Cybersecurity Management Competencies in Critical Infrastructure Organizations: A Review and Research Agenda

Shehu Abubakar and Hanna Paananen
University of Jyväskylä, Finland

Shehu.s.abubakar@jyu.fi
hanna.k.paananen@jyu.fi

Abstract: Critical infrastructure is vital to the economic, social, and technological survival and welfare of nations. Attacks on these infrastructures can be devastating and can lead to serious consequences. The Top Management Team (TMT) is the highest decision-makers who seal the fate of such organizations when it comes to risk management. Regulations and best practices are demanding that the TMT take responsibility for the cybersecurity posture of the critical infrastructure organizations to protect that infrastructure or prevent further damage. Critical infrastructure organizations often have a combination of information technology and operational technology spread across a wider geographical area and extensive regulation that can affect security investments and the TMT composition. Consequently, to effectively carry out their responsibilities, the TMT requires cybersecurity competencies; therefore, the specific cybersecurity management competencies that constitute these requirements need to be identified and tailored to their roles. To identify research in this area, we surveyed prominent journals that publish on cybersecurity, management, and critical infrastructure. We used search terms that address cybersecurity skills, knowledge, and attitudes necessary for top management in strategic decision-making and cybersecurity risk management. To ensure the collection of relevant articles, the literature review follows a systematic review process. A qualitative analysis method was employed to identify five thematic areas, namely leadership, learning, organization, cybersecurity, and competency, through which management's cybersecurity competencies are positioned as strategic requirements that can impact organizational cybersecurity resilience. The strategic responsibilities of the Top Management Team (TMT) are interestingly extending to cybersecurity management in organizations. They are also required to align cybersecurity management with the organization's strategic objectives. Thus, to effectively carry out their responsibilities, the TMT requires cybersecurity competencies. This review has identified relevant cybersecurity skills, knowledge, and attitudes that can be constituted as cybersecurity management competencies that will support TMT in the critical infrastructure protection. The review also reveals research gaps due to the limited number of studies conducted considering the entire TMT cybersecurity management competencies. This review provides a foundation for developing a theoretical framework for studying TMT cybersecurity competencies in critical infrastructure organizations.

Keywords: Cybersecurity, Senior management, Competencies, Critical infrastructure

1. Introduction

Critical infrastructures are consistently faced with an increasing number of attacks. Attacks or disruptions to critical infrastructure can prove disastrous and can negatively affect their reliability and safety (Alcaraz and Zeadally, 2015) with the effect going beyond one national border to another (Lehto, 2022).

These attacks may result in extremely high revenue losses (He et al., 2018), and financial loss is not the only adverse effect can also lead to legal liabilities with serious repercussions (Dynkin and Dynkin, 2018). These attacks are on the rise and are causing losses of billions of dollars (Cremer et al., 2022), as well as loss of market capitalization (Mukhopadhyay *et al.*, 2019). Consequently, directors are more likely to be held responsible when organizations experience attacks (Frank, Grenier and Pyzoha, 2021). Thus, the senior leadership is critical in ensuring responsible cybersecurity within organizations (Panteli, Nthubu and Mersinas, 2025).

The Top Management Teams (TMTs) play a central role in daily operations and are responsible for strategic decisions (Bendig et al., 2023), with cybersecurity being one of their major responsibilities (Li et al., 2018). TMT is duty-bound to ensure effective cyber risk management (Radu & Smaili, 2022). They need to possess cybersecurity knowledge, competence, and skills (Garcia-Granados & Bahsi, 2020). Delegating cybersecurity risk management to the IT department has proven insufficient (Rothrock & Kaplan, 2018). However, many leaders remain inadequately equipped with a technical background for the tasks (Gale et al., 2022).

Various methods and techniques have been developed to enhance cybersecurity awareness among the TMT (Taherdoost, 2024). While awareness aims to instil a proactive attitude toward cybersecurity, skills provide the necessary tools for maintaining security hygiene (Haney & Lutters, 2020). However, their training and awareness programs have received limited scholarly attention, and many remain unaware of key threats (Vrhovec & Markelj, 2024). Moreover, memory retention from an awareness program tends to be short-lived (Ghafir et al., 2018). The lack of sustainable cybersecurity programs within organizations is a recurring concern (Akter et al.,

2025). Additionally, there is no consensus on the metrics for measuring the effectiveness of cybersecurity awareness programs for TMT (Chaudhary et al., 2022).

Chowdhury & Gkioulos (2021b) conducted a literature review of 29 papers addressing workforce knowledge, skills, and competencies. TMT competencies have not been specifically explored in reviews, except for the finding that managers and top executives hold the mandate to ensure effective implementation of cybersecurity measures in their organizations (Vidgren, 2020). This highlights the research gap concerning cybersecurity competencies in top management.

This literature review seeks to answer the following question:

What cybersecurity management competencies have been identified that support TMT strategic responsibilities for cybersecurity management in critical infrastructure organizations?

The paper is structured as follows: Section two defines key concepts, including the top management team, competence, and cybersecurity management competence. Section three outlines the review methodology. Section four presents the findings. Section five discusses the results, and Section six concludes the paper.

2. Key Concepts

2.1 Top Management Team

Numerous academics have examined the concept of the Top Management Team (TMT), they are organization's senior officers (Carpenter, Geletkanycz and Sanders, 2004). TMT are the top senior officers who make and participate in strategic decisions (Amason, 1996). According to Menz (2012a) TMT consists of senior executives with one or more functional responsibilities. They represent the highest and second-highest levels of executive management (Wiersema, 1992). TMT exerts a significant influence on strategy formulation (Nielsen, 2010). They are also responsible for planning and executing strategies (Wu *et al.*, 2017), and are recognized as the senior executives who manage the organization's business (Gao, Wattal and Thatcher, 2025).

Li et al., (2022) identified members such as the chief executive officer, chief financial officer, vice president, general manager, chief executive deputy general manager, and vice manager. Increasingly, the chief information security officer has been included in the TMTs due to growing concerns about cybersecurity (Gao, Wattal and Thatcher, 2025). Other roles include the chief information officer (Bendig *et al.*, 2023), chief technology officer (Gu, Wang and Mai, 2024), chief information officer, chief strategy officer, chief knowledge officer, chief operations officer, and chief marketing officer (Menz, 2012b).

2.2 Competency

The term competence has attracted significant interest in organizational management (Salman, Ganie and Saleem, 2020). Researchers from education, psychology, human resources, management, politics, and information systems have aligned its meaning within their respective fields (Hoffmann, 1999; Bassellier, Benbasat and Reich, 2003). Consequently, competence lacks a universally accepted definition (Jubb and Robotham, 1997). Nonetheless, it continues to be applied across different perspectives

It is viewed as a combination of skills, performance, personal traits, or knowledge essential for the effective delivery of a role (Brophy and Kiely, 2002). It represents the potential that leads to effective behavior and the capability of an individual to perform successfully in a specific role (Anderson, Ahmad and Chang, 2024a). Individual competence contributes to the organization's core competence (Bassellier, Reich and Benbasat, 2001). Blömeke et al. (2015 p. 4) ''criterion behavior as well as the knowledge, cognitive skills, and affective-motivational dispositions that underlie that behavior." More broadly, it reflects the behavior of an entity that enables effective performance in its role (Woodruffe, 1993).

3. Method

To ensure the collection of relevant articles, the review follows the framework proposed by Okoli (Okoli, 2015) which includes the following steps: I) establishing the purpose of the literature review, II) protocol, III) searching for literature, IV) practical screen, V) quality appraisal, VI) data extraction, VII) synthesis of studies, and VII) writing the review.

3.1 Purpose of the Literature Review

The objectives of this literature review are to identify and analyze articles on the cybersecurity competencies of the top management team (TMT) in CI organizations as follows:

- Identify papers published in top information systems, cybersecurity, and critical infrastructure outlets that address cybersecurity competencies necessary for top management in strategic decision-making and cybersecurity management
- Analyze and evaluate the identified research articles to summarize findings related to TMT cybersecurity competencies in critical infrastructure organizations.
- Reveal research gaps concerning cybersecurity competencies of the top management team in the CI organizations.

3.2 Protocol and Literature Search

We conducted a literature search on 14 journals with the search terms: (cybersecurity OR "Information Security") AND ("Top Management" OR "senior management" OR "executive officers") AND ("Critical Infrastructure"). We used the databases Web of Science, Scopus, and Google Scholar, as well as direct searches of the listed journals. The initial search yielded: Google Scholar = 256, Scopus = 71, and Web of Science = 3, for a total of 330 articles. This number was significantly lower than expected. Therefore, to increase the likelihood of finding more relevant articles, a direct search in the chosen journals was conducted. These methods yielded an additional 698 articles; combined with the 330 articles from Google Scholar, Web of Science, and Scopus, a total of 1,028 articles were selected.

3.3 Practical Screening

During practical screening, papers were selected based on their title, abstract, year of publication 2003-2025, discussion, results, and summary, English language, setting related to TMT cybersecurity competency, and Senior Management staff as participants or subjects. Papers that focused on only technical aspects of cybersecurity were excluded.

3.4 Quality Appraisal

Initially, only papers matching the keywords in their titles or abstracts were selected. A total of 104 papers from the journals met these criteria.

Table 1: List of additional papers through forward and backward searches

SN	Forward	Cited	Backward	From the Ref. List
1	(Jewer and McKay, 2025)	(Bassellier, Benbasat and Reich, 2003; Benaroch and Chernobai, 2017; Haislip, Lim and Pinsker, 2021)	(Puhakainen and Siponen, 2010)	(Barton *et al.*, 2016)
2	(Onibere, Ahmad, and Maynard, 2017)	(Ashenden and Sasse, 2013)		
3	(Anderson, Ahmad, and Chang, 2022)	(Ashenden and Sasse, 2013)		

The second selection process resulted in 31 papers that met the criteria. In addition to this selection, backwards searches produced 1 paper and forward searches yielded 3 papers, as indicated in the table above.

Thematic analysis was adopted with inductive coding; therefore, themes are derived based on what the data "tell us".

3.5 Leadership

Strategic cybersecurity leadership comprises executives and managers - the top management team – identified in the literature as those responsible for cybersecurity risk management, governance, and compliance. Their strategic roles influence the organization's cybersecurity risk posture, culture, and resilience. The literature indicates that senior management plays a highly instrumental role in cybersecurity risk decision-making activities (Ashenden and Sasse, 2013; Onibere, Ahmad and Maynard, 2017; Benaroch and Fink, 2021; Haislip, Lim and Pinsker, 2021; Bendig *et al.*, 2022; Shillair *et al.*, 2022; Lorenz and Buchwald, 2023; Jewer and McKay, 2025; Sahin and Vance, 2025)

Several articles have viewed cybersecurity strategic responsibilities as resting on cybersecurity managers and leaders, such as the CTO, CIO, and CISO (Ashenden and Sasse, 2013; Onibere, Ahmad and Maynard, 2017; Kappelman *et al.*, 2019; Anderson, Ahmad and Chang, 2022; Bendig *et al.*, 2022; Ramezan, 2025; Sahin and Vance, 2025), despite the limited access of CISOs to the board (RenÃ, 2022). Furthermore, the inclusion of the CIO in the C-suite is being misunderstood (Bendig *et al.*, 2022).

3.6 Organization

Organizational objectives, strategies, and policies should align with cybersecurity readiness, as security improves when cybersecurity goals are integrated with broader organizational objectives (AlGhamdi, Win and Vlahu-Gjorgievska, 2020; Anderson, Ahmad and Chang, 2022). In practice, the responsibilities of the TMT to their organizations in ensuring effective information security governance and leadership accountability can strengthen the organization's security posture (AlGhamdi, Win and Vlahu-Gjorgievska, 2020; Alshaikh, 2020; Shillair *et al.*, 2022). We found strong connections between the organizational objectives and cybersecurity strategic alignment, and leadership (Onibere, Ahmad and Maynard, 2017; Anderson, Ahmad and Chang, 2022). Additionally, differences in the organizational levels affect cybersecurity management: large and small organizations have boards (Anderson, Ahmad and Chang, 2022) SMEs may face constraints due to limited resources (Almeida, 2025). Evidently, large organizations usually have a dedicated person in charge of cybersecurity, while small organizations may not (Kappelman *et al.*, 2019)

3.7 Cybersecurity

Cybersecurity management comprises a range of roles (Almeida, 2025) that require defense against threats and defense against cyber threats is one of the cybersecurity strategic goals (AlDaajeh *et al.*, 2022), which falls within the purview of the top management (Shillair *et al.*, 2022). Consequently, leaders need to adapt strategies in combating these evolving cyber threats (Anderson, Ahmad and Chang, 2024b).

This theme reflects the continuously evolving nature of cyber threats, vulnerabilities, and risks, along with the corresponding responsibility of the top management to ensure information security governance for organizational success (AlGhamdi, Win and Vlahu-Gjorgievska, 2020), and determination of response to cyber threats (Shillair *et al.*, 2022). The core of this theme highlights how TMT addresses, manages, and responds to cybersecurity practices. Since information security needs to be addressed at the strategic level (Almeida, 2025), this study underscores the critical role of the TMT in addressing these cybersecurity risks.

3.8 Learning

The theme learning focuses on the various education, training, and awareness initiatives adopted by organizations, especially CI organizations, to ensure employees acquire skills, knowledge, and competencies needed to fulfill their responsibilities. Security education, training, and awareness (SETA) has been widely seen to be one of the learning paths to increase cybersecurity culture . Anderson et al. (2022) reported that the SETA program can be seen to be a marketing plan rather than an educational one, and an awareness program for top management has been identified as one of the cybersecurity critical success factors for organizations (Yeoh *et al.*, 2022). However, no literature was found that specifically identifies a learning program mapped to the entire TMT based on its strategic positions, composition, and commitments.

3.9 Competence

Technical competencies or hard skills are typically associated with cybersecurity professionals (Onibere, Ahmad and Maynard, 2017; Furnell, 2021; Anderson, Ahmad and Chang, 2022) . Then again, competencies such as communication skills, risk management, and incident response (Anderson, Ahmad and Chang, 2022, 2024b) are identified as essential in organizational cybersecurity management processes.

The leadership and cybersecurity themes are linked through TMT's strategic responsibilities. For example, AlGhamdi et al.(2020) acknowledged the importance of the TMT in the success of information security. Haislip et al., (2021) emphasized IT governance and (Shillair *et al.*, 2022) highlighted the importance of top management involvement in responding to cyber threats. Connections between leadership and competencies (Furnell, 2021; Anderson, Ahmad and Chang, 2022; Ramezan, 2025) are crucial for top management in carrying out their responsibilities. Some are intended for cybersecurity leaders in general (Anderson, Ahmad and Chang, 2022) or for technical TMT members such as CISOs (Ramezan, 2025) Anderson et al. (2024) Focus on case-based learning to support cybersecurity leaders in their roles and emphasize pedagogical learning accordingly. Additionally, Alshaikh, (2020) reported alignment of cybersecurity awareness with an external campaign, identification of

cybersecurity behaviours, establishment of a cyber champion network, and development of a brand for the cyber team.

3.10 Synthesis

The literature includes works that consider competencies aiding in supporting top management in discharging their cybersecurity strategic responsibilities in Ci organizations. For example, A. B. Anderson et al. (2022) identified several cybersecurity competencies that include skills, knowledge, and attitudes. However, the identified competencies are found to be tailored to cybersecurity leaders. Similarly, Furnell (2021) identified various cybersecurity competencies mapped to the technical members of the TMT. Figure 1 highlights the identified connections among the themes.

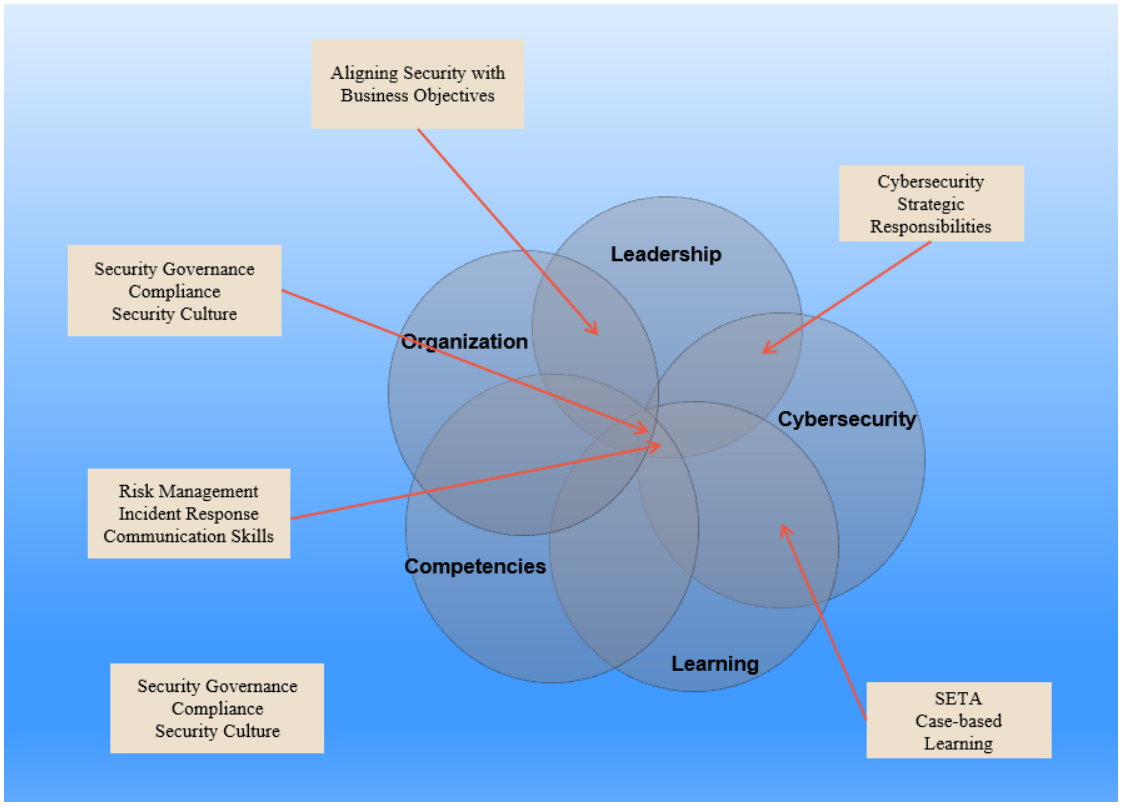

Figure 1: Connections between the identified themes

The study identified the following competencies in Table 2.

Table 2: Summarized connections among the themes

Source	Competency	Rationale
(Anderson, Ahmad, and Chang, 2022) and (Anderson, Ahmad, and Chang, 2024b)	Communication skills	For intra- and inter–team communication and discussions on cybersecurity activities, to enable members to develop a common understanding of terminologies in the decision-making process
	Risk management	To facilitate their cyber risk management decision-making process
	Incident response	To facilitate their understanding of incident mitigation, response, and remediation.
(Furnell, 2021)	Information security governance	To facilitate governance and compliance
	Business resilience	Basic business resilience skills can enhance anticipation, action, and defensive strength.
	Compliance	To facilitate understanding of the relevant acts, regulations, and compliance frameworks.
(Almeida, 2025)	Risk management, organizational factors, and governance	To facilitate their cyber risk management decision-making process

4. Discussion

The research question of this study focuses on identifying the cybersecurity competencies critical to the TMT's strategic cybersecurity management in critical infrastructure organizations. However, the literature on such competencies is very limited. Most studies examine the competencies of cybersecurity experts within the TMT, with particular attention given to roles such as CIO, CISO, and CTO (Anderson, Ahmad and Chang, 2022, 2024b). While the TMT comprises senior management, its functional diversity poses challenges to collaboration (Lorenz and Buchwald, 2023). Consequently, the role of CISO as a technical professional within the team may create functional diversity issues that affect overall decision-making processes (Ashenden and Sasse, 2013).

Our results indicate that board-level IT competencies have received some attention from researchers (Benaroch and Chernobai, 2017; Benaroch and Fink, 2021; Jewer and McKay, 2025) Though their core cybersecurity management competencies remain under-researched. The results indicate that many studies recognize the critical importance of the cybersecurity strategic responsibilities for top management of critical infrastructure organizations. However, most emphasize the competencies and skills of the technical members of the TMT, such as CISO, CIO, CTO, and CDO (Ashenden and Sasse, 2013; Onibere, Ahmad and Maynard, 2017; Kappelman *et al.*, 2019; Bendig *et al.*, 2022; RenÃ, 2022; Lorenz and Buchwald, 2023; Ramezan, 2025). Furthermore, the review suggests that emphasis is often placed on specific TMT members regarding cybersecurity competencies, without acknowledging that all team members share responsibility for organizational cybersecurity governance, resilience, and compliance. Additionally, our review noted discrepancies about the composition of the TMT. While this study does not aim to define team composition, it highlights the strong need for all TMT members to be cybersecurity-proficient and acquire a certain level of cybersecurity management competencies to support strategic cybersecurity management responsibilities and to aid in collective mindfulness (Järveläinen *et al.*, 2025). This is very important in critical infrastructure, where information technology and operational technology are a mix. Finally, we observed that only communication skills, incident response, and risk management are considered, and only for cybersecurity leaders (Anderson et al., 2022, 2024). Information security governance, information security strategy, and information risk management were also identified Furnell, (2021).

5. Conclusion

This study sets out to answer the research question: which cybersecurity management competencies have been identified as supporting TMT strategic responsibilities for cybersecurity management in CI? Despite the strategic importance of cybersecurity management in this sector, our results reveal very limited research addressing the cybersecurity management competencies of the TMT. Most studies focus on the competencies of technical roles, such as CIO, CISO, or CTO, neglecting the overall competencies of all members.

Our review found that although TMT composition, size, and skills vary depending on the size of the organization, it is consistently evident that TMT is primarily responsible for the strategic decisions related to cybersecurity.

The results revealed five main themes that are crucial for critical infrastructure organizational cybersecurity management processes: leadership, organization, cybersecurity, learning, and competence. This supports the identification of competencies essential to TMT's strategic responsibilities. Finally, identifying cybersecurity management competencies will support the enhancement of cybersecurity as the protector of the organizational value creation capabilities of CI. This review also represents a step toward creating a cybersecurity framework tailored to TMT's strategic cybersecurity management responsibilities.

5.1 Limitations and Future Research

This study is limited to some journals. We chose to systematically study a limited sample of high-quality outlets, but future research could identify additional central competencies through a broader search. This review can extend into an empirical study that applies the identified competencies and assesses the extent of TMT's level of cybersecurity management competencies in different types of organizations.

Ethic Declaration: I declare that ethical clearance was not required for this research

AI Declaration: I declare that AI was not used in the creation of the paper; however, Copilot and Grammarly were used for grammar and proofreading.

References

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. Computers & Security, 28(6), 476–490. https://doi.org/10.1016/j.cose.2009.01.003

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Raymond Choo, K.-K. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers & Security, 119, 102754. https://doi.org/10.1016/j.cose.2022.102754

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. Computers & Security, 99, 102030. https://doi.org/10.1016/j.cose.2020.102030

Almeida, F. (2025). Comparative analysis of EU-based cybersecurity skills frameworks. Computers & Security, 151, 104329. https://doi.org/10.1016/j.cose.2025.104329

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

Amason, A. C. (1996). Distinguishing the Effects of Functional and Dysfunctional Conflict on Strategic Decision Making: Resolving a Paradox for Top Management Teams.

Anderson, A., Ahmad, A., & Chang, S. (2022). Competencies of Cybersecurity Leaders: A Review and Research Agenda.

Anderson, A., Ahmad, A., & Chang, S. (2024). Case-based learning for cybersecurity leaders: A systematic review and research agenda. Information & Management, 61(7), 104015. https://doi.org/10.1016/j.im.2024.104015

Anderson, A., Ahmad, A., & Chang, S. (2024). Case-based learning for cybersecurity leaders: A systematic review and research agenda. Information & Management, 61(7), 104015. https://doi.org/10.1016/j.im.2024.104015

Ashenden, D., & Sasse, A. (2013). CISOs and organisational culture: Their own worst enemy? Computers & Security, 39, 396–405. https://doi.org/10.1016/j.cose.2013.09.004

Bakari, J. K., Tarimo, C. N., Yngström, L., Magnusson, C., & Kowalski, S. (2007). Bridging the gap between general management and technicians – A case study on ICT security in a developing country. Computers & Security, 26(1), 44–55. https://doi.org/10.1016/j.cose.2006.10.007

Bandodkar, N. R., South Carolina State University, Grover, V., & University of Arkansas. (2022). Does it Pay to Have CIOs on the Board? Creating Value by Appointing C-Level IT Executives to the Board of Directors. Journal of the Association for Information Systems, 23(4), 838–888. https://doi.org/10.17705/1jais.00747

Barton, K. A., Tejay, G., Lane, M., & Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. Computers & Security, 59, 9–25. https://doi.org/10.1016/j.cose.2016.02.007

Bassellier, G., Benbasat, I., & Reich, B. H. (2003). The Influence of Business Managers' IT Competence on Championing IT. Information Systems Research, 14(4), 317–336. https://doi.org/10.1287/isre.14.4.317.24899

Bassellier, G., Reich, B. H., & Benbasat, I. (2001). Information Technology Competence of Business Managers: A Definition and Research Model. Journal of Management Information Systems, 17(4), 159–182. https://doi.org/10.1080/07421222.2001.11045660

Benaroch, M., & Chernobai, A. (2017). Operational IT Failures, IT Value Destruction, and Board-Level IT Governance Changes. MIS Quarterly, 41(3), 729–762. https://doi.org/10.25300/MISQ/2017/41.3.04

Benaroch, M., & Fink, L. (2021). No Rose without a thorn: Board IT competence and market reactions to operational IT failures. Information & Management, 58(8), 103546. https://doi.org/10.1016/j.im.2021.103546

Bendig, D., Wagner, R., Jung, C., & Nüesch, S. (2022). When and why technology leadership enters the C-suite: An antecedents perspective on CIO presence. The Journal of Strategic Information Systems, 31(1), 101705. https://doi.org/10.1016/j.jsis.2022.101705

Bendig, D., Wagner, R., Piening, E. P., & Foege, J. N. (2023). Attention to Digital Innovation: Exploring the Impact of a Chief Information Officer in the Top Management Team. MIS Quarterly, 47(4), 1487–1516. https://doi.org/10.25300/MISQ/2023/17152

Blömeke, S., Gustafsson, J.-E., & Shavelson, R. J. (2015). Beyond Dichotomies: Competence Viewed as a Continuum. Zeitschrift Für Psychologie, 223(1), 3–13. https://doi.org/10.1027/2151-2604/a000194

Brilingaitė, A., Bukauskas, L., & Juozapavičius, A. (2020). A framework for competence development and assessment in hybrid cybersecurity exercises. Computers & Security, 88, 101607. https://doi.org/10.1016/j.cose.2019.101607

Brophy, M., & Kiely, T. (2002). Competencies: A new sector. Journal of European Industrial Training, 26(2/3/4), 165–176. https://doi.org/10.1108/03090590210422049

Buchler, N., Rajivan, P., Marusich, L. R., Lightner, L., & Gonzalez, C. (2018). Sociometrics and observational assessment of teaming and leadership in a cyber security defense competition. Computers & Security, 73, 114–136. https://doi.org/10.1016/j.cose.2017.10.013

Carpenter, M. A., Geletkanycz, M. A., & Sanders, Wm. G. (2004). Upper Echelons Research Revisited: Antecedents, Elements, and Consequences of Top Management Team Composition. Journal of Management, 30(6), 749–778. https://doi.org/10.1016/j.jm.2004.06.001

Dynkin, B., & Dynkin, B. (2018). DERIVATIVE LIABILITY IN THE WAKE OF A CYBER ATTACK. 28.3.

Eggers, F., Hatak, I., Kraus, S., & Niemand, T. (2017). Technologies That Support Marketing and Market Development in SMEs—Evidence from Social Networks. Journal of Small Business Management, 55(2), 270–302. https://doi.org/10.1111/jsbm.12313

Frank, M. L., Grenier, J. H., & Pyzoha, J. S. (2021). Board liability for cyberattacks: The effects of a prior attack and implementing the AICPA's cybersecurity framework. Journal of Accounting and Public Policy, 40(5), 106860. https://doi.org/10.1016/j.jaccpubpol.2021.106860

Furnell, S. (2021). The cybersecurity workforce and skills. Computers & Security, 100, 102080. https://doi.org/10.1016/j.cose.2020.102080

Gao, Y., Wattal, S., & Thatcher, J. (2025). Chief Information Security Officers on Top Management Teams: Impact on Firms' Innovation. Information Systems Research, isre.2023.0197. https://doi.org/10.1287/isre.2023.0197

Georgiadou, A., Michalitsi - Psarrou, A., & Askounis, D. (2023). A security awareness and competency evaluation in the energy sector. Computers & Security, 129, 103199. https://doi.org/10.1016/j.cose.2023.103199

Gu, Y., Wang, L., & Mai, Y. (2024). Do you need a chief technology officer? The effect of appointing a CTO on innovation activities in high-tech new ventures. Journal of Product Innovation Management, 41(6), 1118–1140. https://doi.org/10.1111/jpim.12749

Guhr, N., Lebek, B., & Breitner, M. H. (2019). The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory. Information Systems Journal, 29(2), 340–362. https://doi.org/10.1111/isj.12202

Haislip, J., Lim, J.-H., & Pinsker, R. (2021). The Impact of Executives' IT Expertise on Reported Data Security Breaches. Information Systems Research, 32(2), 318–334. https://doi.org/10.1287/isre.2020.0986

Hoffmann, T. (1999). The meanings of competency. Journal of European Industrial Training, 23(6), 275–286. https://doi.org/10.1108/03090599910284650

Hsu, C., Lee, J.-N., & Straub, D. W. (2012). Institutional Influences on Information Systems Security Innovations. Information Systems Research, 23(3-part-2), 918–939. https://doi.org/10.1287/isre.1110.0393

Jewer, J., & McKay, K. N. (2025). Unpacking Board-Level IT Competency.

Jubb, R., & Robotham, D. (1997). Competences in management development: Challenging the myths. Journal of European Industrial Training, 21(5), 171–175. https://doi.org/10.1108/03090599710171422

Kappelman, L., Johnson, V., Torres, R., Maurer, C., & McLean, E. (2019). A study of information systems issues, practices, and leadership in Europe. European Journal of Information Systems, 28(1), 26–42. https://doi.org/10.1080/0960085X.2018.1497929

Li, Y., Posey, C., & Stafford, T. (2024). Bureaucracies in information securing: Transitioning from iron cages to iron shields. Information and Organization, 34(3), 100526. https://doi.org/10.1016/j.infoandorg.2024.100526

Li, Z., Wang, B., & Zhou, D. (2022). Financial experts of top management teams and corporate social responsibility: Evidence from China. Review of Quantitative Finance and Accounting, 59(4), 1335–1386. https://doi.org/10.1007/s11156-022-01077-5

Lorenz, F., & Buchwald, A. (2023). A perfect match or an arranged marriage? How chief digital officers and chief information officers perceive their relationship: a dyadic research design. European Journal of Information Systems, 32(3), 372–389. https://doi.org/10.1080/0960085X.2023.2178742

Markus, M. L., & Robey, D. (1988). Information technology and organizational change: Causal structure in theory and research. Management science, 34(5), 583-598. https://doi.org/https://doi.org/10.1287/mnsc.34.5.583

Menz, M. (2012a). Functional Top Management Team Members: A Review, Synthesis, and Research Agenda. Journal of Management, 38(1), 45–80. https://doi.org/10.1177/0149206311421830

Menz, M. (2012b). Functional Top Management Team Members: A Review, Synthesis, and Research Agenda. Journal of Management, 38(1), 45–80. https://doi.org/10.1177/0149206311421830

Mukhopadhyay, A., Chatterjee, S., Bagchi, K. K., Kirs, P. J., & Shukla, G. K. (2019). Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance. Information Systems Frontiers, 21(5), 997–1018. https://doi.org/10.1007/s10796-017-9808-5

Nautiyal, L., & Rashid, A. (2024). A framework for mapping organisational workforce knowledge profile in cyber security. Computers & Security, 145, 103925. https://doi.org/10.1016/j.cose.2024.103925

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (No. NIST SP 800-181; p. NIST SP 800-181). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-181

Nielsen, S. (2010). Top Management Team Diversity: A Review of Theories and Methodologies. International Journal of Management Reviews, 12(3), 301–316. https://doi.org/10.1111/j.1468-2370.2009.00263.x

Okoli, C. (2015). A Guide to Conducting a Standalone Systematic Literature Review. Communications of the Association for Information Systems, 37. https://doi.org/10.17705/1CAIS.03743

Onibere, M., Ahmad, A., & Maynard, S. (2017). The Chief Information Security Officer and the Five Dimensions of a Strategist.

Panteli, N., Nthubu, B. R., & Mersinas, K. (2025). Being Responsible in Cybersecurity: A Multi-Layered Perspective. Information Systems Frontiers. https://doi.org/10.1007/s10796-025-10588-0

Puhakainen & Siponen. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. MIS Quarterly, 34(4), 757. https://doi.org/10.2307/25750704

Ramezan, C. A. (2025). Understanding the chief information security officer: Qualifications and responsibilities for cybersecurity leadership. Computers & Security, 152, 104363. https://doi.org/10.1016/j.cose.2025.104363

RenÃ, M. (2022). Taking a Seat at the Table: The Quest for CISO Legitimacy.

Sahin, Z., & Vance, A. (2025). What do we need to know about the Chief Information Security Officer? A literature review and research agenda. Computers & Security, 148, 104063. https://doi.org/10.1016/j.cose.2024.104063

Salman, M., Ganie, S. A., & Saleem, I. (2020). The concept of competence: A thematic review and discussion. European Journal of Training and Development, 44(6/7), 717–742. https://doi.org/10.1108/EJTD-10-2019-0171

Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & Von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. Computers & Security, 119, 102756. https://doi.org/10.1016/j.cose.2022.102756

Trilling, R. (2018). Creating a New Academic Discipline: Cybersecurity Management Education. Proceedings of the 19th Annual SIG Conference on Information Technology Education, 78–83. https://doi.org/10.1145/3241815.3241860

Wagner, P., & Mapp, W. (2024). Identifying Information Technology (IT) and Cybersecurity Executives' Competencies to Support Comprehensive Cybersecurity Programs. European Conference on Cyber Warfare and Security, 23(1), 617–625. https://doi.org/10.34190/eccws.23.1.2317

Wiersema, M. F. (1992). Top Management Team Demography and Corporate Strategic Change. Academy of Management Journal.

Woodruffe, C. (1993). What is meant by a competency? Leadership & Organization Development Journal, 14(1), 29. https://doi.org/10.1108/eb053651

Wu, T., Wu, Y., Tsai, H., & Li, Y. (2017). Top Management Teams' Characteristics and Strategic Decision-Making: A Mediation of Risk Perceptions and Mental Models. Sustainability, 9(12), 2265. https://doi.org/10.3390/su9122265

Yeoh, W., Wang, S., Popovič, A., & Chowdhury, N. H. (2022). A systematic synthesis of critical success factors for cybersecurity. Computers & Security, 118, 102724. https://doi.org/10.1016/j.cose.2022.102724

Zhou, L., Huang, H., Chen, X., & Tian, F. (2023). Functional diversity of top management teams and firm performance in SMEs: A social network perspective. Review of Managerial Science, 17(1), 259–286. https://doi.org/10.1007/s11846-022-00524-w