intellectual capital lens, finding that human and relational capital, alongside technical infrastructure, materially shape an organization's capacity to respond effectively to a cyber crisis (Garcia-Perez, Sallos, & Tiwasing, 2023).

Manufacturing and construction, historically less digitally mature than finance or healthcare, have generated resilience research focused on the challenge of retrofitting cybersecurity governance onto operational technology environments not originally designed with connectivity or cyber risk in mind. A systemic framework for cybersecurity in construction highlights the sector's fragmented, project-based structure as a distinctive governance challenge, since resilience must be coordinated across shifting networks of contractors and subcontractors rather than within a single stable organizational boundary (Turk, García de Soto, Mantha,

Maciel, & Georgescu, 2022). Similarly, research proposing a sustainability-oriented cybersecurity framework for manufacturing situates resilience within the convergence of operational and information technology, arguing that resilience frameworks built for conventional enterprise information technology need substantial adaptation before they can be applied to industrial control environments (Alqudhaibi, Deshpande, Jagtap, & Salonitis, 2023).

6.4 Precursors, Outcomes and Assurance of Resilience

Beyond conceptual and sectoral frameworks, a smaller body of exploratory empirical work has attempted to identify the specific organizational precursors that give rise to cyber resilience and the outcomes that follow from it. One such study finds that resilience is shaped by a combination of leadership commitment, resource availability and prior incident experience, and that higher resilience in turn predicts faster operational recovery and lower reputational damage following a disruptive event (Tsen, Ko, & Slapnicar, 2022). This precursor–outcome framing offers a useful complement to the more conceptual frameworks discussed above, since it points toward the specific organizational levers that practitioners might act upon rather than describing resilience purely in structural or definitional terms.

A distinct question concerns how organizations obtain assurance regarding their cyber-resilience posture — a matter of particular relevance to boards seeking to discharge their oversight responsibilities credibly. Research on obtaining reasonable assurance over cyber resilience argues that traditional audit approaches, oriented toward point-in-time compliance verification, sit uneasily with a risk domain characterised by continuous change, and proposes that assurance frameworks instead evaluate the organization's dynamic capability to detect and respond to emerging threats, rather than simply confirming the presence of specified controls at a single moment (Caron, 2021). This is reinforced by systematic reviews of cyber-resilience assessment frameworks, which find considerable heterogeneity in the metrics and methodologies used across academic and practitioner assessment tools, complicating efforts to benchmark resilience maturity consistently across organizations and sectors (Sepúlveda Estay, Sahay, Barfod, & Jensen, 2020).

Table 2 summarises the principal conceptual and sectoral resilience frameworks identified in the literature.

Table 2. Conceptual and sectoral frameworks for organizational cyber resilience

Framework or focus	Core contribution	Sector or context	Source
Integrative conceptual framework	Synthesises organizational resilience and cyber resilience literatures into temporal dimensions	Cross-sector	Neri et al. (2026)
Historical-conceptual evolution	Traces definitional development of cyber resilience from engineering to organizational contexts	Cross-sector	Tzavara & Vassiliadis (2024)
Socio-technical sensemaking	Emphasises interpretive and communicative processes during incident response	Cross-sector	Dupont et al. (2023)
Social-technical integration	Argues resilience requires social alongside technological measures	Critical infrastructure	Dunn Cavelty et al. (2023)
Financial-sector resilience	Highlights systemic significance of resilience in financial institutions	Banking and finance	Dupont (2019)
Digital transformation and resilience	Links pace of digitalisation to resilience vulnerability	Healthcare	Garcia-Perez et al. (2023)
Intellectual capital perspective	Links human and relational capital to crisis response capacity	Critical infrastructure	Garcia-Perez et al. (2023)
Systemic project-based framework	Addresses fragmented, multi-contractor governance challenges	Construction	Turk et al. (2022)
Sustainability-oriented framework	Addresses operational technology and information technology convergence	Manufacturing	Alqudhaibi et al. (2023)
Precursor–outcome model	Links leadership, resources and prior experience to recovery speed and reputational impact	Cross-sector	Tsen et al. (2022)
Assurance-based approach	Proposes dynamic, capability-based assurance over static compliance checks	Cross-sector	Caron (2021)

The evidence in this section indicates that organizational cyber resilience has matured into a distinct and theoretically grounded field, yet fragmentation across sectoral applications and assessment methodologies continues to impede the development of comparable, cross-organizational resilience benchmarks — a point taken up directly in Section 11.

7. Human, Cultural and Behavioural Dimensions of Governance

7.1 Culture as a Governance Determinant

A substantial body of scholarship holds that formal governance structures and technical controls are necessary but insufficient conditions for effective cybersecurity, and that organizational culture exerts an independent, often decisive, influence on security outcomes. A systematic review of cybersecurity culture research, examining fifty-eight studies published over the preceding decade, finds that the most consistently identified determinants of a strong security culture are visible top-management support, clearly articulated security policy, and sustained awareness and training, while noting that relatively few proposed cultural frameworks have been rigorously evaluated in real-world organizational settings (Uchendu, Nurse, Bada, & Furnell, 2021). This gap between conceptual sophistication and empirical validation recurs across the culture literature and mirrors the assessment fragmentation identified in resilience scholarship more broadly.

7.2 Behavioural Governance and Knowledge Sharing

Beyond broad cultural climate, research has examined the specific behavioural mechanisms through which security-conscious norms are transmitted and reinforced within organizations. Work grounded in organizational science argues that cybersecurity should be approached as fundamentally a human and organizational challenge rather than a purely technical one, since most successful intrusions exploit human decision-making vulnerabilities rather than purely technical weaknesses, and calls for closer integration between organizational behaviour research and cybersecurity practice to address this gap (Dalal et al., 2022). This reframes governance not merely as a matter of policy design but as an ongoing exercise in shaping employee cognition, motivation and social norms around security-relevant behaviour.

7.3 Leadership, Accountability and the Limits of Awareness Training

While security awareness training remains among the most widely deployed governance interventions, evidence on its standalone effectiveness is mixed, and several reviewed studies caution that training programmes divorced from broader structural and leadership commitment produce limited and often transient behavioural change. This reinforces an argument that runs throughout the governance literature reviewed in Section 4: formal interventions — whether disclosure requirements, board committees or training programmes — achieve their intended protective effect only when embedded within a coherent governance architecture that aligns leadership commitment, resource allocation and cultural reinforcement. The persistent gap between adopting cultural interventions and demonstrating improved security outcomes suggests that culture, like resilience assessment more broadly, needs more rigorous longitudinal and outcome-based evaluation than the field has thus far produced.

8. Supply Chain and Sector-Specific Governance Challenges

8.1 The Extension of Governance beyond Organizational Boundaries

As organizations have become increasingly dependent on networks of suppliers, service providers and technology partners, cybersecurity governance has been forced to extend beyond the boundaries of the individual firm to encompass third-party and supply-chain cyber risk. Research on cyber risk management strategies in supply-chain contexts finds that the choices organizations make about cyber risk strategy directly shape the degree of cybersecurity integration achieved with external partners, and that this integration is a significant predictor of the resilience and robustness of the broader supply chain against cyber disruption (Jazairy et al., 2024). This positions supply-chain governance not as a peripheral extension of internal cybersecurity practice, but as a central determinant of organizational resilience in an interconnected operating environment.

8.2 Governance Challenges in Critical Infrastructure

Critical infrastructure sectors, including energy, water and transport, present particularly acute governance challenges owing to the systemic consequences of disruption and the frequent coexistence of legacy operational technology with modern information technology systems. Research assessing cyber-resilience risk in critical infrastructure contexts emphasises the need for governance frameworks that explicitly incorporate methods, governance mechanisms and standards adapted to the distinctive operational constraints of infrastructure environments, where safety considerations and continuity of physical service delivery limit the pace at which security upgrades can be implemented (Aghazadeh Ardebili, Lezzi, & Pourmadadkar, 2024). Work on protecting smart electricity grids against cyber threats similarly seeks to classify resilience approaches specifically suited to power-system contexts, underscoring that these sectors face governance requirements meaningfully different from those applicable to conventional enterprise information technology environments (Syrmakesis, Alcaraz, & Hatziargyriou, 2022).

8.3 Partnership and Collaborative Governance Models

A distinctive response to the cross-organizational character of contemporary cyber risk has been the development of partnership-based governance models extending beyond individual firms to collaborative arrangements among peer organizations, industry bodies and, in some cases, governmental agencies. Research proposing a global cybersecurity partnership model argues that counteracting sophisticated cyberattacks increasingly requires coordinated action and information sharing across organizational boundaries, since individual firms often lack visibility into threats that manifest first within partner or competitor networks before propagating more widely (Trim & Lee, 2021). This collaborative governance perspective complements the intra-organizational mechanisms discussed earlier and highlights that effective cybersecurity governance is increasingly a matter of inter-organizational, as well as intra-organizational, design.

Table 3 summarises supply-chain and sector-specific governance considerations identified across the reviewed literature.

Table 3. Supply chain and sector-specific cybersecurity governance considerations

Context	Distinctive governance challenge	Recommended response	Source
Supply chain	Cyber risk propagates through interconnected supplier and customer networks	Integrate cyber risk strategy with supply-chain integration decisions	Jazairy et al. (2024)
Critical infrastructure	Legacy operational technology coexists with modern digital systems	Adopt infrastructure-adapted governance and standards	Aghazadeh Ardebili et al. (2024)
Energy and smart grids	High systemic consequence of disruption to power delivery	Classify and tailor resilience approaches to grid architecture	Syrmakesis et al. (2022)
Construction	Fragmented, project-based, multi-contractor structures	Coordinate governance across shifting contractor networks	Turk et al. (2022)
Manufacturing	Operational technology–information technology convergence	Adapt enterprise frameworks to industrial control contexts	Alqudhaibi et al. (2023)
Cross-industry partnerships	Limited visibility into threats emerging outside own network	Establish collaborative, partnership-based governance arrangements	Trim & Lee (2021)

The pattern evident in Table 3 is that sector context materially shapes both the nature of cyber risk exposure and the governance instruments capable of addressing it, so generic, one-size-fits-all governance templates are unlikely to work across the full diversity of organizational operating environments.

9. Financial and Insurance Mechanisms in Cyber Risk Governance

9.1 Cyber Insurance as a Governance Instrument

Cyber insurance has emerged as a significant, though still maturing, mechanism through which organizations transfer residual cyber risk that cannot be eliminated through technical or procedural controls alone. A comprehensive review of the cyber insurance literature characterises the field as fragmented, pointing to persistent barriers including underwriting complexity, scarce reliable historical loss data, and the correlated or systemic nature of cyber losses, which complicate actuarial pricing in ways that distinguish cyber insurance from more established lines of coverage (Tsohou, Diamantopoulou, Gritzalis, & Lambrinoudakis, 2023). Despite these challenges, the review finds that cyber insurance increasingly functions as a risk governance and management instrument in its own right, rather than purely as a financial product, since insurers frequently impose minimum security requirements as a condition of coverage — exerting an indirect but material influence on organizational security practice (Tsohou et al., 2023).

9.2 Interaction between Insurance and Internal Governance

The relationship between cyber insurance uptake and internal governance quality has attracted growing scholarly attention. Organizations with more mature internal risk management and governance structures tend to secure more favourable insurance terms, reflecting insurer assessment of the underlying risk profile, while the underwriting process itself can act as an external forcing mechanism that prompts organizations to formalise governance practices they might not otherwise have prioritised. This bidirectional relationship suggests cyber insurance markets and internal cybersecurity governance are mutually reinforcing rather than substitutable mechanisms, with insurance functioning most effectively as a complement to, not a replacement for, robust internal governance.

9.3 Limitations of Insurance as a Resilience Mechanism

Notwithstanding its growing role, cyber insurance carries important limitations as a governance tool. Financial risk transfer does not itself restore operational capability following an incident, nor does it address reputational or regulatory consequences that may persist independently of financial indemnification. The systemic, correlated character of certain categories of cyber loss — such as those arising from widely exploited software vulnerabilities affecting many policyholders simultaneously — also raises concerns about the capacity of insurance markets to absorb catastrophic, correlated events, echoing debates in other catastrophe-exposed insurance lines (Tsohou et al., 2023). These limitations reinforce an argument running throughout this review: financial and reporting mechanisms, while valuable, are complements to substantive resilience-building investment, not substitutes for it.

10. Regulatory and Standards Landscape

10.1 Evolving Regulatory Architecture

The regulatory environment governing organizational cybersecurity has expanded substantially, encompassing sector-specific requirements, general disclosure obligations and cross-border harmonisation efforts. Within the European Union, network and information security legislation has progressively broadened the scope of covered entities and strengthened incident-reporting and governance-accountability obligations, reflecting a policy judgement that market incentives alone are insufficient to secure adequate levels of organizational cyber resilience across critical and essential sectors. In the United States, mandatory cybersecurity incident and governance disclosure introduced by securities regulators has similarly signalled a shift toward treating cybersecurity as a matter of investor-relevant material risk, rather than a purely internal operational concern (Elsayed et al., 2024).

10.2 Voluntary Standards and Frameworks

Alongside binding regulation, voluntary standards and frameworks continue to shape organizational governance practice. The most widely referenced of these organises cybersecurity outcomes into functional categories

addressing governance, identification, protection, detection, response and recovery, with recent revisions elevating governance to an explicit, cross-cutting function that informs the prioritisation and resourcing of the remaining operational categories. This structural elevation of governance within voluntary frameworks reflects the same conceptual shift documented throughout the academic literature reviewed above: cybersecurity effectiveness is understood increasingly to depend on the quality of organizational decision-making structures, not on technical controls in isolation. International information security management standards, applied widely across both public and private sector organizations, similarly emphasise governance, risk assessment and continuous improvement as foundational requirements; however, research into information security governance more broadly cautions that adherence to a recognised governance standard does not by itself guarantee effective outcomes, since implementation quality varies considerably depending on how deeply governance principles are embedded in day-to-day organizational decision-making rather than treated as a documentation exercise (Schinagl & Shahim, 2020).

10.3 Tensions between Regulatory Compliance and Genuine Resilience

A recurring critique in the reviewed literature is that regulatory and standards-based compliance, while valuable in establishing minimum governance baselines, can create incentives for organizations to prioritise the demonstrable satisfaction of audit and disclosure requirements over the less visible, harder-to-measure work of building genuine adaptive capacity. This echoes the institutional-theory account in Section 3, whereby compliance activity may serve a legitimating function only loosely coupled to underlying risk reduction. Addressing this tension does not mean abandoning regulatory compliance, which remains an important governance floor; it means organizations and regulators alike need outcome-oriented measures capable of distinguishing genuine resilience improvement from compliance-oriented box-ticking — a challenge taken up directly in the next section.

Table 4 summarises the principal regulatory and standards instruments identified in the reviewed literature and their governance implications.

Table 4. Regulatory and standards instruments shaping cybersecurity governance

Instrument type	Jurisdiction or scope	Governance implication	Source
Securities disclosure rules	United States	Mandates board oversight and incident disclosure to investors	Elsayed et al. (2024)
Network and information security legislation	European Union	Expands covered entities and strengthens accountability obligations	Kuzior et al. (2024)
Voluntary cybersecurity framework (governance function)	Cross-jurisdictional, voluntary	Elevates governance as a cross-cutting, prioritising function	Schinagl & Shahim (2020)
Information security management standards	Public and private sector, international	Establishes governance, risk assessment and continuous improvement baseline	Aghazadeh Ardebili et al. (2024)
Sector-specific critical infrastructure standards	Energy, grid and infrastructure sectors	Adapts governance requirements to operational technology constraints	Syrmakesis et al. (2022)

11. Measuring Governance Maturity and Resilience Outcomes

11.1 The Challenge of Outcome Measurement

A persistent limitation running through the literature reviewed in this article is the absence of standardised, validated metrics for assessing cybersecurity governance maturity and resilience outcomes. Financial risk management benefits from decades of established metrics, such as value-at-risk and loss-given-default; comparable metrics for cyber risk remain contested and inconsistently applied across organizations and studies. A systematic review of cyber-resilience assessment frameworks finds substantial heterogeneity in the dimensions measured, the data sources used and the underlying conceptual models adopted, concluding that this

fragmentation significantly impedes cross-organizational benchmarking and longitudinal tracking of resilience improvement (Sepúlveda Estay et al., 2020).

11.2 Readiness and Maturity Assessment Approaches

Empirical work on organizational cybersecurity readiness in technology-intensive sectors has attempted to combine quantitative and qualitative assessment, finding that readiness is shaped by a combination of technical infrastructure maturity, governance formalisation and staff competence, and arguing that assessment instruments relying solely on technical indicators risk an incomplete picture of organizational preparedness (Neri, Niccolini, & Martino, 2024). This supports the broader argument running through this review: resilience and governance maturity are multidimensional constructs that require assessment instruments capable of capturing structural, cultural and technical dimensions simultaneously, rather than instruments confined to a single dimension.

11.3 Toward Outcome-Based Governance Metrics

The literature increasingly calls for a shift away from input-based or activity-based metrics — the number of training sessions delivered, the number of policies published — toward outcome-based metrics capable of demonstrating actual improvement in resilience, such as reduced mean time to detect and contain incidents, or measurable improvement in the continuity of critical business functions during simulated or actual disruption. This shift mirrors developments in enterprise risk management more broadly, where organizations have progressively moved from compliance-checklist approaches toward risk-adjusted performance metrics, and reflects a maturing recognition that the ultimate purpose of cybersecurity governance is not the accumulation of documented controls, but the demonstrable capacity of the organization to sustain its mission under adverse conditions.

Table 5 summarises maturity and outcome measurement approaches identified across the reviewed literature.

Table 5. Approaches to measuring cybersecurity governance maturity and resilience outcomes

Measurement approach	Focus	Principal limitation	Source
Cyber-resilience assessment frameworks (systematic review)	Cross-sector resilience capability	Substantial heterogeneity across instruments impedes benchmarking	Sepúlveda Estay et al. (2020)
Quanti-qualitative readiness assessment	Technical, governance and staff competence dimensions	Requires triangulation across data types, raising assessment cost	Neri et al. (2024)
Assurance-based dynamic capability assessment	Organizational capacity to detect and respond to emerging threats	Departs from familiar point-in-time compliance audit norms	Caron (2021)
Intellectual capital indicators	Human and relational capital in crisis response	Indicators are indirect proxies for resilience outcomes	Garcia-Perez et al. (2023)
Cybersecurity culture evaluation	Awareness, training and leadership support indicators	Few frameworks validated in real-world longitudinal settings	Uchendu et al. (2021)

12. Future Directions

Future research would benefit from longitudinal studies able to trace how governance interventions — disclosure regulation, board composition change, cultural investment — translate over time into measurable improvements in resilience outcomes, rather than relying on cross-sectional snapshots of governance structure alone. Greater methodological convergence around a smaller number of validated, outcome-based resilience metrics would substantially improve comparability across studies and sectors, enabling more robust meta-analytic synthesis than the currently fragmented assessment landscape permits. Further attention should go to the governance of artificial intelligence systems embedded within organizational cybersecurity operations, an area of rapidly growing practical relevance that remains comparatively underexplored in the governance literature reviewed here. Research on small and medium-sized enterprises also warrants expansion, since much of the existing evidence base skews toward large, resource-rich organizations, leaving open questions about how

transferable governance and resilience frameworks are to smaller entities operating under tighter resource constraints. Finally, comparative cross-jurisdictional research on how differing regulatory architectures shape organizational governance behaviour would help clarify which regulatory design features most effectively narrow the gap between formal compliance and substantive resilience identified throughout this review.

13. Conclusions

This review has traced the evolution of organizational cybersecurity governance from an initially narrow, compliance-oriented focus on risk reporting toward a broader, more theoretically grounded concern with organizational cyber resilience. The evidence synthesised across governance structures, enterprise risk management integration, resilience frameworks, cultural determinants, supply-chain dependencies, financial risk-transfer mechanisms, regulatory architecture and measurement practice converges on a consistent conclusion: formal governance mechanisms, including board oversight structures, disclosure regulation and voluntary standards, have expanded considerably over the past decade, yet the substantive capability improvements these mechanisms are meant to produce remain uneven and difficult to verify. Genuine progress from risk reporting toward resilience appears to depend less on the proliferation of governance artefacts and more on the depth of board expertise, the coherence of enterprise risk integration, the strength of organizational culture, and the sophistication of outcome-based measurement. Organizations seeking to move credibly along this trajectory would do well to treat disclosure and compliance as a governance floor rather than a governance ceiling, and to invest correspondingly in the human, cultural and cross-organizational capabilities that the evidence reviewed here identifies as the more decisive determinants of resilience.

14. Limitations

This review is subject to several limitations. As a narrative rather than systematic review, the selection and synthesis of literature, while guided by explicit inclusion and exclusion criteria, retains an element of author judgement that may introduce selection bias relative to a fully protocol-driven systematic methodology. The review is confined to English-language, peer-reviewed academic sources, which may exclude relevant practitioner or non-English scholarship, particularly given the substantial regulatory and governance activity occurring in non-Anglophone jurisdictions. The rapid pace of change in cybersecurity regulation and practice means some empirical findings, particularly those concerning specific disclosure regimes, may become superseded relatively quickly following publication. Finally, the cross-disciplinary scope of the review, while a deliberate strength intended to integrate accounting, management and information systems perspectives, necessarily limits how deeply any single disciplinary literature could be examined relative to a narrower, single-discipline review.

Declaration of AI Use

This manuscript was prepared through the combined contributions of all author(s), including contributions to the study design, data, content development, results, interpretation, and related scholarly work. The author(s) acknowledge the use of Grammarly and ChatGPT to assist with grammar checking, language refinement, reference formatting. These AI-assisted tools were not used as authors and did not replace the intellectual contributions or scholarly judgment of the author(s). All AI-assisted outputs, including content, references, and interpretations, were carefully reviewed, revised, verified, and approved by the author(s). The author(s) accept full responsibility for the accuracy, integrity, and final content of the manuscript.

Competing Interests

Authors have declared that no competing interests exist.

References

Aghazadeh Ardebili, A., Lezzi, M., & Pourmadadkar, M. (2024). Risk assessment for cyber resilience of critical infrastructures: Methods, governance, and standards. *Applied Sciences, 14*(24), Article 11807. https://doi.org/10.3390/app142411807

Alqudhaibi, A., Deshpande, S., Jagtap, S., & Salonitis, K. (2023). Towards a sustainable future: Developing a cybersecurity framework for manufacturing. *Technological Sustainability, 2*(4), 372–387. https://doi.org/10.1108/TECHS-05-2023-0022

Calderon, T. G., & Gao, L. (2022). Comparing the cybersecurity risk disclosures of U.S. and foreign firms. *Journal of Emerging Technologies in Accounting, 19*(2), 61–79. https://doi.org/10.2308/JETA-2020-008

Caluwe, L., Wilkin, C. L., De Haes, S., & Huygh, T. (2024). Board roles required for IT governance to become an integral component of corporate governance. *International Journal of Accounting Information Systems, 54*, Article 100694. https://doi.org/10.1016/j.accinf.2024.100694

Caron, F. (2021). Obtaining reasonable assurance on cyber resilience. *Managerial Auditing Journal, 36*(2), 193–217. https://doi.org/10.1108/MAJ-11-2017-1690

Dalal, R. S., Howard, D. J., Bennett, R. J., Posey, C., Zaccaro, S. J., & Brummel, B. J. (2022). Organizational science and cybersecurity: Abundant opportunities for research at the interface. *Journal of Business and Psychology, 37*(1), 1–29. https://doi.org/10.1007/s10869-021-09732-9

Dunn Cavelty, M., Eriksen, C., & Scharte, B. (2023). Making cyber security more resilient: Adding social considerations to technological fixes. *Journal of Risk Research, 26*(7), 801–814. https://doi.org/10.1080/13669877.2023.2208146

Dupont, B. (2019). The cyber-resilience of financial institutions: Significance and applicability. *Journal of Cybersecurity, 5*(1), Article tyz013. https://doi.org/10.1093/cybsec/tyz013

Dupont, B., Shearing, C., Bernier, M., & Leukfeldt, R. (2023). The tensions of cyber-resilience: From sensemaking to practice. *Computers & Security, 132*, Article 103372. https://doi.org/10.1016/j.cose.2023.103372

Elsayed, D. H., Ismail, T. H., & Ahmed, E. A. (2024). The impact of cybersecurity disclosure on banks' performance: The moderating role of corporate governance in the MENA region. *Future Business Journal, 10*(1), Article 115. https://doi.org/10.1186/s43093-024-00402-9

Ferrari, R. (2015). Writing narrative style literature reviews. *Medical Writing, 24*(4), 230–235. https://doi.org/10.1179/2047480615Z.000000000329

Gao, L., & Calderon, T. G. (2025). Cybersecurity risk governance and companies' cybersecurity risk disclosures in their 10-K filings. *Journal of Accounting and Public Policy, 54*, Article 107376. https://doi.org/10.1016/j.jaccpubpol.2025.107376

Garcia-Perez, A., Cegarra-Navarro, J. G., Sallos, M. P., Martinez-Caro, E., & Chinnaswamy, A. (2023). Resilience in healthcare systems: Cyber security and digital transformation. *Technovation, 121*, Article 102583. https://doi.org/10.1016/j.technovation.2022.102583

Garcia-Perez, A., Sallos, M. P., & Tiwasing, P. (2023). Dimensions of cybersecurity performance and crisis response in critical infrastructure organisations: An intellectual capital perspective. *Journal of Intellectual Capital, 24*(2), 465–486. https://doi.org/10.1108/JIC-06-2021-0166

Jazairy, A., Brho, M., Manuj, I., & Goldsby, T. J. (2024). Cyber risk management strategies and integration: Toward supply chain cyber resilience and robustness. *International Journal of Physical Distribution & Logistics Management, 54*(11), 1–29. https://doi.org/10.1108/IJPDLM-12-2023-0445

Khan, H., Ozkan, K. S. L., Deligonul, S., & Cavusgil, E. (2024). Redefining the organizational resilience construct using a frame-based methodology: A new perspective from the ecology-based approach. *Journal of Business Research, 172*, Article 114397. https://doi.org/10.1016/j.jbusres.2023.114397

Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. *Journal of International Studies, 17*(2), 220–239. https://doi.org/10.14254/2071-8330.2024/17-2/12

Lowry, M. R., Vance, A., & Vance, M. D. (2026). Inexpert supervision: Field evidence on boards' oversight of cybersecurity. *Management Science, 72*(2), 783–804. https://doi.org/10.1287/mnsc.2023.04147

Neri, M., Niccolini, F., & Martino, L. (2024). Organizational cybersecurity readiness in the ICT sector: A quanti-qualitative assessment. *Information & Computer Security, 32*(1), 38–52. https://doi.org/10.1108/ICS-05-2023-0084

Neri, M., Niccolini, F., & Virili, F. (2026). Organizational cyber resilience: Toward an integrative conceptual framework. *Management Review Quarterly, 76*(1), 789–840. https://doi.org/10.1007/s11301-025-00496-7

Romanosky, S., & Petrun Sayers, E. L. (2024). Enterprise risk management: How do firms integrate cyber risk? *Management Research Review, 47*(1), 1–17. https://doi.org/10.1108/MRR-10-2021-0774

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors, 23*(16), Article 7273. https://doi.org/10.3390/s23167273

Schinagl, S., & Shahim, A. (2020). What do we know about information security governance? "From the basement to the boardroom": Towards digital security governance. *Information & Computer Security, 28*(2), 261–292. https://doi.org/10.1108/ICS-02-2019-0033

Sepúlveda Estay, D. A., 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

Slapničar, S., Axelsen, M., Bongiovanni, I., & Stockdale, D. (2023). A pathway model to five lines of accountability in cybersecurity governance. *International Journal of Accounting Information Systems, 51*, Article 100642. https://doi.org/10.1016/j.accinf.2023.100642

Syrmakesis, A. D., Alcaraz, C., & Hatziargyriou, N. D. (2022). Classifying resilience approaches for protecting smart grids against cyber threats. *International Journal of Information Security, 21*(5), 1189–1210. https://doi.org/10.1007/s10207-022-00594-7

Trim, P. R. J., & Lee, Y.-I. (2021). The global cyber security model: Counteracting cyber attacks through a resilient partnership arrangement. *Big Data and Cognitive Computing, 5*(3), Article 32. https://doi.org/10.3390/bdcc5030032

Tsen, E., Ko, R. K. L., & Slapničar, S. (2022). An exploratory study of organizational cyber resilience, its precursors and outcomes. *Journal of Organizational Computing and Electronic Commerce, 32*(2), 153–174. https://doi.org/10.1080/10919392.2022.2068906

Tsohou, A., Diamantopoulou, V., Gritzalis, S., & Lambrinoudakis, C. (2023). Cyber insurance: State of the art, trends and future directions. *International Journal of Information Security, 22*(3), 737–748. https://doi.org/10.1007/s10207-023-00660-8

Turk, Ž., García de Soto, B., Mantha, B. R. K., Maciel, A., & Georgescu, A. (2022). A systemic framework for addressing cybersecurity in construction. *Automation in Construction, 133*, Article 103988. https://doi.org/10.1016/j.autcon.2021.103988

Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: A historical and conceptual review. *International Journal of Information Security, 23*(3), 1695–1719. https://doi.org/10.1007/s10207-023-00811-x

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security, 109*, Article 102387. https://doi.org/10.1016/j.cose.2021.102387

Peer-review history:
The peer review history for this paper can be accessed here:
https://prh.ikprress.org/review-history/15330