ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768314
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

BREAKING CYBERSECURITY SILOS: BRIDGING TECHNICAL SECURITY METRICS AND BUSINESS RISK METRICS IN THE NIGERIAN FINANCIAL SECTOR

ADAMU GARBA MUBI[1] ALIYU BUBA ADAHIRU[3] MOHAMMED KABIRU HALIDU[3]

[1]Computer Science Department, Federal Polytechnic Mubi, Adamawa State Nigeria

[2,3]Computer Engineering Department, Federal Polytechnic Mubi, Adamawa State Nigeria

08069516858, 08029485679

Emails: adamumubi@gmail.com

Abstract

The increasing frequency and sophistication of cyber threats have intensified the need for effective cybersecurity governance within financial institutions. In the Nigerian financial sector, cybersecurity teams frequently rely on technical security metrics such as vulnerability counts, patching rates, intrusion attempts, and incident detection times to evaluate security performance. However, these metrics are often difficult for executive management, boards of directors, and risk managers to interpret in terms of business impact, resulting in a disconnect between cybersecurity operations and enterprise risk management processes. This study examines the challenges associated with bridging technical security metrics and business risk metrics and proposes an integrated framework to enhance cyber risk communication and decision-making within Nigerian financial institutions. The study adopts a qualitative conceptual research design based on a comprehensive review of scholarly literature, industry reports, regulatory guidelines, and cybersecurity governance frameworks published between 2020 and 2026. Drawing upon Enterprise Risk Management Theory, Institutional Theory, and Socio-Technical Systems Theory, the study develops a framework that translates technical cybersecurity indicators into business-oriented risk measures aligned with organizational objectives and regulatory requirements. The study argues that integrating technical security metrics with business risk metrics improves cyber risk visibility, strengthens governance, enhances executive

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768314
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

decision-making, and supports regulatory compliance. The proposed framework contributes to cybersecurity governance literature by providing a structured approach for aligning cybersecurity measurement with business risk management, thereby enabling Nigerian financial institutions to improve resilience and manage cyber risks more effectively in an increasingly digital financial ecosystem.

Keywords: Cybersecurity Metrics; Business Risk Metrics; Cyber Risk Governance; Nigerian Financial Sector; Enterprise Risk Management; Cyber Risk Quantification; Organizational Resilience

1. Introduction

The rapid digital transformation of the financial sector has significantly increased reliance on information and communication technologies for service delivery, operational efficiency, and customer engagement. In Nigeria, the widespread adoption of digital banking, financial technology (FinTech), cloud computing, and real-time payment systems has improved financial inclusion and operational performance but has simultaneously expanded the cyber threat landscape (Central Bank of Nigeria, 2023; World Bank, 2022). Consequently, cybersecurity has evolved from a technical concern to a strategic governance issue requiring effective integration with enterprise risk management (ERM) to safeguard organizational assets, ensure regulatory compliance, and maintain stakeholder confidence (NIST, 2024; World Economic Forum, 2024).

Financial institutions remain prime targets for cyberattacks because of the high value of financial assets, sensitive customer information, and interconnected digital infrastructures. Threats such as ransomware, phishing, insider attacks, business email compromise, and data breaches continue to challenge organizational resilience despite substantial investments in cybersecurity technologies, threat intelligence, and incident response capabilities (ENISA, 2024; IBM Security, 2024). A persistent challenge, however, is that cybersecurity performance is typically measured using technical indicators—such as vulnerabilities, security alerts, patch compliance, and incident response times—which are often difficult for executives and boards to interpret in terms of business risk, financial impact, and strategic decision-making (Kaplan & Mikes, 2021; Zhang et al., 2022).

This disconnect between technical cybersecurity metrics and business-oriented risk measures has emerged as a major concern in cybersecurity governance. While enterprise risk management requires risks to be evaluated in relation to organizational objectives, financial performance, regulatory obligations, and operational resilience, cybersecurity measurement frequently remains confined to technical domains, limiting its value for strategic governance (COSO, 2017; ISO, 2018; Yaraghi & Sharman, 2021). As a result, organizations increasingly require measurement approaches capable of translating technical cybersecurity

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768314
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

information into business-relevant risk intelligence that supports executive decision-making and enterprise-wide risk management.

Although cybersecurity governance and enterprise risk management have received considerable research attention, existing studies largely examine these areas independently. Relatively limited research has developed integrated frameworks that systematically connect technical cybersecurity metrics with business risk metrics, particularly within highly regulated financial sectors in emerging economies such as Nigeria. This gap has become increasingly important as digital transformation, evolving cyber threats, and regulatory expectations continue to reshape the Nigerian financial landscape (Central Bank of Nigeria, 2023; World Economic Forum, 2025).

Accordingly, this study develops an integrated framework for aligning cybersecurity metrics with business risk metrics within the Nigerian financial sector. The proposed framework is intended to improve communication between cybersecurity professionals, risk managers, executive leadership, and boards of directors by translating technical security information into meaningful business risk intelligence. In doing so, the study seeks to strengthen cybersecurity governance, enhance enterprise risk management, and support more informed strategic decision-making in digitally enabled financial institutions.

2. Literature Review

The rapid growth of digital technologies has transformed cybersecurity into a strategic governance issue, particularly within financial institutions where cyber incidents can result in significant financial, operational, regulatory, and reputational consequences. Consequently, organizations increasingly rely on cybersecurity metrics to monitor security performance, evaluate vulnerabilities, support incident response, and assess overall security posture. Traditional cybersecurity metrics, including vulnerability counts, patch compliance, intrusion alerts, and incident response times, provide valuable operational information but often fail to communicate the business implications of cyber risk to executive management and boards of directors (Kaplan & Mikes, 2021; Yaraghi & Sharman, 2021).

Enterprise Risk Management (ERM) has broadened the perspective of cybersecurity governance by recognizing cyber risk as an enterprise-wide business risk rather than solely a technical issue. ERM frameworks emphasize evaluating risks according to their impact on organizational objectives, financial performance, operational continuity, regulatory compliance, and stakeholder value. Consequently, business risk metrics—such as potential financial loss, operational disruption, regulatory exposure, and reputational damage—provide decision-makers with information that is more relevant for strategic planning than technical security indicators alone (COSO, 2017; ISO 31000, 2018).

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768314
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Recent literature increasingly advocates integrating cybersecurity metrics with business risk metrics to bridge the communication gap between technical specialists and organizational leadership. Rather than reporting isolated technical indicators, researchers recommend translating cybersecurity events into business-oriented measures that reflect potential financial losses, service disruptions, compliance risks, and organizational resilience. Such integration improves executive understanding, supports risk-based decision-making, strengthens governance, and facilitates more effective allocation of cybersecurity resources (Olaniyi & Reidolf, 2021; Zhang et al., 2022).

Cyber risk quantification approaches, including FAIR and other quantitative risk assessment models, further support this transition by expressing cyber risks in measurable business terms. Although these approaches improve strategic decision-making, challenges remain regarding data availability, model complexity, and the consistent estimation of cyber-related losses, particularly within highly regulated sectors such as financial services (Bouveret, 2020; Radanliev et al., 2020).

The study is anchored on Enterprise Risk Management Theory**,** Socio-Technical Systems Theory**, and** Institutional Theory. Collectively, these perspectives emphasize that cybersecurity outcomes are shaped by the interaction of technology, organizational processes, governance structures, and external regulatory requirements. They further suggest that effective cyber risk management depends on integrating technical security information with organizational decision-making and enterprise governance.

Empirical evidence consistently indicates that organizations integrating cybersecurity measurement with enterprise risk management demonstrate stronger governance, improved cyber risk visibility, better executive decision-making, and greater organizational resilience (Zwikael & Meredith, 2021; Trompeter et al., 2022). Nevertheless, existing studies largely examine cybersecurity metrics, cyber risk quantification, and enterprise risk management independently. Relatively limited research has developed integrated frameworks that systematically connect technical cybersecurity indicators with business risk metrics, particularly within the Nigerian financial sector, where rapid digital transformation and evolving regulatory requirements continue to increase cyber risk exposure.

This study addresses this gap by developing an integrated framework that aligns cybersecurity metrics with business risk metrics to improve cybersecurity governance, executive communication, enterprise risk management, and strategic decision-making within Nigeria's financial sector.

3. Theoretical and Conceptual Foundations

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768314
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

This study is grounded in Enterprise Risk Management (ERM) Theory**,** Institutional Theory**, and** Socio-Technical Systems Theory**,** which collectively explain the integration of cybersecurity metrics with business risk metrics. ERM Theory views cyber risk as an enterprise-wide risk that should be evaluated alongside financial, operational, regulatory, and strategic risks to support organizational decision-making. Institutional Theory explains that regulatory requirements, industry standards, and stakeholder expectations compel financial institutions to strengthen cybersecurity governance and demonstrate effective cyber risk management. Socio-Technical Systems Theory emphasizes that cybersecurity outcomes are shaped by the interaction of technology, people, organizational processes, and governance structures rather than by technical controls alone.

A central concept underpinning this study is cyber risk quantification, which translates technical cybersecurity indicators into measurable business impacts such as financial loss, operational disruption, regulatory exposure, and reputational damage. Traditional cybersecurity metrics—including vulnerability counts, patch compliance, incident response time, and intrusion detection—primarily support operational security management, whereas business risk metrics evaluate organizational consequences and strategic performance. Integrating these two perspectives enables technical cybersecurity information to be transformed into business-relevant risk intelligence that supports executive decision-making, enterprise risk management, and organizational resilience.

Table 1: Comparison of Technical Cybersecurity Metrics and Business Risk Metrics

Dimension	Technical Cybersecurity Metrics	Business Risk Metrics
Focus	Security controls	Business impact
Audience	IT & Security Teams	Executives & Boards
Indicators	Vulnerabilities, Patch Rate, MTTD	Financial Loss, Downtime
Purpose	Operational monitoring	Strategic decision-making
Output	Security posture	Enterprise risk

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768314
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

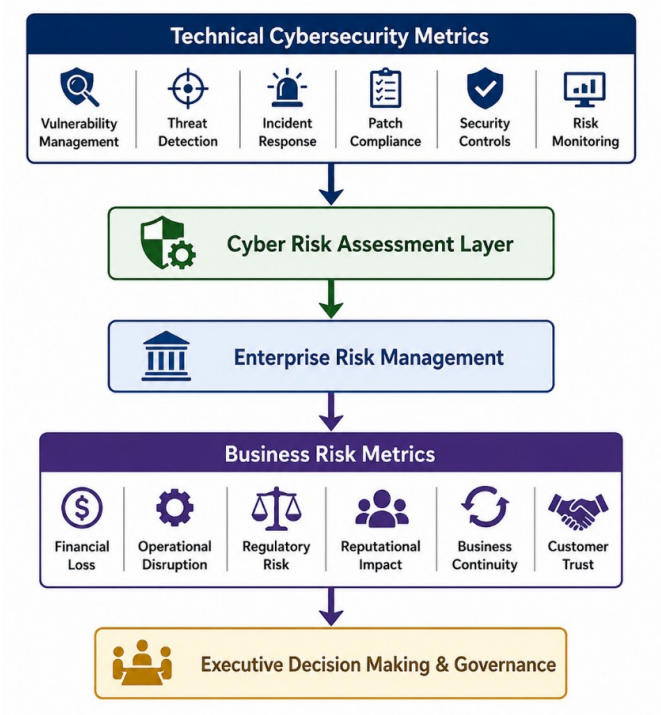

Figure 1: Theoretical Relationship between Cybersecurity Metrics and Business Risk Metrics

Source: Developed by the Author (2026)

Table 1 presents the key distinctions between technical cybersecurity metrics and business risk metrics, while **Figure 1** illustrates the

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768314
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

conceptual relationship through which technical security indicators are translated into business risk outcomes. Together, these theoretical and conceptual foundations provide the basis for the integrated framework proposed in this study to strengthen cybersecurity governance and strategic risk management within the Nigerian financial sector.

4. Methodology

This study adopted a **qualitative conceptual research approach** to examine the disconnect between technical cybersecurity metrics and business risk metrics and to develop an integrated framework for improving cybersecurity governance within the Nigerian financial sector. The approach was appropriate because the study focused on synthesizing existing knowledge rather than collecting primary data or testing hypotheses.

A literature-based research design was employed using secondary data obtained from peer-reviewed journal articles, conference papers, industry reports, regulatory publications, international standards, and professional frameworks published between 2020 and 2026. Key sources included the NIST Cybersecurity Framework**,** ISO/IEC 27001**,** ISO 31000**, the** COSO Enterprise Risk Management Framework**,** COBIT, and relevant Central Bank of Nigeria cybersecurity guidelines. Literature was selected based on its relevance to cybersecurity metrics, enterprise risk management, cyber risk quantification, governance, and financial sector resilience.

The collected literature was analysed using thematic analysis to identify recurring concepts, relationships, and best practices relating to cybersecurity measurement and business risk assessment. The analysis focused on how technical cybersecurity indicators can be translated into business-oriented risk metrics to improve executive communication, governance, and enterprise risk management.

The proposed framework was developed through conceptual synthesis by integrating insights from Enterprise Risk Management Theory**,** Institutional Theory**,** Socio-Technical Systems Theory, contemporary cybersecurity governance literature, and internationally recognized standards. Table 4 summarizes the methodological components adopted in the study. Since the research relied exclusively on publicly available secondary sources, no ethical approval was required.

Table 2: Summary of Methodological Components

Component	Description
Research Approach	Qualitative conceptual study
Research Design	Literature-based review
Data Sources	Secondary sources

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768314
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Time Scope	2020–2026
Data Analysis	Thematic analysis
Framework Basis	ERM, Institutional Theory, Socio-Technical Systems Theory
Outcome	Integrated cybersecurity–business risk framework

5. Framework Development and Discussion

The literature reveals a persistent disconnect between technical cybersecurity operations and enterprise-level decision-making within financial institutions. Although cybersecurity teams generate extensive technical data including vulnerability assessments, security alerts, incident response metrics, and patch compliance these indicators are often difficult for executives and boards to interpret in terms of business impact, regulatory exposure, financial loss, and organizational resilience. This communication gap weakens cybersecurity governance and limits the integration of cyber risk into enterprise risk management, particularly within Nigeria's rapidly digitalizing financial sector.

To address this challenge, this study proposes an Integrated Cybersecurity–Business Risk Metrics Framework that translates technical cybersecurity information into business-oriented risk intelligence. The framework positions cybersecurity metrics as inputs to enterprise risk management rather than isolated technical indicators. It comprises five interconnected stages: technical security monitoring, cyber risk contextualization, business risk translation, enterprise risk integration, and executive decision support, supported by continuous monitoring and organizational learning.

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768314
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768314
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Figure 2: Integrated Cybersecurity–Business Risk Metrics Framework

Source: Developed by the Author (2026)

The framework begins with the collection of operational cybersecurity metrics, including vulnerabilities, patch compliance, incident response performance, and security control effectiveness. These technical indicators are subsequently evaluated within the context of critical business assets, operational processes, regulatory obligations, and organizational objectives to determine their potential business consequences. The resulting information is then translated into business-oriented metrics such as financial exposure, operational disruption, regulatory risk, reputational impact, and business continuity implications, enabling executives to evaluate cyber risks using a common organizational language.

Table 3: Examples of Technical Security Metrics and Corresponding Business Risk Metrics

Technical Metric	Business Metric	Strategic Interpretation
Critical Vulnerabilities	Financial Exposure	Potential financial loss
Mean Time to Detect	Operational Risk	Incident impact duration
Mean Time to Respond	Business Continuity	Recovery capability
Patch Compliance	Regulatory Risk	Compliance readiness
Phishing Rate	Human Risk	Staff awareness
Security Incidents	Reputational Risk	Customer confidence
Unauthorized Access	Fraud Risk	Financial exposure

Table 3 illustrates examples of how technical cybersecurity metrics can be mapped to corresponding business risk metrics, while **Figure 2** presents the overall framework. Once translated, these metrics are incorporated into enterprise risk management processes, executive dashboards, and governance reports, allowing cyber risks to be assessed alongside financial, operational, and strategic risks. This integration improves executive communication, supports risk-based resource allocation, strengthens regulatory compliance, and enhances organizational resilience.

The framework is particularly relevant to the Nigerian financial sector, where increasing digital transformation, evolving cyber threats, and

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768314
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

stricter regulatory expectations demand stronger cybersecurity governance. By aligning technical cybersecurity measurement with enterprise risk management, the framework provides financial institutions with a practical mechanism for improving governance, strengthening strategic decision-making, and enhancing organizational resilience.

Table 4: Expected Benefits of the Integrated Framework

Benefit	Cybersecurity Outcome	Business Outcome
Improved Communication	Better reporting	Executive understanding
Stronger Governance	Better oversight	Strategic decisions
Better Risk Visibility	Threat awareness	Enterprise resilience
Efficient Resource Allocation	Risk-based investment	Cost optimization
Regulatory Compliance	Stronger controls	Reduced regulatory exposure
Organizational Resilience	Better preparedness	Faster recovery

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768314
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Figure 3: Cyber Risk Decision-Making Cycle Using Integrated Metrics

Source: Developed by the Author (2026)

The expected organizational benefits are summarized in **Table 4**, while **Figure 3** illustrates the continuous cyber risk decision-making cycle that supports ongoing performance improvement and adaptive resilience. Overall, the proposed framework offers a structured and practical approach for bridging the gap between cybersecurity operations and

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768314
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

business risk management, thereby enabling more effective governance and risk-informed decision-making within Nigerian financial institutions.

6. Conclusion

This study examined the disconnect between technical cybersecurity metrics and business risk metrics within the Nigerian financial sector and proposed an **Integrated Cybersecurity–Business Risk Metrics Framework** to address this challenge. The study demonstrated that technical cybersecurity indicators alone are insufficient for supporting executive decision-making because they often fail to communicate the organizational impact of cyber risks. By integrating cybersecurity metrics with business risk measures, the proposed framework improves cyber risk visibility, strengthens governance, enhances enterprise risk management, and supports strategic decision-making.

Grounded in **Enterprise Risk Management Theory**, **Institutional Theory**, and **Socio-Technical Systems Theory**, the framework provides a structured approach for translating technical cybersecurity information into business-oriented risk intelligence. The framework offers practical value for financial institutions by improving communication between cybersecurity professionals and executive leadership, supporting regulatory compliance, and strengthening organizational resilience. Future research should empirically validate the framework across different financial institutions and explore the application of emerging technologies, including artificial intelligence and machine learning, to enhance cyber risk quantification and business risk assessment.

7. Recommendations

Financial institutions should adopt integrated cybersecurity measurement frameworks that align technical security metrics with enterprise risk management and business objectives. Regulators should promote standardized cybersecurity reporting practices that emphasize business-oriented risk metrics, while organizations should strengthen collaboration among cybersecurity, risk management, and executive teams. Continuous capacity building, performance monitoring, and the adoption of emerging technologies such as artificial intelligence and predictive analytics will further enhance cyber risk communication, governance effectiveness, and organizational resilience.

8. Acknowledgements

This research has been sponsored by the Tertiary Education Trust Fund (TETFUND-ABUJA)

References

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768314
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Aven, T. (2021). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research, 253*(1), 1–13.

Bada, M., Nurse, J. R. C., & Goldsmith, M. (2021). Cybersecurity awareness campaigns: Why do they fail to change behaviour? *International Journal of Information Management, 58*, 102280.

Boyes, H. (2021). The cyber security body of knowledge and organisational resilience. *Computers & Security, 105*, 102241.

Crawford, M., & Jabbour, C. (2022). Enterprise risk management and organizational resilience in the digital era. *Journal of Risk Research, 25*(8), 1054–1072.

Ghadge, A., Wei, H., Caldwell, N., & Wilding, R. (2022). Managing cyber risk in supply chains through integrated risk governance. *Supply Chain Management: An International Journal, 27*(4), 531–547.

Greitzer, F. L., & Frincke, D. A. (2021). Combating the insider cyber threat. *IEEE Security & Privacy, 19*(1), 61–64.

Herath, T., & Herath, H. (2020). Coping with cyber threats: Integration of enterprise risk management and information security. *Information Systems Management, 37*(2), 120–134.

Institute of Risk Management. (2022). *Risk appetite and resilience guidance*. IRM.

International Organization for Standardization. (2022). *ISO/IEC 27001: Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. ISO.

International Organization for Standardization. (2022). *ISO 22301: Security and resilience—Business continuity management systems—Requirements*. ISO.

Kaplan, R. S., & Mikes, A. (2021). Risk management: The reinvention of risk management in the digital age. *Harvard Business Review, 99*(3), 48–57.

Kshetri, N. (2021). Cybersecurity management in developing and developed economies. *Journal of Global Information Technology Management, 24*(2), 81–89.

Lundqvist, S. A. (2020). Why firms implement risk governance frameworks. *Risk Management, 22*(2), 121–139.

ISSN: 2971-7760 | VOL 6, ISS 2 | 03 AUGUST 2026
https://doi.org/10.5281/zenodo.21768314
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Mikes, A., & Kaplan, R. S. (2020). Toward a contingency theory of enterprise risk management. *Management Accounting Research, 46*, 100643.

National Institute of Standards and Technology. (2024). *Cybersecurity framework (CSF) 2.0*. U.S. Department of Commerce.

National Institute of Standards and Technology. (2024). *Integrating cybersecurity and enterprise risk management (NISTIR 8286 Rev. 1)*. U.S. Department of Commerce.

National Institute of Standards and Technology. (2024). *Cybersecurity supply chain risk management practices for systems and organizations*. U.S. Department of Commerce.

Nielsen, M., & Madsen, S. (2022). Enterprise risk management and digital resilience: Emerging perspectives. *International Journal of Risk Assessment and Management, 25*(1), 45–62.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2020). Determining employee awareness using cybersecurity culture assessments. *Computers & Security, 94*, 101817.

Reason, J. (2020). Human error and organizational resilience in complex systems. *Safety Science, 130*, 104874.

Scott, W. R. (2022). *Institutions and organizations: Ideas, interests, and identities* (5th ed.). Sage Publications.

Sheffi, Y. (2021). *The new (ab)normal: Reshaping business and supply chain strategy beyond COVID-19*. MIT Press.

United States Government Accountability Office. (2023). *Cybersecurity risk management and oversight*. GAO.

Von Solms, R., & Van Niekerk, J. (2021). From information security to cybersecurity. *Computers & Security, 38*, 97–102.

Yaraghi, N., & Sharman, R. (2021). Enterprise cybersecurity and organizational resilience. *Journal of Cyber Policy, 6*(3), 337–353.