# Integrating Cybersecurity Risk Management and Business Continuity of Family-Owned Businesses in Anambra State, Nigeria: A Conceptual Model

**Chinwe Gloria Obananya[1], Paschal Anosike[2] and Chidimma Odira Okeke [1]**
[1]Chukwuemeka Odumegwu Ojukwu University, Anambra State, Nigeria
[2]University of West England, UK

cg.obananya@coou.edu.ng
paschal.anosike@uwe.ac.uk
oc.okeke@coou.edu.ng

**Abstract:** With the growing dependence on digital technologies and integrated systems, the contemporary business environment is becoming more susceptible to cyber threats, especially family-owned businesses which in most cases have loosely organized cybersecurity systems. Family-owned businesses in the Anambra State of Nigeria contribute to economic growth in the country, however, family-owned businesses in the developing economies are the most vulnerable to cyber-attacks and most times they operate informal structures which are not well equipped to survive external cyber threats. Affirming business continuity theory and protection motivation theory, cybersecurity risk management ensures business detects, evaluates, and reduce possible threats while maintain operations during and after disruptions. Thus, this study is an effort to propose a cyber-resilience integration model to help family-owned businesses incorporate cybersecurity risk management into structures of business continuity and core strategy of organizational survival. With direct synthesis of relevant literature, this study postulates how cybersecurity risk management can be applied to business continuity planning amongst family-owned enterprises. In specific, it delineates risk identification, threat assessment, and incident response planning and recovery strategies contribution to business continuity of family owned enterprises. This paper offers useful information to business owners, policymakers, and researchers because it offered a guide to enhancing the preparedness of cybersecurity and the need to maintain sustainable business operations. This contribution is an important move towards making the family-owned businesses within emerging economies to be more resilient.

**Keywords:** SME cybersecurity, Business continuity, Conceptual model, Family business resilience, Cybersecurity risk management

## 1. Introduction

With the rate information and communication technology (ICT) continues to advance, the fundamentals of business operations in the whole world have continued to evolve, where organisations can now enhance efficiency, customer interaction and market penetration in the speed of light. As cited by the International Telecommunication Union (2023), this augmented reliance on digital frameworks have unleashed companies to a large disparate cybersecurity challenges that comprise information breaches, malware attacks, phishing attacks, ransomware and unlawful access to confidential data. Unfortunately, these cyber threats are increasingly becoming sophisticated and common, with the risk to organizational continuity and economic stability being seriously affected. Also, World Economic Forum (2022) informed us that cyber-attacks are among the most prominent risks to business organizations worldwide because of their ability to destabilize business activities and lead to massive financial damages. These trends highlighted the increasing need to consider cybersecurity as a central aspect of business management.

Small and medium enterprises (SMEs) particularly in Anambra State and Nigeria in general, have strong presence of family-owned businesses as their entrepreneurial activities are well embedded in their socio-economic life and cultural belief. These businesses play a significant role in job creation and economic growth however, majority of these SMEs usually have informal or semi-formal operational structures and technological deficit which makes them very susceptible to computer predators. According to Akinola and Akinyele (2023); Ogunleye and Adeoye (2022), they opined that most SMEs in Nigeria do not have written cybersecurity practice guide and risk management systems; hence they remain more vulnerable to cyber threats and cybercrimes. These attacks can be traced to lack of awareness and sufficient investment in cybersecurity infrastructure by small businesses is a major setback to their capabilities to protect digital assets and ensure a stable operation (National Information Technology Development Agency, 2021).

Due to the growing uncertainties, business continuity management has been introduced as a strategic tool of ensuring that organizations are capable of preserving important operations during the incident and beyond the event of disrupted occurrences. Conventionally, business continuity models tend to cover physical risks to the

business like natural calamities and operations malfunction, but the computerization of the business process has led to the need to revise the approach to include cybersecurity risks. As ISO 22301 (2019) postulated, to have an effective business continuity planning, it is pertinent to adopt the risk management approach that has the cyber threats as its component. Research by Adams and Yusuf (2021); Eze and Chukwu (2023) were of the view that the implementation of cybersecurity risk management into business continuity models strengthens organization resiliency, increases their incident management capabilities and minimizes the period of downtime during cyber-related outages. Such integration is especially necessary in the current digital economy whereby cyber incidents are likely to paralyze business operations in a few days.

However, the efficacy of these cybersecurity practices may largely depend on organizational factors, specifically leadership ICT awareness. Leadership ICT awareness refers to the degree to which business proprietors and top executives comprehend, increase in value, and support the practice of information and communication technologies and cybersecurity strategies within the organization. In most family-owned businesses, decision-making is consolidated around the business owner or executives representing the family whose awareness and perception of ICT risks significantly affect organizational investment in cybersecurity. Leaders with high ICT awareness are more likely to prioritize cybersecurity compliance, invest in digital protection systems, cybersecurity training, and enforce innovation-driven resilience strategies. Although previous studies have examined cybersecurity adoption and business continuity separately (Nwafor & Ijeoma, 2022), limited empirical research has explored how leadership ICT awareness mediates the relationship between cybersecurity management practices and business continuity outcomes among family-owned businesses in Anambra State, Nigeria. This study therefore has developed a conceptual model explaining this relationship.

## 2. Conceptual Background

### 2.1 Exposition of Cybersecurity Risk Management Practices

Cybersecurity management practice is defined as a strategic-level capability of an organization to protect their information technology systems, digital processes and information resources within an evolving cyber-threat environment (Rajan *et al.,* 2021). Effective cybersecurity management practice ensures that an organization protects the integrity, confidentiality and availability of its information through legal, administrative, and managerial control (Ye, 2026). It involves developing policies and practices that can ensure the mitigation of risks related to information systems and digital resources (Adam & Yusuf, 2021).

Research on organizational cybersecurity management, described efficient cybersecurity practice to involve employee awareness training, cyber-threat risk assessment process, incident response planning, cyber access control mechanism, continuous monitor of digital systems, and information governance (Rajan *et al.,* 2021). Also, scholars have argued that cybersecurity has moved from just a technical practice to a more strategic responsibility of organization which needs the required managerial support, leadership commitment and organizational support (Nwafor & Ijeoma, 2022; Akinola & Akinyele, 2023; Junior *et al.,* 2023; Ye, 2026). These practices allow organization to be prepared in order to mitigate weakness expose to operational disruption and reputational damage that manifest through cyber-threats and attacks.

### 2.2 Description of Business Continuity Outcomes Management

Business continuity sometimes referred to as business continuance can be defined as the capacity of an organization to put in place processes and procedures to make sure that critical function can continue during and after disaster at acceptable predefined levels following the disruptive incident (Olubiyi *et al*., 2022). Business continuity management comprises organizational planning, preparedness, crisis response apparatus, disaster-recovery systems, and building resilience tactics designed at sustaining organizational functionality under adverse conditions (Ali *et al*., 2023; Russo *et al*., 2024).

Business continuity outcome management can also be described to encompass adaptive resilience, organizational flexibility, proactive learning, and knowledge preservation (Ali *et al.,* 2023) because it serves as antidote for quick recovery from disruption and long term performance sustainability. In the context of family-owned business, continuity management goes further than operational survival to include generational sustainability, succession continuity, and preservation of family legacy (Olubiyi *et al*., 2022).

### 2.3 Exposition of Leadership ICT Awareness

Leadership ICT awareness is defined as the degree to which administrative leaders appreciate, comprehend, and strategically apply information and communication technologies (ICTs) for organizational value,

innovativeness, security, and sustainability (Vrhovec & Markeli, 2024). Leadership ICT awareness is progressively accepted as a strategic competence that impacts organizational readiness for cyber-risk management and digital transformation and leaders who possessed this awareness are more probable to sustain investments in innovation systems, cybersecurity infrastructure, employee training, and business continuity planning (Russo et al*,* 2024).

Literature opined that ICT-aware leaders are catalyst that can enhance organizational adaptability and crisis readiness (Russo *et al*., 2024) and they have better capacity to identify digital vulnerabilities, thereby integrate cybersecurity into strategic plan that will promote digital resilience throughout organizational structure (Rajan *et al*., 2021). Within the context of family-owned businesses, leadership ICT awareness is principally imperative because decisions are often determined by family members who might possess different degrees of technological competency (Nwuke & Adeola, 2023) and the nonappearance of ICT awareness by family business leaders can hinder cybersecurity readiness, innovation adoption, and digital transformation (Nwuke & Adeola, 2023; Oriazowanlan & Ekenam, 2024). Conversely, leadership that is technologically informed facilitates healthier risk management process, knowledge transmission, and continuity planning.

### 2.4 Description of Family-owned Business

Family-owned businesses can be described as business enterprise owned, managed, and organized by the same family members, often with the intent to transfer ownership and management from one generation to another generation. Family-owned businesses make-up a considerable percentage of businesses globally and contribute significantly to wealth creation, economic development, and employment generation (Olubiyi *et al*., 2022). In Nigeria, family-owned businesses dominate the SME sector and play important roles in economic sustainability (Olubiyi *et al*., 2019).

Studies on leadership transition in Nigerian family-owned SMEs reveal that ineffective succession processes, poor mentoring culture, and lack of managerial competence often threaten long-term survival and effective succession planning therefore enhances continuity, stability, and organizational sustainability (Nwuke & Adeola, 2022). Additionally, knowledge management has been identified as a major factor supporting continuity in family businesses (Olubiyi *et al*., 2019). Knowledge sharing, mentoring, and transfer of managerial expertise strengthen organizational resilience and improve survival across generations (Oriazowanlan *et al*., 2024). In recent years, digital transformation has emerged as another important factor influencing family business sustainability and family-owned firms that integrate ICT systems, cybersecurity management practices, and innovation strategies tend to demonstrate greater resilience and competitiveness than those relying solely on traditional operational models (Ali *et al*., 2023).

## 3. Conceptual Model to Explicate Cyber Resilience Integration Model (CRIM), Cybersecurity Risk Management Integration, Business Continuity Outcomes, and Leadership ICT Awareness

### 3.1 Cyber Resilience Integration Model (CRIM)

Cyber Resilience Integration Model (CRIM) framework is an outline that was developed to incorporate cybersecurity risk management as a part of business continuity procedures in family-owned businesses. It was conceptualized on the basis of the Nation Institute of Standards and Technology Framework of Cybersecurity and the ISO 22301 International Organization Standards. The CRIM in Fig. 1 was adapted to fit the reality of small medium enterprises and family-owned businesses. The CRIM is comprised of three main elements namely cybersecurity risk identification, business continuity planning and the ability of an organization to respond to it. These aspects combined together guarantee that cyber threats are perceived as essential business risks and are addressed in a systematic way to guarantee business continuity. CRIM also integrates a continuous feedback mechanism to monitor, evaluate and improve cyber resilience processes so that businesses can keep pace with changing cyber threats. It can be progressed into varying degrees Basic, Intermediate and Advanced depending on the technological capability and resources of the organization. Technical, human and managerial conditions such as awareness of all the employees and commitment of the leadership all form the components of CRIM to be used as the holistic approach to resilience which is why it is specifically used to provide the sustainability and overall performance of the family-owned business in the dynamic environments like the Anambra State, Nigeria.

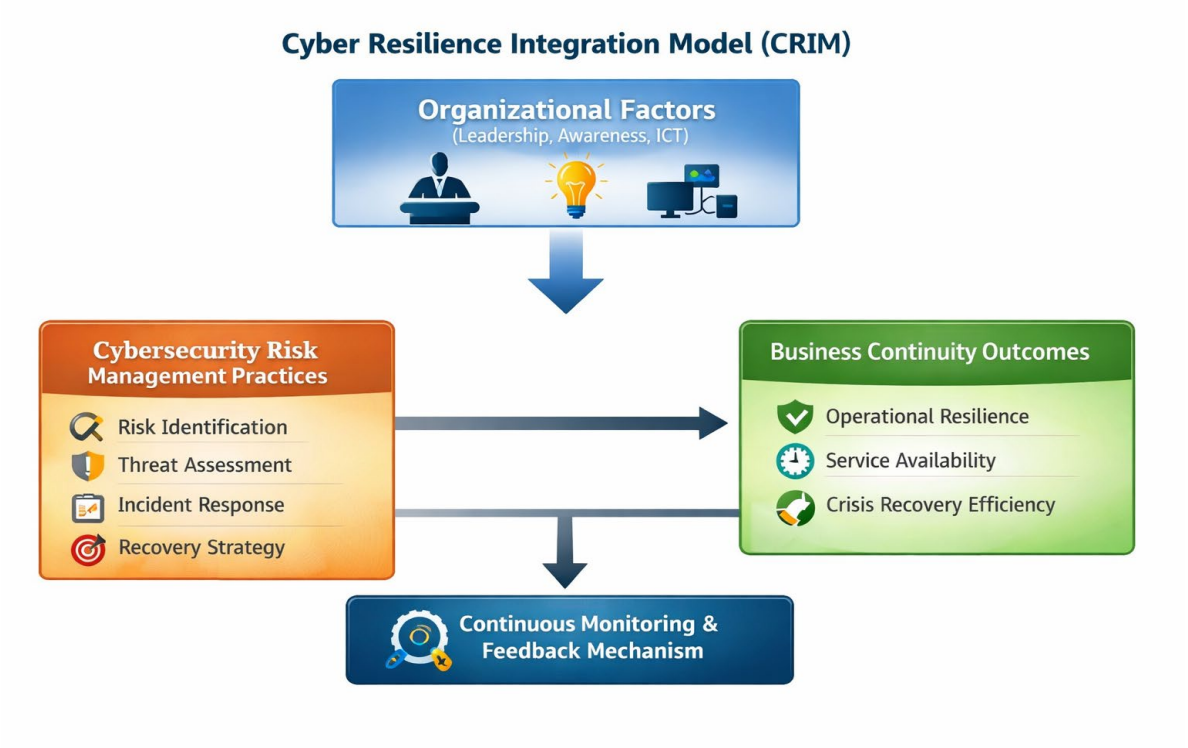


**Figure 1: CRIM conceptual model integrating cybersecurity risk management practices, leadership ICT awareness, and business continuity outcomes with a continuous monitoring and feedback mechanism**

The cyber resilience integration model (CRIM) in Fig.1 revealed how the practices of cybersecurity risk management play the most dominant role in business continuity outcomes, and organizational factor – leadership ICT awareness is the mediator variable that either makes or breaks the business continuity outcomes. The integrated monitoring and feedback control mechanism keeps the model agile to new cyber threats. This comprehensive CRIM illustrated how technical cybersecurity efforts with organizational preparedness strengthen the resilience, increase access to services and foster effective recovery in family-owned enterprises.

**Table 1: Components of the Cyber Resilience Integration Model (CRIM)**

| Component | Description | Key Elements | Expected Outcome |
|---|---|---|---|
| **Cybersecurity risk management practice** | Focuses on detecting and evaluating cyber threats affecting business operations | Threat monitoring, vulnerability assessment, risk analysis | Early detection of cyber risks and reduced exposure |
| **Business continuity planning** | Integrates cybersecurity into continuity strategies to ensure uninterrupted operations | Disaster recovery plans, data backup, incident response planning | Sustained operations during disruptions |
| **Organizational leadership ICT awareness and response capability** | Emphasizes human and managerial readiness in handling cyber incidents | Staff training, leadership commitment, communication systems | Improved crisis response and faster recovery |

The Cyber Resilience Integration Model (CRIM), as seen in Table 1, indicates how the framework of business continuity integrates cybersecurity risk management. The model focuses on a rational connection between the identification of cyber risks, disruption planning and the capacity building of the organization to recover successfully. Every element can help improve its operational resilience and the sustainability of the business.

### 3.2 Cybersecurity Risk Management Integration

The idea of incorporating the concept of cybersecurity risk management (CRM) into the organizational operations has turned out to be a measure to mitigate the threat and securing the digital resources (Adams and Yusuf, 2021). The purpose of this integration is to identify, evaluate, and rank risks in a systematic manner

and put controls in place to mitigate possible effects on operations. In particular, the NIST Cybersecurity Framework, the ISO/IEC 27001, and COBIT frameworks are widely used to help organizations enhance alignment between cybersecurity and business practices (Kraemer et al., 2020; AlHogail, 2021). Research has revealed that the integration of cybersecurity into enterprise governance facilitates proactive identification and management of threats. As an illustration, predictive analytics, and real-time tracking methods are being used as risk assessment tools to identify vulnerabilities and prevent cases of exploitation (Nguyen et al., 2022; Balantrapu, 2024). Also, patterns of network traffic, anomalies flagging, and predicting potential attack vectors have also been analyzed using machine learning models, which has led to an improvement in situational awareness (Patel and Kumar, 2022). These strategies have decreased the use of reactive strategies, and thus organizations have had more effective tools to use to prevent rectificatory actions.

The most significant benefit of integrating cybersecurity is the comprehensive coordination between cybersecurity policies and the business continuity planning as a whole. Integrating cybersecurity risk assessment into continuity frameworks will help organizations to avoid major disruptions brought about by malware, ransomware, or insider threats that can cripple the core functions (Smith et al., 2021; Chen et al., 2023). In addition, integration facilitates security awareness culture among all organizational levels, exposing collaborations among IT, risk management, and the top leadership of the organization. Regardless of these developments several obstacles still exist, such as the scarcity of resources, the ever-changing facet of cyber threats and the challenges of implementing CRM into the existing business processes (AlHogail, 2021; Kraemer et al., 2020). To remain resilient, small and medium enterprises and family owned organizations have to constantly revise their risk management procedures, invest in training of their staff, and use automation technologies. Future studies venture towards adaptive CRM framework that synthesizes AI-monitored predictive and organizational agility to offer scalable real-time security against the emerging cybersecurity threats. Based on the above, the following proposition is suggested:

*P1a: Cybersecurity risk identification practices is a positive factor which impacts the business continuity outcomes of family-owned businesses*

*P1b: Cybersecurity threat assessment practices is a positive factor which impacts the business continuity outcomes of family-owned businesses*

*P1c: Cybersecurity incident response practices is a positive factor which impacts the business continuity outcomes of family-owned businesses*

*P1d: Cybersecurity recovery strategy practices is a positive factor which impacts the business continuity outcomes of family-owned businesses*

### 3.3 Organizational Factors - Leadership ICT Awareness

Leadership ICT awareness refers to the extent to which organizational leaders understand, appreciate, and support information and communication technology (ICT) systems, digital innovation, cybersecurity issues, and technology-driven organizational processes. Leadership ICT awareness involves knowledge of emerging technologies; understanding of cybersecurity risks; appreciation of digital transformation; support for ICT investment; technology-driven strategic decision-making; promotion of digital culture within organizations.

Leadership awareness significantly influences organizational technology adoption and cybersecurity readiness. Leaders who possess strong ICT awareness are more likely to allocate resources toward cybersecurity infrastructure, employee digital training, business continuity planning, and innovation. In contrast, leaders with low ICT awareness may underestimate cyber risks, delay technological investments, or fail to establish appropriate cybersecurity governance structures. In family-owned businesses, leadership ICT awareness is especially critical because leadership decisions are often centralized within family members who may rely on traditional management approaches. In many cases, generational differences also influence ICT awareness levels. Younger generations in family businesses may demonstrate greater digital orientation than older founders or owners. Studies suggest that leadership ICT awareness contributes positively to organizational resilience, digital adaptability, and business continuity preparedness. Based on the above, the following proposition is suggested:

*P2a: The higher the level of leadership ICT awareness of executives, the more likely family-owned businesses will be more proactive business operational resilience*

*P2b: The higher the level of leadership ICT awareness of executives, the more likely family-owned businesses will be more proactive business service availability*

*P2c: The higher the level of leadership ICT awareness of executives, the more likely family-owned businesses will be more proactive business crisis recovery efficiency*

## 4. Limitations

The use of the Cyber Resilience Integration Model (CRIM) in the study is prone to various limitations, especially to family owned businesses in Anambra State. One constraint is associated with the informal nature and low technological capacity of most family-owned businesses. They are not in line with large organizations where cybersecurity infrastructures have been thoroughly built, but these businesses usually do not have any standardized procedures, trained staff, or finances to employ complex cybersecurity and business continuity models. This limitation can have an impact concerning the level of implementation of cybersecurity risk management training like risk threat assessment, incident response planning, and recovery measures, and hence impact the performance of the model in general.

Moreover, integrating the cybersecurity risk management into the business continuity frameworks has practical challenges that are complex. The model presupposes a certain degree of equality between organizational aspects, cybersecurity practices and continuity outcomes which might not be the case in reality. Implementation inconsistency may arise due to variations in the size of business, industry type, and maturity of digital. There are external factors also like regulatory environment, technology infrastructure, and the socio-economic conditions that can also affect effectiveness of the integration, but not completely reflected in the model.

Lastly, there is also an upper limit in quantifying the effect of cybersecurity integration on business continuity outcomes, just as it is in the case of empirical models. Some of these interruptions, especially those that involve complex attacks by the cyber community or other systemic awareness, might be unpreventable irrespective of the degree of readiness. That points at fundamental limitations of the model and the necessity to continuously advance it, better data gathering techniques, and create frameworks that are more context-sensitive when it comes to small and family-owned businesses.

## 5. Conclusion

In this paper, the Cyber Resilience Integration Model (CRIM) was proposed as a systematic approach to manifesting the management of cybersecurity risk in business continuity regimes among family-owned enterprises in Nigeria, Anambra State. Introducing vital elements like risk identification, threat assessment, planning incident response, and recovery strategies along with organizational elements such as leadership ICT awareness and employee awareness, the model offers an overall approach to boosting operational resilience. This method helped to even further explicate the relationships between cybersecurity management practices and the business continuity, providing useful information about the ways in which integrated strategies could enhance service availability and efficiency of crisis recovery.

The conceptualized postulations highlighted the paramount necessity to integrate cybersecurity factors in business continuity plans, especially among the segments of small and family-owned businesses that are more vulnerable to cyber threats. Even though the model has good potential on enhancing organizational resilience, other challenges identified during the review of the study include limited resources, insufficiency of technical skills and a dynamic cyber threat. Future studies are needed to come up with more adaptive and scalable models, include longitudinal data, and the capacity-building efforts are to be improved. On the whole, the current paper is relevant to the existing literature on cybersecurity management and business continuity as it offers a valuable conceptual model to enhance the stability and competitiveness of family-owned businesses operating in new economies.

**Ethics and AI Declaration:** This research did not include sensitive data/information that needs approval from any institutional review board (IRB). The authors affirm that AI tool, which include ChatGPT from OpenAI, were only used specifically to edit language and enhance the manuscript clarity of expression. The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

## References

Adams, T., & Yusuf, A. (2021). Cybersecurity risk management in modern organizations: Strategies and best practices. Journal of Information Security, 12(3), 45–60.

Akinola, O., & Akinyele, S. (2023). Digital risk management and SME performance in Nigeria. African Journal of Business Management, 17(4), 112–125.

AlHogail, A. (2021). Integrating cybersecurity frameworks in enterprise risk management. International Journal of Cybersecurity and Digital Forensics, 10(2), 101–115.

Ali, A., & Kumar, S. (2018). Advances in file recovery techniques for digital forensics. Springer.

Ali, Q. S. A., Hanafiah, M. H., & Mogindol, S. H. (2023). Systematic literature review of Business Continuity Management (BCM) practices: Integrating organisational resilience and performance in Small and medium enterprises (SMEs) BCM framework. International Journal of Disaster Risk Reduction, 99, 104135.

Balantrapu, R. (2024). Cyber resilience in modern organizations: Integrating security with business continuity. Journal of Information Security, 15(2), 45–60.

Chen, L., Zhang, H., & Li, Y. (2023). AI-enabled risk management for cybersecurity: Predictive monitoring and threat mitigation. International Journal of Business Continuity and Risk Management, 14(1), 12–28.

Dauda, A. (2013) Business Continuity and Challenge of Succession in Nigeria: What Happens When the CEO Leaves? Journal of Business and Management, 8, 59-65. https://doi.org/10.9790/487X-0845965

Eze, P., & Chukwu, B. (2023). Cyber risk integration and business continuity planning in emerging markets. International Journal of Management Sciences, 11(1), 67–82.

Herbane, B. (2010). Small business research: Time for a crisis-based view. International Small Business Journal, 28(1), 43–64.

Hiles, A. (2020). The definitive handbook of business continuity management (5th ed.). Wiley.

International Telecommunication Union (2023). Global Cybersecurity Index Report. Geneva: ITU.

Junior, C. R., Becker, I., & Johnson, S. (2023). Unaware, unfunded and uneducated: A systematic review of SME cybersecurity. arXiv preprint arXiv:2309.17186.

Kraemer, S., Carayon, P., & Clem, J. (2020). Cybersecurity governance and risk management frameworks: A review. Computers & Security, 92, 101–120.

National Information Technology Development Agency (2021). National Cybersecurity Policy Framework. Abuja: NITDA.

Nguyen, T., Pham, H., & Tran, L. (2022). Real-time cybersecurity risk assessment using machine learning techniques. Journal of Network and Computer Applications, 200, 103–118.

Nwafor, C., & Ijeoma, N. (2022). Cybersecurity awareness and risk perception among SMEs in Southeast Nigeria. Nigerian Journal of Management Research, 9(3), 89–104.

Nwuke, O., & Adeola, O. (2023). Leadership transition and survival strategies for family-owned SMEs in an emerging economy. Journal of Family Business Management, 13(4), 1343-1365.

Ogunleye, O., & Adeoye, A. (2022). Information security challenges in small businesses in Nigeria. Journal of Entrepreneurship and Innovation, 14(2), 55–70.

Olubiyi, O., Lawal, A. T., & Adeoye, O. O. (2022). Succession planning and family business continuity: Perspectives from Lagos State, Nigeria. Organization and Human Capital Development, 1(1), 40-52.

Olubiyi, T. O., Egwakhe, J., & Akinlabi, B. H. (2019). Knowledge management and family business continuity: The moderating effect of length of time in Existence. Global Journal of Management and Business Research, 19(5), 29-35.

Oriazowanlan, O. A., & Ekenam, E. D. (2024). Effect of leadership succession management crises on family-owned businesses in Benin-City, Edo State, Nigeria. International Journal of Intellectual Discourse, 7(1), 411-425.

Patel, R., & Kumar, V. (2022). Modern approaches to business continuity: Technology-driven resilience. Journal of Business Research, 144, 101–112.

Rajan, R., Rana, N. P., Parameswar, N., Dhir, S., & Dwivedi, Y. K. (2021). Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management. Technological Forecasting and Social Change, 170, 120872.

Russo, N., Reis, L., Silveira, C., & Mamede, H. S. (2024). Towards a comprehensive framework for the multidisciplinary evaluation of organizational maturity on business continuity program management: A systematic literature review. Information Security Journal: A Global Perspective, 33(1), 54–72. https://doi.org/10.1080/19393555.2023.2195577

Smith, J., Lee, P., & Robinson, K. (2021). Cloud-based solutions for business continuity planning: Opportunities and challenges. Journal of Enterprise Information Management, 34(5), 1502–1517.

Vrhovec, S., & Markelj, B. (2024). We need to aim at the top: Factors associated with cybersecurity awareness of cyber and information security decision-makers. Plos one, 19(10), e0312266.

World Economic Forum (2022). Global Risks Report. Geneva: WEF.

Ye, W. (2026). Strengthening Cybersecurity in Small and Medium-Sized Enterprises: Balancing Technology, Costs, Compliance, and Employee Awareness. Sage Open, 16(1), 21582440251414951.

Zhang, X., Li, Y., & Zhao, Q. (2022). Real-time replication and disaster recovery in cloud-based business continuity. Computers & Security, 111, 102512.