REACH Journal
Management & Applied Research

Exploring the Role of Cybersecurity Leadership in Strengthening Organisational Cyber Resilience: A Qualitative Study of Corporate Organisations

Khairul Anwar bin Mustapha 1[a]

The increasing sophistication and frequency of cyber threats have elevated cybersecurity from a technical concern to a strategic organisational priority, particularly as organisations become increasingly dependent on digital technologies, interconnected systems, and data-driven operations. Despite substantial investments in cybersecurity technologies and protective mechanisms, cyber incidents continue to disrupt organisational operations, compromise critical assets, and threaten long-term sustainability, indicating that technological controls alone are insufficient to address contemporary cybersecurity challenges. While existing cybersecurity research has predominantly focused on technical safeguards, risk management practices, and governance mechanisms, comparatively limited attention has been given to the role of cybersecurity leadership in strengthening organisational cyber resilience. This study therefore explores the role of cybersecurity leadership in enhancing organisational cyber resilience within corporate organisations. A qualitative research approach was adopted, and data were collected through semi-structured interviews involving cybersecurity leaders, governance practitioners, and organisational decision-makers from corporate organisations. The interview data were analysed using thematic analysis supported by NVivo software to identify recurring patterns and themes. The findings revealed that cybersecurity leadership plays a critical role in strengthening organisational cyber resilience through strategic direction, governance coordination, organisational preparedness, cybersecurity culture development, and adaptive response capability. Effective cybersecurity leaders facilitate organisational alignment, improve communication and decision-making processes, promote cybersecurity awareness, and enhance organisational readiness to anticipate, respond to, recover from, and learn from cyber incidents. The study contributes to the growing body of cybersecurity leadership literature by providing an integrated organisational perspective on how leadership supports resilience development and extends current understanding of organisational cyber resilience beyond technological considerations. The findings further highlight leadership as a strategic enabler of resilience capability and offer practical insights for organisations seeking to strengthen cybersecurity resilience through leadership-driven governance, preparedness, and organisational development initiatives.

Keywords: *Cybersecurity Leadership, Organisational Cyber Resilience, Cybersecurity Governance, Organisational Preparedness, Cybersecurity Culture.*

Affiliation: a: Faculty of Business & Management, Innovative University College, Kuala Lumpur, Malaysia. b: Olympia Innovative School of Strategic Leadership and Sustainable Management (OISSM), Olympia Education Group, Kuala Lumpur, Malaysia

**Corresponding author: hangtuah895@gmail.com*

INTRODUCTION

The rapid advancement of digital technologies has transformed organisational operations, communication systems, and strategic decision-making processes across industries. Contemporary organisations increasingly rely on interconnected digital infrastructures, cloud computing, artificial intelligence, and data-driven systems to improve operational efficiency, innovation, and business performance. However, this growing dependence on digital technologies has simultaneously expanded organisational exposure to cybersecurity threats, including ransomware attacks, data breaches, phishing campaigns, and other forms of cyber disruption. Such incidents can significantly affect organisational continuity, operational stability, stakeholder trust, and long-term sustainability (Gordon et al., 2011; Kwon & Johnson, 2015). As cyber threats continue to evolve in sophistication and frequency, cybersecurity has become a strategic organisational concern that extends beyond technical system protection and requires greater organisational coordination and leadership involvement (Von Solms & Van Niekerk, 2013; Cojocaru & Coles-Kemp, 2025).

Despite substantial investments in cybersecurity technologies and protective mechanisms, organisations continue to experience cybersecurity incidents that disrupt critical operations and compromise organisational resilience. Existing cybersecurity research has predominantly focused on technical controls, information security systems, risk management frameworks, and governance mechanisms (Singer & Friedman, 2014; ISACA, 2019). While these studies provide valuable insights into cybersecurity protection and risk mitigation, comparatively limited attention has been given to the role of cybersecurity leadership in strengthening organisational cyber resilience. There remains insufficient understanding of how cybersecurity leaders influence organisational preparedness, strategic decision-making, communication, and adaptive response capabilities during cybersecurity disruptions (Lehto, 2021; Triplett & Mills, 2022). Furthermore, existing studies have largely adopted technology-oriented and quantitative approaches, resulting in limited qualitative understanding of how cybersecurity leadership contributes to resilience development within organisational contexts (Parkin et al., 2023). This limitation has created a significant research gap in understanding the organisational and leadership dimensions of cybersecurity resilience.

Therefore, this study aims to explore the role of cybersecurity leadership in strengthening organisational cyber resilience within corporate organisations. Drawing upon Transformational Leadership Theory and Organisational Resilience Theory, the study examines how cybersecurity leadership contributes to resilience capability through organisational coordination, preparedness, communication, and strategic influence. Using a qualitative research approach, the study seeks to provide a deeper understanding of leadership-driven resilience development within corporate environments. The findings are expected to contribute to the growing body of knowledge on cybersecurity leadership and organisational resilience while offering practical insights for organisations

seeking to strengthen their cyber resilience in increasingly complex and dynamic digital environments.

METHODOLOGY

This study adopted a qualitative research approach within a constructivist paradigm to explore the role of cybersecurity leadership in strengthening organisational cyber resilience. A qualitative approach was considered appropriate because the study sought to obtain an in-depth understanding of participants' experiences, perceptions, and interpretations regarding cybersecurity leadership and resilience-related practices within organisational contexts. The exploratory nature of the study enabled a comprehensive examination of leadership behaviours, organisational interactions, and resilience mechanisms that may not be adequately captured through quantitative methods.

Purposive sampling was employed to select participants with substantial knowledge and professional experience in cybersecurity management, governance, and organisational leadership. The participants consisted of cybersecurity leaders, governance practitioners, information security managers, and organisational decision-makers from corporate organisations operating in digitally intensive environments. These individuals were selected because of their direct involvement in cybersecurity governance, strategic decision-making, risk management, and organisational resilience initiatives. The sampling strategy ensured that participants could provide rich and relevant insights into the relationship between cybersecurity leadership and organisational cyber resilience.

Data were collected through semi-structured interviews, which allowed participants to share their experiences and perspectives while providing flexibility for further exploration of emerging issues. The interview protocol was developed based on the research objective, research question, and relevant literature on cybersecurity leadership and organisational resilience. Interviews were conducted either face-to-face or through virtual communication platforms, recorded with participants' consent, and subsequently transcribed for analysis. To enhance the credibility of the study, participants were assured of confidentiality and anonymity throughout the research process.

The collected data were analysed using Braun and Clarke's six-phase thematic analysis approach. The analysis involved data familiarisation, initial coding, category development, theme identification, theme refinement, and interpretation of findings. NVivo software was utilised to support data organisation, coding, and theme development. Through this process, recurring patterns and relationships were identified, leading to the emergence of key themes related to cybersecurity leadership and organisational cyber resilience. To ensure the trustworthiness of the findings, the study adopted established qualitative research criteria, including credibility, dependability, confirmability, and transferability.

Table 1 Participant Profile

Participant Code	Position	Functional Area
P1	Chief Information Security Officer	Cybersecurity Leadership
P2	Cybersecurity Director	Governance
P3	IT Security Manager	Information Security
P4	Risk Manager	Risk Governance
P5	Cybersecurity Manager	Cybersecurity Operations
P6	Information Security Lead	Organisational Security
P7	Governance Practitioner	Compliance and Governance
P8	Senior Decision-Maker	Strategic Management

RESULTS AND DISCUSSIONS

The thematic analysis revealed that cybersecurity leadership plays a significant role in strengthening organisational cyber resilience within corporate organisations. The findings indicate that cybersecurity leadership contributes to resilience through five interconnected dimensions: strategic leadership and vision, governance coordination, organisational preparedness, cybersecurity culture development, and adaptive response capability. Collectively, these dimensions demonstrate how leadership influences an organisation's ability to anticipate, respond to, recover from, and adapt to cybersecurity disruptions.

Table 2 Summary of Themes and Sub-Themes

Main Theme	Sub-Themes
Strategic Leadership and Vision	Strategic Direction, Decision-Making, Resource Allocation
Governance Coordination	Accountability, Risk Oversight, Cross-Functional Collaboration
Organisational Preparedness	Incident Response Planning, Business Continuity, Training and Awareness
Cybersecurity Culture Development	Employee Awareness, Leadership Commitment, Shared Responsibility
Adaptive Response and Resilience Capability	Adaptability, Recovery Capability, Organisational Learning

The findings suggest that cybersecurity leadership extends beyond technical management and functions as a strategic organisational capability. Participants consistently highlighted the importance of leadership in establishing a clear

cybersecurity vision, aligning cybersecurity objectives with organisational priorities, and ensuring that cyber risks receive appropriate attention at the executive level. Effective cybersecurity leaders were described as individuals who could translate complex technical risks into strategic business concerns, thereby facilitating informed decision-making and encouraging organisational commitment to cybersecurity initiatives. These findings support Transformational Leadership Theory, which emphasises the role of leaders in providing strategic direction, influencing organisational behaviour, and promoting alignment towards shared objectives. The findings further suggest that organisations with strong cybersecurity leadership are better positioned to integrate cybersecurity into broader organisational strategies and resilience planning.

The analysis also revealed that cybersecurity leadership contributes significantly to governance coordination. Participants emphasised that effective leaders establish accountability structures, improve communication between technical and non-technical stakeholders, and ensure that cybersecurity activities remain aligned with organisational goals. Leadership involvement was found to enhance risk oversight and facilitate collaboration across departments, enabling organisations to respond more effectively to emerging cybersecurity challenges. These findings are consistent with Risk Governance Theory, which highlights the importance of leadership oversight and governance mechanisms in managing organisational risks. The results indicate that governance coordination strengthens resilience by creating a structured environment in which cybersecurity responsibilities, decision-making processes, and risk management activities are clearly defined and effectively implemented.

Another important finding relates to organisational preparedness. Participants reported that cybersecurity leaders play a central role in promoting preparedness initiatives, including incident response planning, business continuity management, cybersecurity awareness programmes, disaster recovery planning, and simulation exercises. These activities were perceived as essential for ensuring organisational readiness and reducing the impact of cybersecurity incidents. Participants further noted that preparedness should be viewed as an ongoing organisational process rather than a one-time exercise. Effective leaders continuously evaluate emerging threats, update preparedness strategies, and encourage proactive risk management practices. This finding supports Organisational Resilience Theory, which identifies preparedness as a critical component of organisational resilience. The results demonstrate that leadership commitment is essential in embedding preparedness practices within organisational operations and strengthening resilience capability over time.

The findings further revealed that cybersecurity leadership influences the development of a positive cybersecurity culture. Participants highlighted that leaders play an important role in shaping employee attitudes, behaviours, and awareness regarding cybersecurity responsibilities. Leadership support for awareness programmes, communication initiatives, and organisational learning activities contributed to greater employee engagement and accountability. Cybersecurity culture was viewed as a shared

organisational responsibility rather than a function limited to technical departments. Organisations with strong leadership commitment to cybersecurity were perceived to have higher levels of employee awareness and stronger adherence to cybersecurity policies and practices. These findings suggest that cybersecurity culture serves as an important organisational mechanism through which leadership enhances resilience capability by encouraging vigilance, responsible behaviour, and collective participation in cybersecurity efforts.

Finally, the findings indicate that cybersecurity leadership contributes directly to organisational cyber resilience by enhancing adaptive response and recovery capability. Participants described resilience as the ability to anticipate, withstand, respond to, recover from, and learn from cybersecurity disruptions. Effective leaders were found to facilitate communication during crises, coordinate organisational responses, support recovery efforts, and promote continuous improvement following cybersecurity incidents. Organisational learning emerged as a particularly important aspect of resilience development, as participants emphasised the value of post-incident reviews, knowledge sharing, and lessons learned initiatives. These activities enabled organisations to strengthen future preparedness and improve their ability to adapt to evolving cyber threats. The findings therefore suggest that cybersecurity leadership functions as a critical enabler of resilience by supporting adaptability, recovery, and continuous organisational learning.

Overall, the findings demonstrate that cybersecurity leadership is a foundational organisational capability that influences cyber resilience through strategic direction, governance coordination, preparedness enhancement, cultural development, and adaptive response capability. The study extends existing cybersecurity literature by providing empirical evidence that leadership plays a central role in shaping resilience outcomes within corporate organisations. Consistent with Transformational Leadership Theory and Organisational Resilience Theory, the findings indicate that resilience is not solely dependent on technological controls but is also influenced by leadership-driven organisational processes that strengthen preparedness, adaptability, and long-term resilience capability. Consequently, organisations seeking to enhance cyber resilience should complement technological investments with leadership development initiatives that foster strategic coordination, organisational learning, and resilience-oriented practices.

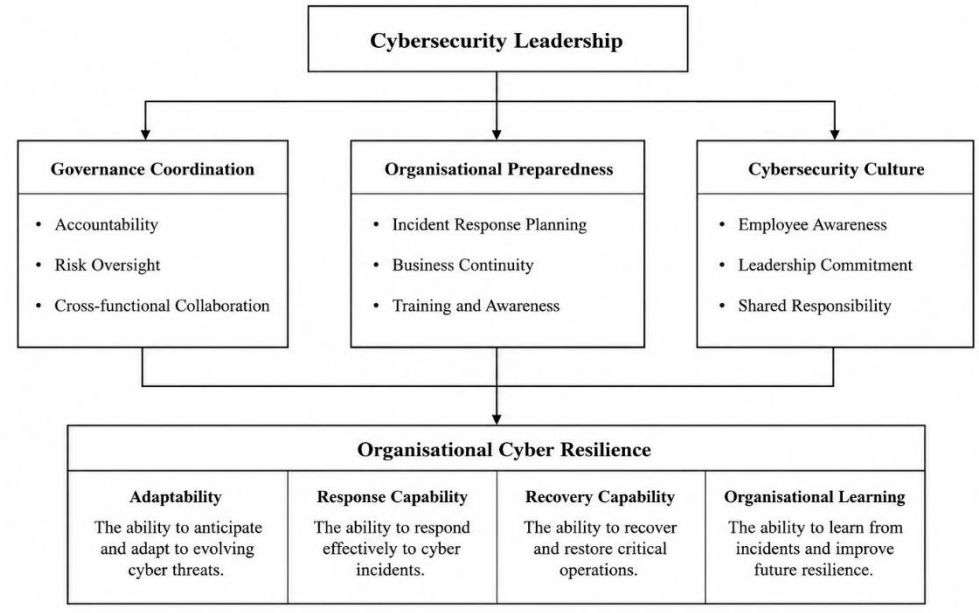

Figure 1 The role of cybersecurity leadership in strengthening organisational cyber resilience

Figure 1 summarises the relationship between cybersecurity leadership and organisational cyber resilience that emerged from the thematic analysis. The findings indicate that cybersecurity leadership acts as the primary organisational driver influencing governance coordination, organisational preparedness, and cybersecurity culture, which collectively contribute to organisational cyber resilience.

CONCLUSIONS

This study explored the role of cybersecurity leadership in strengthening organisational cyber resilience within corporate organisations. The study was motivated by the increasing complexity of cyber threats and the limited attention given to leadership-related factors in existing cybersecurity research, which has predominantly focused on technological controls and risk management mechanisms. The primary objective of the study was to examine how cybersecurity leadership contributes to organisational cyber resilience from an organisational and strategic perspective.

The findings revealed that cybersecurity leadership plays a critical role in enhancing organisational cyber resilience through strategic direction, governance coordination, organisational preparedness, cybersecurity culture development, and adaptive response capability. Effective cybersecurity leaders were found to facilitate organisational alignment, strengthen communication and decision-making processes, promote cybersecurity awareness, and support preparedness initiatives that improve an organisation's ability to anticipate, respond to, recover from, and learn from cybersecurity incidents. The findings further suggest that organisational cyber resilience is not solely dependent on technological capabilities but is significantly influenced by leadership-driven organisational processes and behaviours.

This study contributes to the growing body of knowledge on cybersecurity leadership by providing an integrated organisational perspective on the relationship between leadership and cyber resilience. The findings extend current understanding of organisational cyber resilience beyond technical considerations and highlight leadership as a strategic enabler of resilience capability. From a practical perspective, the study offers valuable insights for organisational leaders, cybersecurity professionals, and decision-makers seeking to strengthen resilience through leadership-driven governance, preparedness, and organisational development initiatives.

Several limitations should be acknowledged. First, the study adopted a qualitative approach focusing on participants from corporate organisations, which may limit the generalisability of the findings to other organisational contexts. Second, the findings were derived from participants' experiences and perceptions, which may be influenced by organisational and industry-specific factors. Future research may employ quantitative approaches to validate the relationships identified in this study and examine the influence of cybersecurity leadership on organisational cyber resilience across different industries, organisational settings, and geographical regions. Comparative and longitudinal studies may also provide deeper insights into how cybersecurity leadership evolves in response to emerging cyber threats and changing organisational environments.

Overall, the study highlights the importance of cybersecurity leadership as a foundational organisational capability that supports resilience development and contributes to the long-term sustainability of organisations operating in increasingly complex digital environments.

REFERENCES

Bhamra, R., Dani, S., & Burnard, K. (2011). Resilience: The concept, a literature review and future directions. *International Journal of Production Research, 49*(18), 5375–5393. https://doi.org/10.1080/00207543.2011.563826

Bongiovanni, I., Renaud, K., & Carroll, J. M. (2023). Cybersecurity governance: A systematic review of organisational approaches and challenges. *Computers & Security, 125*, 103022. https://doi.org/10.1016/j.cose.2022.103022

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Braun, V., & Clarke, V. (2022). *Thematic analysis: A practical guide*. Sage Publications.

Cojocaru, I., & Coles-Kemp, L. (2025). Organisational preparedness and cybersecurity resilience in digitally transformed environments. *Journal of Cybersecurity, 11*(1), 1–17.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security, 19*(1), 33–56. https://doi.org/10.3233/JCS-2010-0398

Harel, A. (2025). Board oversight and cybersecurity governance in contemporary organisations. *Cybersecurity Governance Review, 12*(1), 15–29.

ISACA. (2019). *COBIT 2019 framework: Governance and management objectives*. ISACA.

Kwon, J., & Johnson, M. E. (2015). Proactive versus reactive security investments in the healthcare sector. *MIS Quarterly Executive, 14*(1), 43–56.

Lehto, M. (2021). Cybersecurity leadership and organisational resilience: Emerging leadership challenges in the digital era. *Information and Computer Security, 29*(4), 601–617.

Linkov, I., & Kott, A. (2019). *Fundamental concepts of cyber resilience: Introduction and overview*. Springer. https://doi.org/10.1007/978-3-319-77492-3

Parkin, S., Nurse, J. R. C., & Rashid, A. (2023). Cybersecurity leadership and strategic organisational decision-making. *Computers & Security, 128*, 103204. https://doi.org/10.1016/j.cose.2023.103204

Panteli, N., Sarker, S., & Sarker, S. (2025). Leadership, collaboration, and cyber resilience in complex organisational environments. *Information Systems Journal, 35*(2), 221–244.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Slay, J., & Miller, M. (2019). Lessons learned from cybersecurity failures: Governance, leadership, and organisational challenges. *Computers & Security, 87*, 101568. https://doi.org/10.1016/j.cose.2019.101568

Tsen, T. H., Bakar, N. A. A., & Abdullah, N. H. (2022). Organisational preparedness and cyber resilience capability: Evidence from digital organisations. *Journal of Information Security and Applications, 66*, 103145. https://doi.org/10.1016/j.jisa.2022.103145

Triplett, C., & Mills, R. (2022). Human factors and cybersecurity leadership effectiveness. *Information Management Review, 37*(4), 45–58.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cybersecurity. *Computers & Security, 38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business School Press.

Woods, D. D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering & System Safety, 141*, 5–9. https://doi.org/10.1016/j.ress.2015.03.018

Yukl, G. (2012). *Leadership in organizations* (8th ed.). Pearson Education.