A Conceptual Review of Cyber Risk Management and Business Continuity Planning in The Digital Economy

Abia Lawrence Agi
Department of Accountancy
University of Cross River State
https://doi.org/10.56201/ijebm.vol.12.no9.2026.pg16.23

Abstract
The purpose of the study was to examine cyber risk management and business continuity planning in the digital economy. Cyber risk management has therefore become an important mechanism through which organizations identify, assess and respond to potential cyber threats. Cyber risk management has therefore become an important mechanism through which organizations identify, assess and respond to potential cyber threats. In the digital environment, this capability is particularly important because a cyberattack can simultaneously affect information systems, financial transactions, customer services and internal operations. The study recommended that organizations should establish continuous cyber risk identification and monitoring mechanisms. Management should regularly identify emerging cyber threats, system vulnerabilities, critical digital assets and business processes that could be affected by cyber incidents. Organizations should develop formal and periodic cyber risk assessment procedures. Cyber risks should be evaluated according to their likelihood, potential financial impact, operational consequences and effects on critical business functions. The results should be incorporated directly into business continuity and disaster recovery plans so that resources are concentrated on the organization's most critical risks.

Keywords: *Cyber risk management, business continuity planning, digital economy, cyber risk management, cyberattack*

Introduction

The rapid development of the digital economy has fundamentally changed the way organizations conduct business, interact with customers, store information, and deliver products and services. However, this increasing dependence on digital technologies has also created new vulnerabilities, exposing organizations to cyber threats such as ransomware, phishing, malware, data breaches and system disruptions. According to Bouveret (2020), cyber incidents can generate significant operational and financial consequences because organizations are increasingly interconnected through digital systems. Similarly, Craigen et al. (2022) argue that the growing sophistication and interconnectedness of digital technologies have made cybersecurity an important organizational and strategic concern rather than merely a technical issue. Cyber risk management has therefore become an important mechanism through which organizations identify, assess and respond to potential cyber threats. Aven (2020) explains that effective risk management involves systematic identification and assessment of uncertainties that may affect organizational objectives. In the context of cybersecurity, Tatar et al. (2021) maintain that organizations need to develop proactive approaches that enable them to understand cyber threats and reduce their potential impact before

they result in serious operational disruption. Similarly, Soomro et al. (2022) emphasize that effective cybersecurity practices require organizations to combine technological controls with appropriate managerial processes, policies and employee awareness.

Business continuity planning provides an important complement to cyber risk management because not all cyber incidents can be completely prevented. Herbane (2020) notes that business continuity management enables organizations to prepare for disruptive events and maintain critical operations despite unexpected interruptions. In the digital environment, this capability is particularly important because a cyberattack can simultaneously affect information systems, financial transactions, customer services and internal operations. Ali et al. (2021) further observe that organizational resilience depends substantially on an organization's ability to anticipate disruptions, respond effectively and recover its critical activities within an acceptable period.

The connection between cyber risk management and business continuity planning has consequently become increasingly important in the digital economy. Linkov and Trump (2020) argue that organizational resilience requires an integrated approach to anticipating threats, absorbing disruptions and recovering from adverse events. Similarly, Ganin et al. (2021) demonstrate that resilience-oriented approaches can help organizations understand the relationships between interconnected risks and develop stronger responses to disruptive events. Effective cyber risk management can therefore reduce the probability and severity of cyber incidents, while effective business continuity planning provides the mechanisms required to sustain or restore critical operations when such incidents occur. Against this background, cyber risk management and business continuity planning have become critical determinants of organizational resilience and sustainable performance in the digital economy. Organizations that fail to adequately identify and manage cyber risks may experience operational downtime, financial losses, reputational damage and loss of stakeholder confidence. This study therefore examines the relationship between cyber risk management and business continuity planning in the digital economy, with particular emphasis on how effective management of cyber risks can enhance organizational preparedness, resilience and the continuity of critical business operations.

Theoretical Framework

Dynamic Capabilities Theory, originally developed by Teece et al. (1997) and subsequently developed by Teece (2007, 2018), explains how organizations develop and reconfigure their resources and capabilities to respond to rapidly changing business environments. The theory proposes that organizations must be able to sense opportunities and threats, seize opportunities, and transform or reconfigure their resources in response to environmental changes. The theory is particularly relevant to cyber risk management because the digital economy is characterized by rapidly changing technologies and constantly evolving cyber threats. Teece (2018) argues that organizations operating in dynamic environments require capabilities that enable them to identify changes, make timely decisions and reconfigure organizational resources. In the context of this study, cyber risk identification represents the organisation's ability to sense emerging threats, while cyber risk assessment helps management evaluate the significance of those threats. Cybersecurity risk mitigation represents the organization's ability to deploy appropriate resources and controls, while cyber incident response reflects its ability to rapidly reconfigure resources and respond when a cyber disruption occurs. The theory therefore suggests that organizations with stronger dynamic capabilities should be better positioned to anticipate cyber threats and adjust their technological, human and organizational resources accordingly. This capability can subsequently strengthen business continuity by enabling organizations to maintain or restore critical operations following

cyber incidents. Warner and Wäger (2019) further demonstrate the relevance of dynamic capabilities to digital transformation, arguing that organizations need sensing, seizing and transforming capabilities to remain resilient in rapidly changing digital environments. Dynamic Capabilities Theory is appropriate because cyber threats are dynamic, unpredictable and continuously evolving. Organizations cannot rely solely on existing cybersecurity resources; they must continuously identify new threats, assess vulnerabilities, strengthen protective measures and modify their response capabilities. Teece (2018) supports this perspective by emphasizing the importance of organizational capabilities for adapting to rapidly changing environments.

Organizational Resilience Theory

Organizational Resilience Theory provides a second important foundation for the study. The theory focuses on an organization's capacity to anticipate, withstand, respond to and recover from disruptive events while maintaining essential functions. Duchek (2020) conceptualizes organizational resilience as a meta-capability involving three major stages: anticipation, coping and adaptation. This perspective is particularly applicable to business continuity planning because continuity planning is fundamentally concerned with ensuring that organizations can continue essential operations during and after disruptive events. In relation to this study, cyber risk identification and cyber risk assessment correspond strongly with the anticipation dimension of organizational resilience. Organizations must understand potential threats and evaluate their possible consequences before disruption occurs. Cybersecurity risk mitigation contributes to the coping dimension by reducing the severity of cyber incidents and enabling organizations to absorb disruptions. Similarly, cyber incident response supports the coping and adaptation dimensions by enabling organisations to respond quickly, recover affected systems and learn from cyber incidents. Hillmann and Guenther (2021) emphasize that organizational resilience involves the ability to maintain functionality and adapt in the face of unexpected changes. From this perspective, business continuity planning is not simply a collection of recovery procedures; it represents an organizational capability that supports preparedness, response and recovery. This makes Organizational Resilience Theory highly appropriate for explaining the dependent variable of the study. Organizational Resilience Theory is equally appropriate because the ultimate concern of business continuity planning is not simply preventing disruption but ensuring that the organization can continue critical activities, respond effectively and recover quickly when disruption occurs. Duchek (2020) provides a particularly strong foundation because her anticipation–coping–adaptation framework closely corresponds with the processes involved in cyber risk management and business continuity.

Cyber Risk Management

Cyber risk management refers to the systematic process through which organizations identify, assess, control and respond to risks arising from the use of digital technologies and interconnected information systems. As organizations increasingly depend on digital platforms for their daily operations, cyber risks have moved beyond the traditional information technology function and become an important component of organizational risk management. Aven (2020) explains that effective risk management requires organizations to systematically understand sources of uncertainty and their possible consequences for organizational objectives. In the cybersecurity context, Bouveret (2020) similarly argues that cyber risk can generate significant operational and financial consequences, making proactive risk management necessary for organizations operating in increasingly digital environments. Cyber risk management is particularly relevant to business continuity because cyber incidents can interrupt critical organizational processes. Herbane (2020)

argues that organizational resilience depends on the capacity of organizations to anticipate disruptions, respond to them and recover essential operations. Consequently, cyber risk management should not be limited to preventing attacks but should also prepare organisations for situations where security controls fail. The major dimensions considered in this study are cyber risk identification, cyber risk assessment, cybersecurity risk mitigation and cyber incident response.

Cyber Risk Identification and Business Continuity Planning

Cyber risk identification involves the systematic process of recognising potential cyber threats, vulnerabilities, assets and activities that could disrupt organizational operations. It provides the foundation for effective cyber risk management because an organization cannot adequately manage a risk that it has failed to recognize. Aven (2020) maintains that risk identification is an essential stage of risk analysis because it enables organizations to understand possible sources of adverse outcomes. Similarly, Soomro et al. (2022) emphasise that information security requires organizations to understand their technological vulnerabilities, organizational weaknesses and human-related security risks. In relation to business continuity planning, effective cyber risk identification enables organizations to determine which digital assets and business processes are most vulnerable to disruption. Herbane (2020) notes that organizations become more resilient when they are capable of anticipating potential sources of disruption rather than responding only after an event has occurred. When cyber threats are properly identified, organizations can incorporate relevant scenarios into their continuity plans, establish appropriate recovery priorities and allocate resources to critical functions. Cyber risk identification can therefore strengthen business continuity planning by providing information required for developing realistic disruption scenarios. Organisations that continuously monitor emerging cyber threats, identify vulnerabilities and understand their critical digital assets are better positioned to develop appropriate continuity strategies. Linkov and Trump (2020) similarly emphasise that resilience requires organisations to anticipate potential threats and understand the vulnerabilities that may affect their ability to maintain essential functions.

Cyber Risk Assessment and Business Continuity Planning

Cyber risk assessment involves analyzing identified cyber risks in terms of their likelihood, potential consequences and significance to organizational objectives. It enables management to distinguish between risks that require immediate attention and those that can be managed through routine controls. According to Aven (2020), risk assessment provides a basis for making informed decisions concerning the treatment and prioritization of risks. In the digital economy, such assessment is particularly important because organizations face multiple and interconnected cyber threats. The relationship between cyber risk assessment and business continuity planning arises from the need to prioritise critical business activities and determine the consequences of potential disruptions. Bouveret (2020) observes that cyber incidents can produce substantial financial and operational effects, suggesting that organisations need to evaluate the potential consequences of cyber events rather than merely identifying their existence. Proper cyber risk assessment can therefore help organizations estimate potential downtime, financial losses, data compromise and service interruptions. Furthermore, Ganin et al. (2021) demonstrate that organisational resilience is multidimensional and requires an understanding of how disruptions can affect interconnected organizational systems. This implies that cyber risk assessment should consider not only individual information systems but also the wider effects of their failure on customers, employees, suppliers

and other critical stakeholders. Effective assessment can consequently help organisations establish appropriate recovery priorities and strengthen business continuity planning.

Cybersecurity Risk Mitigation and Business Continuity Planning

Cybersecurity risk mitigation refers to measures designed to prevent, reduce or control the likelihood and consequences of cyber incidents. These measures may include access controls, data protection, network security, employee cybersecurity awareness, authentication mechanisms, regular system updates and security monitoring. Soomro et al. (2022) argue that information security requires a holistic approach involving technological, organizational and human dimensions rather than dependence on technology alone. The importance of risk mitigation to business continuity lies in its ability to reduce the severity of disruptions when cyber incidents occur. Effective preventive and protective measures can reduce system vulnerabilities and limit the extent to which an attack affects critical business functions. Tatar et al. (2021) emphasise the importance of combining cybersecurity capabilities with organizational resilience so that organizations are capable not only of protecting their systems but also of maintaining operations when disruptions occur. Similarly, Herbane (2020) suggests that resilience-oriented organizations require preventive and adaptive capabilities that enable them to withstand disruptive events. From this perspective, cybersecurity risk mitigation forms an important part of business continuity planning because effective controls can reduce the probability of operational interruption and improve an organisation's capacity to continue delivering essential services.

Cyber Incident Response and Business Continuity Planning

Cyber incident response refers to the processes and procedures used by an organisation to detect, contain, investigate and recover from cybersecurity incidents. It represents the reactive component of cyber risk management and becomes particularly important when preventive controls fail. Tatar et al. (2021) argue that cyber resilience requires organisations to develop capabilities for responding to and recovering from cyber incidents rather than focusing exclusively on prevention. Effective incident response can contribute significantly to business continuity because delays in responding to cyber incidents can increase operational disruption and financial losses. Bouveret (2020) highlights the potential economic consequences of cyber incidents, reinforcing the need for organizations to establish mechanisms for rapid detection and response. A well-designed incident response process can enable an organization to isolate affected systems, protect critical data, communicate with relevant stakeholders and restore essential services. Linkov and Trump (2020) further explain that organizational resilience involves the capacity to absorb disruption, adapt to changing conditions and recover from adverse events. Consequently, cyber incident response should be integrated into business continuity plans rather than treated as a separate technical activity. Organizations with clearly defined response responsibilities, communication channels, escalation procedures and recovery arrangements are more likely to maintain critical operations during cyber disruptions.

Empirical Review

Empirical evidence on cyber risk management and organizational continuity has continued to demonstrate that the growing dependence on digital technologies creates both opportunities and significant risks for organizations. Tetteh and Otioma (2025), using data from the 2016 Enterprise ICT Survey of Kenya, examined the effect of cybersecurity breaches on firm productivity and the moderating role of cyber risk mitigation capabilities. The researchers employed Principal

Component Analysis to construct measures of cyber risk mitigation capabilities and used Ordinary Least Squares regression alongside a simultaneous equation approach to address endogeneity. The findings revealed that cybersecurity breaches significantly reduce firm-level labour productivity, while employee upskilling helps to mitigate the negative effects of cyberattacks, particularly among small and medium-sized enterprises. The study further established that IT policy and IT security capabilities can improve productivity, although they may not be sufficient on their own to completely offset the consequences of cyberattacks. These findings demonstrate the importance of cybersecurity risk mitigation in reducing the operational consequences of cyber threats and provide useful evidence for the present study.

Closely related to this, Gaudenzi and Baldi (2024) empirically examined cyber resilience in organizations and supply chains, focusing on managers' perceptions of cyber risks, the adoption of cyber-resilience strategies and the perceived effectiveness of those strategies. Using primary data collected through a survey of Italian organizations, the researchers applied structural equation modelling to examine the relationships among cyber-risk perceptions, resilience strategies and their effectiveness. Their findings showed that awareness of the negative consequences of cyber risks, particularly business and supply-chain disruptions, encourages organizations to adopt cyber-resilience strategies. The study further demonstrated that proactive evaluation of cyber risks and the adoption of appropriate mitigation strategies can contribute to stronger cyber resilience. This finding supports the argument that cyber risk identification and cyber risk assessment are important foundations for effective organizational continuity, because organizations must first understand their exposure and potential consequences before developing appropriate responses.

The importance of understanding cyber risks before developing response strategies is further reinforced by the findings of Gaudenzi and Baldi (2024), who emphasised that cyber-risk awareness is a necessary condition for adopting a multifunctional portfolio of cyber-resilience strategies. Their study moved beyond traditional approaches that focus largely on technical security measures and demonstrated the importance of considering the potential consequences of cyber risks across organizational processes and supply chains. This perspective is particularly relevant to the present study because cyber risk identification and assessment should not be restricted to information technology departments but should form part of broader organisational planning. When organizations understand the risks associated with critical digital processes, they are better positioned to determine appropriate mitigation measures and incorporate potential cyber disruptions into their continuity arrangements.

The issue of responding effectively after a cyber incident has also received empirical attention. A 2023 study published in Computers & Security investigated how big-data-analytics-enabled dynamic capabilities can facilitate agile cybersecurity incident response. Using a field-study case approach and drawing on Dynamic Capabilities Theory, the study examined the dimensions of dynamic capabilities that enable organizations to respond more rapidly to diverse cybersecurity threats. The findings emphasized the importance of agility in incident response and showed that big-data analytics can contribute to more effective and timely responses to cybersecurity incidents. This evidence is important to the present study because cyber incident response represents the point at which an organization’s preparedness is translated into practical action following a cyber disruption. The study therefore suggests that organizations need more than preventive controls; they also require the capabilities to detect, contain and respond quickly when cyber incidents occur.

Taken together, the findings of these empirical studies suggest that cyber risk management and organizational continuity are closely connected. Tetteh and Otioma (2025) established that cyberattacks can reduce organizational productivity and that mitigation capabilities, particularly

employee upskilling, can reduce their adverse effects. Gaudenzi and Baldi (2024), on the other hand, demonstrated that awareness and evaluation of cyber risks can encourage organisations to adopt resilience strategies, while the 2023 study on agile cybersecurity incident response showed that dynamic capabilities and data-driven technologies can improve organizational responses to cyber incidents. Collectively, these findings indicate that organizations need to identify cyber risks, assess their potential consequences, implement appropriate mitigation measures and develop effective incident-response capabilities if they are to maintain critical operations during digital disruptions. However, an important gap remains in the existing empirical literature. Most previous studies have concentrated on individual aspects of cybersecurity, such as cyberattacks, mitigation capabilities, cyber resilience or incident response, while relatively limited empirical attention has been given to the combined effect of cyber risk identification, cyber risk assessment, cybersecurity risk mitigation and cyber incident response on business continuity planning. Furthermore, much of the available evidence comes from Kenya, Italy and other international contexts, creating a contextual gap regarding organizations operating within the Nigerian digital economy. The present study therefore extends existing knowledge by examining how these four dimensions of cyber risk management influence business continuity planning, thereby providing a more integrated explanation of how organizations can prepare for, respond to and recover from cyber-related disruptions.

Conclusion

Cyber risk management has therefore become an important mechanism through which organizations identify, assess and respond to potential cyber threats. In the context of cybersecurity, organizations need to develop proactive approaches that enable them to understand cyber threats and reduce their potential impact before they result in serious operational disruption. In the digital environment, this capability is particularly important because a cyberattack can simultaneously affect information systems, financial transactions, customer services and internal operations.

Recommendations

1. Organisations should establish continuous cyber risk identification and monitoring mechanisms. Management should regularly identify emerging cyber threats, system vulnerabilities, critical digital assets and business processes that could be affected by cyber incidents. Periodic vulnerability assessments and employee reporting mechanisms should also be encouraged so that emerging risks can be detected before they develop into major disruptions.
2. Organizations should develop formal and periodic cyber risk assessment procedures. Cyber risks should be evaluated according to their likelihood, potential financial impact, operational consequences and effects on critical business functions. The results should be incorporated directly into business continuity and disaster recovery plans so that resources are concentrated on the organisation's most critical risks.
3. Organizations should strengthen their preventive and protective cybersecurity controls. Management should invest in appropriate security technologies, access controls, data backup systems, multi-factor authentication, employee cybersecurity training and regular software updates. These measures should be reviewed periodically to ensure that they remain effective against changing cyber threats.

References

Aven, T. (2020). *The science of risk analysis: Foundation and practice*. Routledge.

Bouveret, A. (2020). Cyber risk for the financial sector: A framework for quantitative assessment. IMF Working Paper, 2020(143), 1–40.

Duchek, S. (2020). Organizational resilience: A capability-based conceptualization. *Business Research,* 13, 215–246.

Ganin, A. A., Quach, L., Panwar, M., Etter, D., Stanley, K., Kott, A., & Linkov, I. (2021). Multidimensional resilience: A quantitative approach to assessment. Nature Communications, 11, 531.

Gaudenzi, B., & Baldi, B. (2024). Cyber resilience in organisations and supply chains: From perceptions to actions. *The International Journal of Logistics Management, 35*(7), 99–122. https://doi.org/10.1108/IJLM-09-2023-0372

Herbane, B. (2020). Rethinking organizational resilience and strategic renewal in SMEs. *Entrepreneurship & Regional Development, 32*(7–8), 620–635.

Hillmann, J., & Guenther, E. (2021). Organizational resilience: A valuable construct for management research? *International Journal of Management Reviews, 23*(1), 7–44.

Linkov, I., & Trump, B. D. (2020). *The science and practice of resilience.* Springer.

Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., & Siddiqui, A. M. (2023). Moving towards agile cybersecurity incident response: A case study exploring the enabling role of big data analytics-embedded dynamic capabilities. Computers & Security, 135, 103525. https://doi.org/10.1016/j.cose.2023.103525

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2022). Information security management needs more holistic approach: A literature review. *International Journal of Information Management,* 45, 215–225.

Tatar, U., Gheorghe, A. V., & Kuchar, J. (2021). *Cybersecurity and cyber resilience: Concepts, methods and practices.* Springer.

Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of sustainable enterprise performance. *Strategic Management Journal, 28*(13), 1319–1350.

Teece, D. J. (2018). Business models and dynamic capabilities. *Long Range Planning, 51*(1), 40–49.

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal, 18*(7), 509–533.

Tetteh, G. K., & Otioma, C. (2025). Cyberattack, cyber risk mitigation capabilities, and firm productivity in Kenya. *Small Business Economics, 64*(3), 1493–1514. https://doi.org/10.1007/s11187-024-00946-8

Warner, K. S. R., & Wäger, M. (2019). Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal. *Long Range Planning, 52*(3), 326–349.