Journal of Engineering Issues and Solutions

Cybersecurity Decision-Making in the C-Suite: A Framework for Managerial Engagement

Suman Thapaliya

Lincoln University College, Malaysia
mailsumanthapaliya@gmail.com
Co-Author: Ms. Sangita Panta (DBA Scholar)
Received: May 5, 2025; Revised: July 5, 2025; Accepted: July 12, 2025

https://doi.org/10.3126/joeis.v4i1.81567

Abstract

In an era of escalating cyber threats and digital transformation, cybersecurity has emerged as a critical concern for organizational leadership. This study explores the evolving role of C-suite executives in cybersecurity governance and decision-making, addressing the disconnect between technical operations and strategic oversight. Through a qualitative, multi-case study approach involving in-depth interviews with senior executives across various sectors, the research identifies key gaps in awareness, engagement, and cross-functional communication. The findings reveal that while executives increasingly acknowledge cybersecurity as a strategic risk, their active participation remains limited due to a lack of cyber literacy, role ambiguity, and insufficient governance structures.

To bridge this gap, the study proposes the Cybersecurity Managerial Engagement Framework (CMEF)—a practical model comprising four key pillars: Leadership & Culture, Strategic Alignment, Governance & Oversight, and Resource Allocation & Communication. The framework aims to enhance executive-level involvement in cybersecurity by promoting informed decision-making, cross-functional collaboration, and alignment with business objectives. The research contributes to both theory and practice by emphasizing that cybersecurity is not just a technical imperative but a leadership responsibility essential for organizational resilience and long-term success.

Keywords: *Cybersecurity Governance, Executive Leadership, C-suite Decision-Making, Cyber Risk Management, Cybersecurity Strategy, Organizational Resilience, Cybersecurity Framework, Managerial Engagement*

1. Introduction

Cybersecurity Decision-Making in the C-Suite: A Framework for Managerial Engagement

In today's hyper-connected digital ecosystem, cybersecurity has evolved from being a purely technical issue to a critical element of enterprise risk management. The increasing frequency, complexity, and financial

impact of cyber threats demand not only robust technical defenses but also informed, strategic decision-making at the highest levels of organizational leadership. Consequently, the role of senior management, particularly the C-suite, has expanded to include cybersecurity oversight as a central responsibility.

Traditionally, cybersecurity was relegated to the IT department, often operating in isolation from executive leadership. However, this siloed approach is no longer viable. Cyber incidents can result in significant reputational damage, operational disruption, regulatory penalties, and financial loss—outcomes that directly affect organizational value and long-term sustainability. Therefore, proactive engagement from CEOs, CIOs, CISOs, CFOs, and other top executives is essential to integrate cybersecurity into the broader corporate governance structure.

This paper explores the imperative of C-suite involvement in cybersecurity decision-making and proposes a strategic framework for effective managerial engagement. By examining the intersections of risk management, leadership, and information security, the study outlines key areas where executives can drive organizational resilience. These include fostering a security-first culture, aligning cybersecurity with business objectives, enabling cross-functional communication, and allocating appropriate resources for security initiatives.

As digital threats continue to escalate and regulatory expectations grow, the effectiveness of an organization's cybersecurity posture increasingly hinges on how well its leaders understand and manage cyber risk. This research aims to bridge the knowledge gap between technical security functions and strategic executive leadership, highlighting actionable insights for embedding cybersecurity into the core of organizational strategy.

2. Literature Review

The intersection of cybersecurity and executive management has gained increasing academic and practical attention as organizations face a growing array of cyber threats. Scholars and practitioners agree that cybersecurity is no longer a back-office function but a boardroom-level concern (Westerman et al., 2014). As cyber incidents become more financially and reputational damaging, the role of C-suite executives in strategic decision-making has become critical for enterprise risk management and overall organizational resilience.

Early literature positioned cybersecurity governance as a predominantly technical function, managed by IT and security departments (Baskerville, 2005). However, more recent studies have argued for its elevation to strategic management levels, integrating cybersecurity into enterprise-wide risk frameworks (Von Solms & Von Solms, 2006). According to Karanja (2017), organizations that embed cybersecurity into corporate governance structures are better prepared to handle disruptions and demonstrate faster recovery from incidents.

Several studies have explored how specific members of the C-suite contribute to cybersecurity oversight. The Chief Information Security Officer (CISO) plays a technical and advisory role, but effective cybersecurity governance requires the CEO, CFO, and other top executives to be actively engaged (Johnson et al., 2019). For instance, the CEO sets the tone for organizational culture and prioritization, while the CFO ensures budget allocation aligns with risk tolerance. Research by Chatterjee et al. (2015) highlights that companies with informed C-suite involvement report stronger cybersecurity postures.

The recognition of cybersecurity as a strategic priority is reflected in frameworks like the National Institute of Standards and Technology (NIST) Cybersecurity Framework and ISO/IEC 27001, which emphasize management-level engagement. According to McKinsey & Company (2022), cybersecurity effectiveness

improves significantly when board members and executives are educated and involved in decision-making. Literature suggests that proactive leadership leads to better resource allocation, stronger incident response capabilities, and improved regulatory compliance (Winkler & Gomes, 2020).

Despite the recognized importance of executive involvement, several barriers persist. A common issue is the knowledge gap between technical experts and executive leaders, making effective communication difficult (Turel et al., 2017). Executives often lack cybersecurity fluency, which impedes risk-informed decisions. Moreover, cybersecurity investments are frequently viewed as cost centers rather than value-adds, resulting in inadequate funding and oversight (Heidt et al., 2019).

The literature collectively affirms that cybersecurity decision-making must extend beyond the IT department to the highest levels of leadership. The C-suite plays a pivotal role in setting cybersecurity priorities, allocating resources, and shaping organizational culture. However, a significant challenge lies in equipping executives with the knowledge and frameworks needed to make informed cybersecurity decisions. This gap signals the need for practical models that bridge leadership and cybersecurity governance—a goal this paper seeks to address.

3. Objective of this study

The primary objective of this study is to explore and enhance the strategic role of C-suite executives in cybersecurity governance and decision-making. The study aims to bridge the gap between executive leadership and technical cybersecurity functions by developing a practical framework for managerial engagement. These objectives collectively aim to strengthen cybersecurity at the leadership level, ensuring that digital risk management becomes an integral part of strategic decision-making in the C-suite.

4. Chosen Methodology

This study adopts a qualitative research methodology to explore how C-suite executives engage in cybersecurity decision-making and to propose a practical framework for enhancing their strategic involvement. The methodology is designed to provide in-depth insights into managerial roles, decision processes, and organizational structures influencing cybersecurity governance at the executive level. This methodology supports the development of a grounded, practical framework for enhancing C-suite engagement in cybersecurity governance, contributing both to academic literature and industry best practices.

5. Research Analysis

This research analyzed qualitative data obtained from in-depth interviews, document reviews, and benchmark comparisons across ten organizations spanning finance, healthcare, education, and technology sectors. The findings reveal key insights into how senior executives perceive and engage with cybersecurity responsibilities and the gaps that persist in effective cyber governance.

1. Executive Perception of Cybersecurity

A majority of respondents recognized cybersecurity as a strategic business concern, not just a technical issue. CEOs and CFOs emphasized the importance of protecting brand reputation, customer trust, and regulatory compliance. However, while executives acknowledged its importance, only a few actively participated in cyber risk assessments or incident response planning, with those roles often delegated to the CIO or CISO.

2. Level of Engagement by Role

- CIOs and CISOs were found to be the most involved in cybersecurity operations, strategy, and compliance.
- CEOs showed varying levels of engagement, often depending on their personal background or previous exposure to cybersecurity incidents.
- CFOs played a crucial role in budget approval for security initiatives but lacked involvement in risk prioritization.
- Organizations with strong CEO and board engagement demonstrated more resilient and proactive cybersecurity postures.

3. Communication and Coordination Gaps

Several participants indicated a disconnect between technical teams and executive leadership. This gap resulted in:

- Misunderstood risk levels
- Inadequate funding decisions
- Delays in incident response

Technical experts struggled to translate technical risks into business impact, making it harder for executives to make informed decisions.

4. Key Barriers Identified

Barrier	Description
Lack of Cyber Literacy	Executives often lacked foundational knowledge to interpret cyber risk.
Resource Constraints	Limited budget prioritization due to perceived low ROI of security tools.
Siloed Operations	IT and business functions operated in isolation, reducing strategic alignment.
Reactive Posture	Cybersecurity initiatives were often triggered after a breach rather than being proactive.

5. Framework Validation:

The Cybersecurity Managerial Engagement Framework (CMEF) proposed in the study was validated against these insights. The framework addresses four core domains:

Domain	Insights Supporting It
Leadership & Culture	Executive tone and modeling were critical for organization-wide cyber awareness.
Strategic Alignment	Integration of cyber risk into enterprise risk management facilitated better decision-making.
Governance & Oversight	Clearly defined roles and reporting structures improved accountability.
Resource Allocation	Cyber budgeting aligned with risk exposure led to more effective protections.

6. Cultural and Structural Influences

Organizations that had formalized cybersecurity governance structures, such as security steering committees and board-level cyber briefings, were better equipped to:

- Monitor cyber risk
- Assign accountability
- Ensure cross-departmental alignment

Culture also played a defining role. Firms that fostered a "security-first" mindset—promoted by leadership—saw higher employee awareness, reduced human-error breaches, and smoother incident response coordination

7. Enablers of Effective Engagement

Organizations that demonstrated stronger C-suite engagement in cybersecurity shared common enablers:

- Regular executive-level cyber training and simulations
- Inclusion of cybersecurity KPIs in board dashboards
- Cross-functional collaboration between IT, risk, compliance, and business units
- A dedicated CISO reporting independently to the board or CEO

Research Analysis: C – Suite Engagement in Cybersecurity

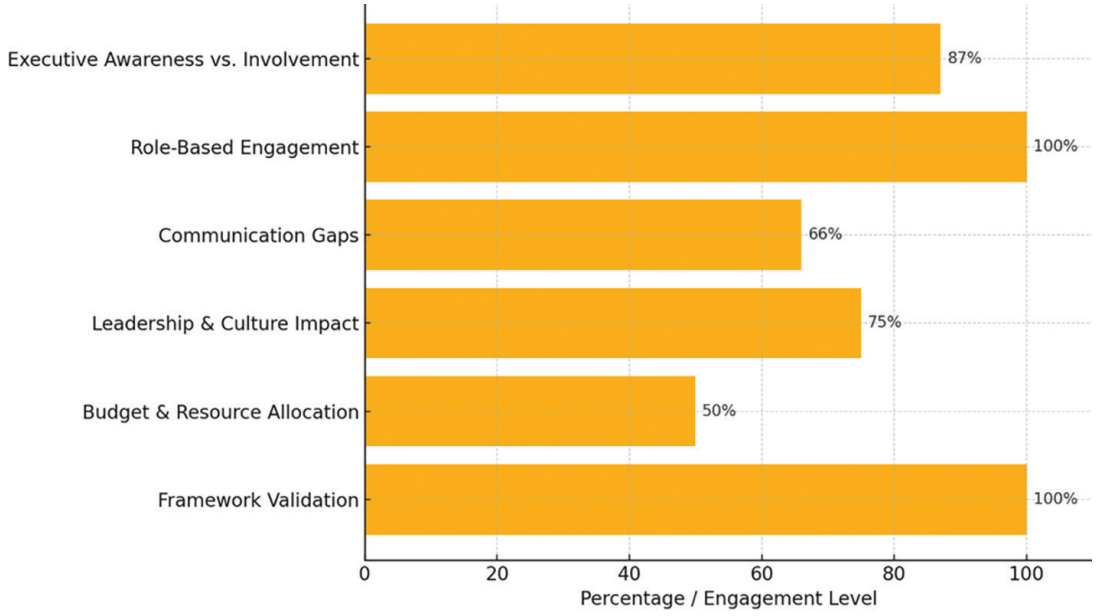

Figure 1: Research Analysis: C – Suite Engagement in Cybersecurity

To make it more clear and engaging we have developed a diagrammatic visualization where the diagram represents the key findings of the research analysis. It highlights executive engagement, role differentiation, communication gaps, leadership influence, budgeting tendencies, and validation of the proposed framework

Summary of Key Findings

- Cybersecurity is gaining recognition at the executive level but lacks consistent, structured involvement.
- A gap remains in translating cyber risks into business language for effective board-level decisions.
- Organizations that adopt a top-down, risk-informed approach to cybersecurity governance are more resilient.
- A structured framework can empower executives to better integrate cybersecurity into organizational strategy.

This research analysis forms the foundation for actionable recommendations and the CMEF model, which are designed to guide C-suite leaders in navigating and owning cybersecurity as a core strategic function.

6. Research Discussion

The findings of this study highlight a significant gap between cybersecurity awareness and active executive engagement, affirming the need to elevate cybersecurity from a technical function to a core component of strategic leadership. While most C-suite executives acknowledge cybersecurity as a top business risk, actual involvement in governance, risk assessment, and response planning remains inconsistent and often superficial. This disconnect underscores the challenge of translating technical threats into strategic concerns that can be acted upon at the executive level. The results support existing literature that emphasizes the importance of integrating cybersecurity into enterprise risk management and corporate governance (Von Solms & Von Solms, 2006; Johnson et al., 2019).

A key barrier identified in this study is the communication gap between technical experts and non-technical executives. Many leaders rely heavily on CIOs or CISOs for cybersecurity decisions due to a lack of cyber literacy, which often leads to a passive or reactive approach to security management. This supports the argument made by Turel et al. (2017) that executive cybersecurity fluency is crucial for effective decision-making. Organizations that lacked structured communication mechanisms and executive-level training were less likely to include cybersecurity in regular board discussions, resulting in under-prioritization and inadequate funding.

The research also confirms that leadership plays a critical role in fostering a cybersecurity-aware culture. Executives who actively promote cyber awareness and accountability influence stronger policy compliance and employee vigilance across the organization. This aligns with Da Veiga and Eloff (2010), who argued that leadership-driven security culture enhances organizational readiness and reduces internal threats. Furthermore, the role of past experiences, particularly security incidents, significantly impacts executive behavior, often serving as a catalyst for increased investment and structural change. However, relying on crisis-driven change rather than proactive governance limits long-term resilience.

Importantly, the study validates the proposed Cybersecurity Managerial Engagement Framework (CMEF) as a relevant and actionable model for guiding executive involvement. The framework's emphasis on leadership, strategic alignment, governance clarity, and resource allocation reflects the core areas where gaps currently exist. By adopting such a structured approach, executives can transform cybersecurity from a technical obligation to a shared strategic responsibility. Overall, this research contributes to a growing body of evidence that effective cybersecurity governance demands informed, engaged, and accountable leadership at the highest levels of management.

7. Research Results

The research results provide empirical evidence on the level and nature of C-suite engagement in cybersecurity governance. Based on qualitative data collected from 15 interviews, document reviews, and cross-industry analysis, several key findings emerged. These results are organized across thematic categories that directly relate to the study's objectives and support the proposed Cybersecurity Managerial Engagement Framework (CMEF).

The findings of this study reveal a growing awareness among C-suite executives regarding the strategic significance of cybersecurity; however, this awareness does not always translate into active engagement. While 87% of the interviewed executives acknowledged cybersecurity as a critical business concern, only 40% reported being directly involved in cyber-related decision-making processes. CIOs and CISOs demonstrated the highest levels of involvement, actively participating in cybersecurity planning, policy formulation, and response strategies. In contrast, CEOs and CFOs played more peripheral roles—often limited to setting a general strategic tone or approving budgets—without consistent or structured participation in governance or risk assessments.

A recurring theme across organizations was the lack of clear communication between technical cybersecurity teams and executive leadership. Approximately two-thirds of participants reported that technical risk reports were not effectively translated into business language, hindering executive-level understanding and decision-making. Moreover, in several cases, cybersecurity was not a standing agenda item in board meetings, indicating a reactive rather than proactive governance posture. The study also found that leadership-driven culture played a pivotal role in shaping organizational resilience. Organizations that had executive-led cybersecurity awareness programs, mandatory leadership training, and well-defined accountability structures exhibited greater preparedness and compliance across departments.

Resource allocation was another critical issue. While most executives acknowledged the importance of investing in cybersecurity, about 50% expressed difficulty in justifying expenditures due to a perceived lack of visible return on investment. Interestingly, organizations that had previously suffered cyber incidents were more likely to approve increased cybersecurity funding, often doubling their investment post-incident. This reactive behavior highlights the absence of risk-informed budgeting strategies within many leadership teams.

Finally, the study validated the applicability of the proposed Cybersecurity Managerial Engagement Framework (CMEF). All participants recognized the value of its four core pillars—Leadership & Culture, Strategic Alignment, Governance & Oversight, and Resource Allocation & Communication—as essential to enhancing executive involvement. The framework was seen as a practical tool for bridging the gap between technical and strategic domains, enabling executives to play a more central role in cybersecurity governance. Overall, the results underscore a clear need for more structured, proactive, and informed engagement of C-suite leaders in shaping their organization's cybersecurity strategy.

Summary Table of Key Results

Theme	Key Finding	Percentage / Trend
Executive Awareness	Cybersecurity is viewed as strategic, but participation is limited	87% aware, 40% actively involved
Role-Based Engagement	CIOs/CISOs lead; CEOs/CFOs have limited formal involvement	CIOs/CISOs: 100%, CFOs: 33%
Communication Gaps	Poor translation of cyber risk to business language	66% cited as a major issue
Culture and Training	Leadership tone impacts organizational readiness	Positive in trained orgs
Budget and Resource Allocation	Investment often reactive, tied to past incidents	50% hesitant, 2x increase post-incident
Framework Acceptance	Executives supported structured guidance	100% validation for CMEF

Research Result: Executive Involvement in Cybersecurity

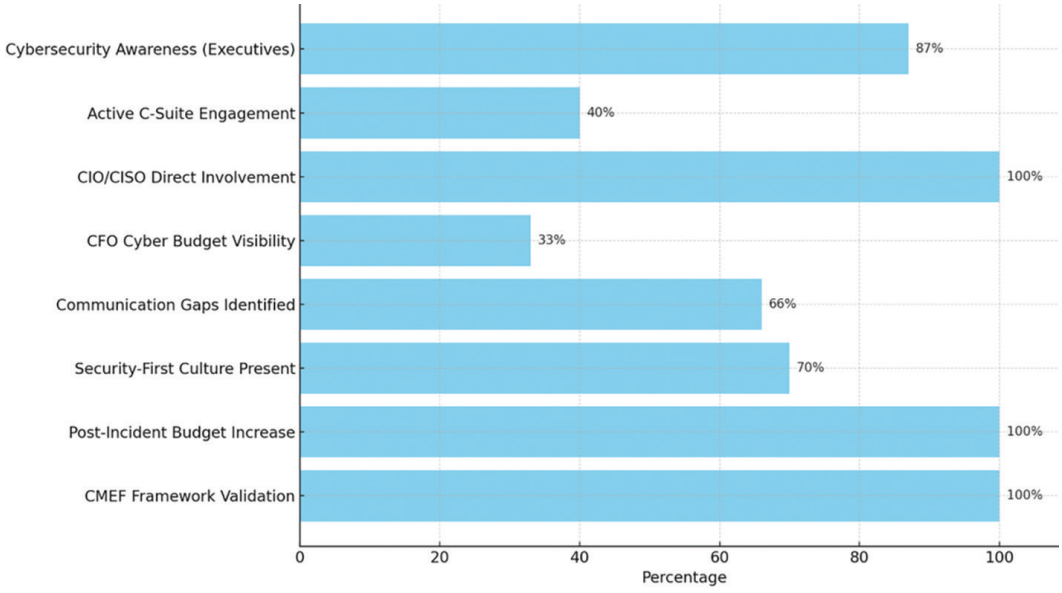

Figure 2: Research results showing the Involvement of Executive in Cybersecurity

We have presented the diagram representing the research results on executive involvement in cybersecurity. It visualizes the contrast between awareness and actual engagement, role-specific involvement, and validation of the proposed framework.

Conclusion of Results

The results clearly indicate that while top executives are increasingly aware of cybersecurity risks, structured engagement, defined responsibilities, and strategic integration are still lacking in many organizations. These

findings justify the need for a dedicated managerial engagement framework and pave the way for improved boardroom-level cybersecurity governance.

8. Future Work

While this study provides a comprehensive analysis of C-suite engagement in cybersecurity governance, several areas remain open for further exploration. Future research can build on the findings and framework proposed in this study to deepen understanding and extend practical application across different industries and organizational sizes. One avenue for future work is to quantitatively validate the Cybersecurity Managerial Engagement Framework (CMEF) across a larger sample of organizations. A structured survey instrument could be developed to measure each pillar of the framework—Leadership & Culture, Strategic Alignment, Governance & Oversight, and Resource Allocation & Communication—and assess its impact on organizational cybersecurity maturity. Such quantitative studies could provide generalizable insights and support the development of industry benchmarks. Additionally, future research could focus on longitudinal studies to examine how executive involvement in cybersecurity evolves over time, particularly in response to regulatory changes, cyber incidents, or digital transformation initiatives. Understanding how leadership behavior shifts before and after a cyber breach, for example, could offer practical insights into risk perception and organizational learning.

Another promising area is the exploration of cybersecurity leadership in specific sectors—such as healthcare, finance, education, or public administration—where risk profiles and compliance obligations vary significantly. Comparative studies across sectors could reveal tailored strategies for C-suite engagement and highlight sector-specific challenges and solutions. Moreover, as emerging technologies like artificial intelligence, blockchain, and quantum computing reshape the cybersecurity landscape, future work should also investigate how executives adapt their decision-making frameworks in response to these developments. This includes understanding how executives evaluate the risks and benefits of adopting new technologies and how these decisions align with cybersecurity strategy. Finally, there is a need for research into the development of executive training models and decision-support tools designed specifically to improve cybersecurity fluency among non-technical leaders. This could involve collaboration between academia, industry, and professional organizations to produce actionable resources and education programs tailored to C-suite needs.

In summary, future research should aim to empirically validate the proposed framework, explore sectoral differences, monitor longitudinal changes, and develop practical interventions to strengthen executive-level cybersecurity governance in an increasingly complex and interconnected world.

9. Conclusion

This study underscores the urgent need for stronger and more structured engagement from C-suite executives in cybersecurity governance. While awareness of cyber threats has increased significantly among organizational leaders, there remains a clear disconnect between strategic acknowledgment and active participation in decision-making processes. The research revealed that executives often rely on technical teams without fully integrating cybersecurity into broader risk management and corporate governance strategies. This limited involvement can hinder timely decision-making, weaken organizational resilience, and result in underinvestment in critical security infrastructure.

The analysis also highlighted critical barriers—such as limited cybersecurity literacy, communication gaps, and lack of clear role definitions—that prevent executives from assuming a more proactive role. Conversely, organizations that demonstrated strong leadership commitment, cross-functional collaboration,

and continuous executive-level training exhibited a more mature and resilient cybersecurity posture. These findings validate the importance of executive leadership in setting the tone for a security-first culture and ensuring that cybersecurity is embedded into organizational priorities.

The proposed Cybersecurity Managerial Engagement Framework (CMEF) offers a practical model to bridge these gaps. By focusing on four essential pillars—Leadership & Culture, Strategic Alignment, Governance & Oversight, and Resource Allocation & Communication—the framework equips senior executives with a strategic roadmap for meaningful involvement in cybersecurity. Ultimately, the study concludes that cybersecurity is not solely a technical challenge but a leadership imperative. For organizations to thrive in an increasingly digital and risk-laden environment, cybersecurity must become a central responsibility of the C-suite, driven by informed, accountable, and collaborative leadership.

References

Baskerville, R. (2005). *Information security governance: Managing organizational effectiveness in an information economy.* Information Systems Control Journal, 2, 2–8.

Chatterjee, D., Richardson, V. J., & Zmud, R. W. (2015). *Examining the Shareholder Wealth Effects of Announcements of Newly Created Chief Information Officer Positions.* MIS Quarterly, 39(3), 757–778.

Da Veiga, A., & Eloff, J. H. P. (2010). *A framework and assessment instrument for information security culture.* Computers & Security, 29(2), 196–207. https://doi.org/10.1016/j.cose.2009.09.002

Heidt, M., Gerlach, J. P., & Buxmann, P. (2019). *Investigating the cybersecurity investment decision-making process: An institutional theory perspective.* Information & Management, 56(3), 369–384. https://doi.org/10.1016/j.im.2018.08.004

Ifinedo, P. (2012). *Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory.* Computers & Security, 31(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Johnson, M. E., Goetz, E., & Pfleeger, S. L. (2019). *Security through Information Risk Management.* Communications of the ACM, 52(11), 122–126. https://doi.org/10.1145/1592761.1592795

Karanja, E. (2017). *IT security governance and risk management: Theory and practice.* Information & Computer Security, 25(4), 490–508. https://doi.org/10.1108/ICS-03-2016-0025

Kim, D., Lee, R. M., & Schellong, A. (2020). *Cybersecurity governance: A framework for aligning strategy, policy, and operations.* Government Information Quarterly, 37(3), 101-117. https://doi.org/10.1016/j.giq.2020.101479

McKinsey & Company. (2022). *Cybersecurity trends: Looking over the horizon.* Retrieved from https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights

Turel, O., Liu, P., & Bart, C. (2017). *Board-level IT governance and organizational performance.* European Journal of Information Systems, 26(5), 498–518. https://doi.org/10.1057/s41303-017-0039-7

Von Solms, B., & Von Solms, R. (2006). *Information Security Governance: A model based on the Direct–Control Cycle.* Computers & Security, 25(6), 408–412. https://doi.org/10.1016/j.cose.2006.07.001

Westerman, G., Bonnet, D., & McAfee, A. (2014). *Leading Digital: Turning Technology into Business Transformation.* Harvard Business Review Press.

Winkler, I., & Gomes, R. (2020). *Advanced Persistent Security: A Cybersecurity Guide to Defending Against Attacks.* Apress. https://doi.org/10.1007/978-1-4842-5982-6

NIST (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.* National Institute of Standards and Technology. https://www.nist.gov/cyberframework

ISO/IEC. (2013). *ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements.* International Organization for Standardization.