The Asian Journal of Professional and Business Studies, Volume 6, Issue 2 (June) 2025, pp. 85-103
https://journal.uptm.edu.my/index.php/ajpbs
e-ISSN 2716-666X, ISSN 2462-1072

Building Cyber Resilient Organisations Through Strategic Risk Management and Digital Preparedness

Shahri Abu Seman[1*],Azahari Jamaludin[2], Ahmad Fauzi Ahmad Zaini[3]

[12,3] Faculty of Business and Accountancy, Universiti Poly-Tech Malaysia, Malaysia

*Corresponding Author: shahri@uptm.edu.my

ABSTRACT

The increasing dependence of organisations on digital technologies has created significant opportunities for operational efficiency, connectivity, and business growth while simultaneously increasing exposure to complex cyber risks. This article examines how strategic risk management and digital preparedness can strengthen cyber resilience and support organisational continuity in increasingly interconnected business environments. The analysis focuses on four important dimensions comprising strategic cyber risk management and governance, digital preparedness and human cybersecurity capability, cyber resilience and business continuity, and cyber risk across digital ecosystems and supply chains. The article identifies several challenges that can weaken organisational cyber resilience, including limited integration of cyber risk into strategic decision making, inadequate employee and organisational preparedness, difficulties in maintaining critical operations during cyber incidents, and vulnerabilities arising from external digital dependencies. These challenges demonstrate that cybersecurity should not be treated solely as a technical responsibility because cyber incidents can generate operational, financial, reputational, and strategic consequences. The article proposes stronger cyber risk governance, continuous development of human and digital capabilities, closer integration between cybersecurity and business continuity, and improved coordination across digital supply chains. Overall, effective cyber resilience requires organisations to combine technological protection with strategic governance, organisational learning, preparedness, response capability, and adaptive capacity. This integrated approach can enable organisations to manage evolving cyber threats more effectively, protect critical business activities, and strengthen long term organisational resilience in increasingly digital business environments.

Keywords: Cybersecurity, Resilience, Preparedness, Governance, Continuity

How to Cite:
Abu Seman, S., Jamaludin, A., & Ahmad Zaini, A. F. (2021). Building Cyber Resilient Organisations Through Strategic Risk Management and Digital Preparedness. *The Asian Journal of Professional & Business Studies*, *2*(2), 85–103. https://doi.org/10.61688/ajpbs.v2i2.378

1. INTRODUCTION

Digital technologies have become fundamental to modern business operations as organisations increasingly depend on interconnected information systems, cloud services, digital platforms, automated processes, and data driven decision making. While these technologies improve efficiency and connectivity, they also create greater exposure to cyber threats capable of disrupting operations, compromising sensitive information, and affecting organisational performance. Cybersecurity has therefore developed from a predominantly technical concern into an important strategic business issue. Anderson and Moore (2006) demonstrate that information security involves economic and organisational considerations that extend beyond technical protection. Gordon et al. (2003) similarly establish that information sharing can contribute to cybersecurity management by improving collective understanding of security threats. Cavusoglu et al. (2004) further demonstrate that security breaches can produce measurable market consequences, illustrating the potential business impact of cybersecurity failures. Acquisti et al. (2006) highlight the economic significance of privacy and information protection, while Gordon and Loeb (2002) demonstrate that organisations must make strategic decisions concerning the appropriate level of investment in information security. Together, these studies indicate that cyber threats should be considered within broader organisational risk management because cybersecurity incidents can influence financial resources, operational continuity, reputation, stakeholder confidence, and long term business performance.

Cyber risk has become more complex as organisations expand their digital connections across customers, suppliers, employees, logistics providers, and other external partners. Increasing connectivity can create additional points of vulnerability because cybersecurity weaknesses may originate outside the organisation's immediate technological boundaries. Boyson (2014) identifies cybersecurity as an important supply chain risk and emphasises the need for organisations to address cyber vulnerabilities across interconnected business relationships. Abdullah et al. (2020) similarly argue that information security should be recognised as a management responsibility rather than being treated solely as a technical function. Their review demonstrates the importance of senior management involvement in establishing effective information security practices. Nurse et al. (2017) further highlight the importance of understanding insider threats because organisational cybersecurity can be affected by both technical vulnerabilities and human behaviour. Radanliev et al. (2020) extend this concern to Industry 4.0 and industrial Internet of Things environments, where interconnected technologies create increasingly complex cyber risk conditions across supply chains. Their analysis highlights the growing relevance of cyber risk analytics and predictive approaches within digitally connected business environments. Sobb et al. (2020) similarly identify emerging cybersecurity challenges associated with Supply Chain 4.0, demonstrating that increasing digital integration can improve operational capability while simultaneously creating new forms of cyber exposure.

Strategic risk management provides an important foundation for addressing these challenges because cyber risk cannot be managed effectively through isolated security controls. Organisations need to understand how cybersecurity exposures interact with strategic objectives, business processes, financial resources, operational dependencies, and stakeholder expectations. Bromiley et al. (2015) argue that enterprise risk management should be integrated with organisational strategy and managerial decision making rather than operating primarily as a compliance mechanism. Abd Wahab and Yusof (2020) similarly emphasise that different categories of organisational risk require different management approaches, indicating that cyber risks should be evaluated according to their characteristics and potential business consequences. Florio and Leoni (2017) demonstrate that advanced enterprise risk management implementation is positively associated with organisational performance and market valuation, while Callahan and Soileau (2017) identify positive relationships between ERM process maturity and operating performance. Malik et al. (2020) further demonstrate that ERM effectiveness positively influences firm performance and that strong risk governance can complement this relationship. These perspectives suggest that cybersecurity should be incorporated into organisational risk governance, strategic planning, resource allocation, and managerial oversight. Strategic risk management can provide the organisational structure required to identify cyber exposures, determine their potential consequences, establish priorities, allocate resources, and coordinate responses across different organisational functions.

Cyber resilience extends this perspective by recognising that organisations cannot completely prevent every cyberattack or eliminate all technological vulnerabilities. Effective cybersecurity therefore requires organisations to prepare for the possibility that preventive controls may fail. Linkov and Kott (2019) explain cyber resilience through the capacity of systems to prepare for, absorb, recover from, and adapt to adverse cyber events. This

perspective shifts attention from prevention alone towards maintaining critical functions and restoring organisational capability after disruption. Dupont (2019) similarly examines different approaches to cyber resilience and emphasises the importance of organisational capabilities for responding to cyber incidents. Organisational resilience research provides additional support for this broader perspective. Duchek (2020) conceptualises resilience through anticipation, coping, and adaptation, demonstrating that organisations require capabilities before, during, and after disruptive events. Hillmann and Guenther (2021) further position organisational resilience as a multidimensional capability involving preparation, response, adaptation, and learning. These perspectives are particularly relevant to cybersecurity because cyber incidents can develop rapidly and may affect multiple organisational activities simultaneously. Building cyber resilient organisations therefore requires more than installing security technologies. Organisations need appropriate governance, communication, decision processes, recovery capability, organisational learning, and strategic flexibility that allow essential activities to continue or recover when cyber incidents occur.

Human behaviour represents another critical dimension of cyber resilience and digital preparedness. Even organisations with sophisticated security technologies may remain vulnerable when employees lack awareness, misunderstand security responsibilities, or fail to follow established security practices. Herath and Rao (2009) demonstrate that employee information security behaviour is influenced by organisational, social, and individual factors, indicating that cybersecurity compliance requires more than formal policies. Bulgurcu et al. (2010) similarly find that employee awareness and attitudes influence intentions to comply with information security policies. Yusof and Abd Wahab (2020) demonstrate that information security training and organisational communication can contribute to improved employee compliance, highlighting the importance of continuous security education. Siponen and Vance (2010) further explain how employees may neutralise or justify noncompliance with information security policies, showing that organisations need to understand behavioural factors that weaken cybersecurity practices. Ifinedo (2012) provides additional evidence that employee security behaviour is influenced by perceptions, attitudes, and organisational factors. These studies demonstrate that digital preparedness requires an organisation wide security culture in which employees understand cyber risks and their responsibilities for protecting information and systems. Cyber resilience should consequently combine technological protection with employee awareness, management commitment, clear security responsibilities, and continuous organisational learning.

Digital preparedness also requires organisations to understand how cyber threats can spread through interconnected business networks. Cybersecurity vulnerabilities are increasingly associated with third parties, supply chains, digital services, and shared technological infrastructures, meaning that organisations cannot evaluate cyber risk only within their internal systems. Radanliev et al. (2020) demonstrate that Industry 4.0 supply chains create complex cyber risk environments in which interconnected technologies require improved analytics and decision support capabilities. Sobb et al. (2020) similarly identify multiple cybersecurity challenges associated with increasingly digital supply chains and highlight the need for stronger approaches to managing emerging vulnerabilities. Colicchia et al. (2021) examine cyber supply chain risk management within digital transformation and demonstrate that effective cyber resilience requires alignment among different supply chain actors rather than concentrating only on individual organisations. Ghadge et al. (2021) further demonstrate that information, material, and financial flows within supply chains can create entry points through which cyber risks affect interconnected operations. These findings indicate that digital preparedness should include understanding critical external dependencies, evaluating third party cyber exposure, strengthening information sharing, and considering how disruptions affecting business partners may influence organisational continuity. Cyber resilience therefore increasingly depends on the security and preparedness of the wider business ecosystem.

Small and medium sized enterprises may face particular difficulties in developing cyber resilience because their technological dependence is not always matched by equivalent cybersecurity resources and expertise. Digitalisation provides SMEs with opportunities to improve productivity, customer access, communication, and business growth, but it can simultaneously expose them to cyber risks that management may underestimate. Heidt et al. (2019) demonstrate that information security management within SMEs is influenced by organisational characteristics and managerial perceptions, highlighting the importance of understanding cybersecurity within the specific context of smaller businesses. Benz and Chatterjee (2020) further identify significant cybersecurity risk management challenges among SMEs, including limited understanding of cyber threats from a management perspective. These limitations can weaken digital preparedness when organisations adopt technologies more rapidly than they develop corresponding security capabilities. Cybersecurity investment decisions also require

careful prioritisation because organisations operate with limited resources. Gordon and Loeb (2002) demonstrate that information security investment should be determined according to the characteristics and potential consequences of vulnerabilities rather than assuming that maximum expenditure always represents the most efficient approach. Strategic risk management is therefore particularly relevant because it can help organisations prioritise critical assets, evaluate potential business consequences, and allocate cybersecurity resources according to organisational exposure and strategic importance.

Building cyber resilient organisations ultimately requires a shift from reactive cybersecurity towards strategic risk management and continuous digital preparedness. Organisations should not assume that cybersecurity success is demonstrated only by the absence of attacks because sophisticated threats may eventually overcome preventive controls. Instead, resilience requires organisations to understand critical assets, identify vulnerabilities, prepare employees, establish response capabilities, protect essential operations, and learn from cybersecurity incidents. Duchek (2020) emphasises that resilience develops through anticipation, coping, and adaptation, while Hillmann and Guenther (2021) demonstrate that organisational resilience involves interconnected capabilities rather than a single response mechanism. Radanliev et al. (2020) further show that emerging digital environments require increasingly sophisticated approaches to cyber risk analysis and management. The growing interdependence of digital supply chains reinforces this requirement because cybersecurity weaknesses can extend across organisational boundaries (Colicchia et al., 2021; Sobb et al., 2020). This article therefore examines how strategic risk management and digital preparedness can contribute to building cyber resilient organisations. Particular attention is given to cyber risk governance, human and technological preparedness, business continuity, external digital dependencies, and organisational adaptation as interconnected capabilities for protecting business operations and strengthening resilience in increasingly digital environments.

2. LITERATURE REVIEW

Cyber resilience increasingly requires organisations to combine strategic risk management with digital preparedness rather than relying primarily on technical security controls. Effective cyber resilience involves governance, risk assessment, human capability, technological readiness, incident response, and organisational learning. Existing research demonstrates that cybersecurity has developed into a strategic business concern requiring coordination across organisational functions and external relationships (Schinagl & Shahim, 2020; Annarelli et al., 2020). The literature is therefore examined through four areas comprising strategic cyber risk management, digital preparedness and human capability, cyber resilience and business continuity, and cyber risk across interconnected digital ecosystems.

2.1 Strategic Cyber Risk Management and Governance

Strategic cyber risk management requires organisations to understand cybersecurity as a business risk that can influence strategic objectives, financial resources, operations, reputation, and stakeholder relationships. Gordon and Loeb (2002) demonstrate that information security investment requires economic judgement because organisations must determine how much protection is appropriate relative to potential losses. Cavusoglu et al. (2004) further show that information security breaches can produce measurable economic consequences, illustrating why cybersecurity decisions should extend beyond technical departments. Anderson and Moore (2006) similarly position information security within broader economic and organisational considerations. As digital dependence has expanded, governance has consequently become increasingly important. Schinagl and Shahim (2020) demonstrate that information security governance has moved from a narrow technical concern towards a strategic issue with implications extending to senior management and board level responsibilities. Their analysis reinforces the importance of aligning cybersecurity with business governance and digital strategy. Cyber risk management should therefore identify critical information assets, evaluate the strategic consequences of cyber incidents, determine appropriate risk priorities, and establish clear management accountability. Such an approach enables cybersecurity decisions to become part of organisational strategy rather than remaining primarily the responsibility of information technology specialists.

Strategic cyber risk management also benefits from integration with broader enterprise risk processes because cyber exposures frequently interact with operational, financial, legal, and reputational risks. Bromiley et al. (2015) argue that enterprise risk management should be closely connected with strategy and organisational decision making, while Yusof and Abd Wahab (2020) demonstrate that different forms of organisational risk require

different management approaches. Cybersecurity should therefore be evaluated according to the organisation's particular vulnerabilities, critical assets, strategic priorities, and operating environment. Malik et al. (2020) provide further evidence that effective enterprise risk management can positively influence firm performance, highlighting the potential value of stronger risk governance. More specifically, Goel et al. (2020) develop the PRISM framework around prioritisation, resources, implementation, standardisation, and monitoring to support strategic cybersecurity risk assessment and management decision making. Their framework demonstrates that organisations need structured mechanisms for connecting cybersecurity risks with investment and resource decisions. Cybersecurity risk management should consequently involve senior managers, technology specialists, risk professionals, and operational managers who can collectively evaluate business consequences. Strategic integration enables organisations to prioritise cyber risks more effectively, allocate resources according to exposure, and maintain stronger alignment between cybersecurity investments and organisational objectives.

2.2 Digital Preparedness and Human Cybersecurity Capability

Digital preparedness depends not only on technological infrastructure but also on employees who understand cybersecurity responsibilities and consistently apply appropriate security practices. Human behaviour remains particularly important because technical controls can be weakened when employees misunderstand policies, respond incorrectly to threats, or adopt insecure work practices. Herath and Rao (2009) demonstrate that employee security behaviour is influenced by organisational, social, and individual factors, suggesting that compliance cannot be achieved through written policies alone. Bulgurcu et al. (2010) similarly show that information security awareness and employee attitudes influence intentions to comply with organisational security policies. Puhakainen and Siponen (2010) further demonstrate the importance of security training and communication in developing employee compliance behaviour. More recent evidence also shows that behavioural conditions can influence cybersecurity performance. D'Arcy and Teh (2019) find that security related stress, frustration, fatigue, and neutralisation can affect information security policy compliance. These findings demonstrate that digital preparedness requires organisations to develop employee capability rather than assuming that security awareness automatically produces secure behaviour. Cybersecurity training should therefore be continuous, relevant to employee responsibilities, and supported by management communication, clear expectations, and organisational practices that encourage responsible security behaviour.

The development of a strong information security culture provides another important foundation for digital preparedness. Da Veiga and Eloff (2010) emphasise that information security culture influences the human behaviours required to protect organisational information assets. Organisational culture can establish shared expectations concerning how employees handle information, use technology, and respond to security responsibilities. This perspective is supported by research showing that information security culture and wider organisational culture influence employee compliance behaviour. In addition, Ait Maalem Lahcen et al. (2020) highlight behavioural dimensions of cybersecurity and demonstrate that effective cybersecurity requires greater understanding of human motivations and actions alongside technological protection. Digital preparedness should therefore involve organisational capability across technology, people, and processes. Hasan et al. (2021) provide empirical evidence that cybersecurity readiness is influenced by technological, organisational, and environmental factors and that improved security performance can contribute to organisational performance. This holistic perspective indicates that preparedness should incorporate employee competence, leadership support, security policies, technological infrastructure, environmental awareness, and appropriate organisational resources. Organisations that develop these elements together are likely to establish stronger readiness for recognising and responding to cyber threats than those concentrating mainly on technical security investment.

2.3 Cyber Resilience and Business Continuity

Cyber resilience extends cybersecurity beyond the prevention of attacks towards maintaining and restoring essential organisational capabilities when preventive measures are unsuccessful. This distinction is important because organisations cannot realistically eliminate every cyber threat, particularly as technologies, attack methods, and digital dependencies continue to develop. Sepúlveda Estay et al. (2020) define cyber resilience around the ability to respond promptly and coherently to cyber incidents so that their disruptive effects on operations can be minimised. Their systematic review of cyber resilience assessment frameworks demonstrates that resilience involves multiple approaches and application contexts rather than one universally applicable model. Annarelli et al. (2020) similarly examine the management of cyber resilient systems and identify managerial

actions, contextual conditions, and organisational learning as important components of cyber resilience. These findings align with the broader resilience perspective developed by Duchek (2020), who conceptualises organisational resilience through anticipation, coping, and adaptation. Cyber resilience can therefore be understood as a continuous capability that exists before, during, and after an incident. Organisations require preventive controls, but they also need detection mechanisms, response responsibilities, recovery resources, communication procedures, and learning processes that enable critical operations to continue or recover when cyber disruption occurs.

The development of cyber resilience also requires organisations to examine vulnerabilities in relation to their capacity to adapt rather than evaluating cyber risk exclusively through the likelihood and impact of specific attacks. Scholz et al. (2020) extend traditional risk analysis by connecting digital threats with organisational vulnerability and adaptive capacity, demonstrating that resilience management requires consideration of how organisations can respond to changing digital conditions. Cyber resilience consequently involves both protection and adaptation. Yusof and Abd Wahab (2021) similarly conceptualise resilience in software intensive systems as the ability to deal with uncertainty and changing conditions throughout system life cycles. Such perspectives are important for business continuity because cyber incidents may disrupt essential processes even when security systems function as designed. Organisations therefore need to identify critical operations, determine acceptable levels of disruption, establish alternative operating arrangements, and ensure that recovery resources are available. Annarelli et al. (2020) further highlight employee learning and technological capability in the management of cyber resilient systems. These findings suggest that business continuity and cybersecurity should be coordinated rather than managed separately. Strong cyber resilience enables organisations to protect critical activities while maintaining sufficient adaptive capability to restore services, modify operating arrangements, and learn from incidents that reveal weaknesses in existing cybersecurity preparations.

2.4 Cyber Risk Across Digital Ecosystems and Supply Chains

Digital preparedness increasingly extends beyond organisational boundaries because firms rely on suppliers, cloud providers, logistics partners, customers, digital platforms, and interconnected technologies. These relationships improve information sharing and operational efficiency but also create pathways through which cyber vulnerabilities can spread across organisational networks. Pandey et al. (2020) identify multiple cybersecurity risks within globalised supply chains and classify these risks according to supply, operational, and demand related exposures. Their work demonstrates that information and communication technologies can simultaneously strengthen supply chain performance and create security vulnerabilities. Radanliev et al. (2020) similarly examine cyber risk within Industrial Internet of Things and Industry 4.0 supply chains, highlighting the complexity generated by interconnected devices, data, artificial intelligence, and expanding digital environments. Sobb et al. (2020) identify related cybersecurity challenges within Supply Chain 4.0, reinforcing the importance of examining cyber exposure beyond individual organisational systems. Digital preparedness should consequently include knowledge of external technological dependencies, third party access, data sharing arrangements, and potential vulnerabilities created through partner connections. Organisations need to understand where cyber risks can enter their wider business networks and how external disruption may influence their own operational continuity.

Cyber supply chain risk management therefore requires coordination between organisations because vulnerabilities cannot always be managed effectively through internal security controls. Colicchia et al. (2021) demonstrate that cyber supply chain risk management requires alignment among different supply chain actors and should move beyond the technical functioning of individual organisations. Their research highlights the importance of integrating people, processes, technology, and relationships when strengthening cyber resilience across digital supply chains. Ghadge et al. (2021) further demonstrate that information, material, and financial flows can become entry points for cyber risks, showing how cyber threats can affect interconnected supply chain activities. Cyber supply chain risks are also increasingly associated with third party compromise, making supplier relationships an important dimension of digital preparedness. Research examining cybersecurity frameworks for critical infrastructure indicates that supply chain threats require stronger coverage within organisational security approaches (Melnyk et al., 2021). These studies demonstrate that organisations should evaluate cyber resilience at an ecosystem level. Strong digital preparedness requires visibility of critical partners, appropriate information sharing, assessment of third party vulnerabilities, coordinated response arrangements, and clear cybersecurity responsibilities across organisational boundaries. Such practices can reduce the possibility that weaknesses elsewhere in the digital network undermine otherwise effective internal cybersecurity capabilities.

3. ISSUES IN BUILDING CYBER RESILIENT ORGANISATIONS THROUGH STRATEGIC RISK MANAGEMENT AND DIGITAL PREPAREDNESS

Building cyber resilient organisations remains challenging because cybersecurity risks extend beyond technological vulnerabilities and increasingly involve governance, employee behaviour, operational continuity, and interconnected digital relationships. Information security has developed into a strategic business issue that requires stronger management and board involvement rather than being managed only by technical specialists (Schinagl & Shahim, 2020). At the same time, organisations face difficulties in developing effective cyber resilience capabilities that support prevention, response, recovery, and adaptation following cyber incidents (Yusof et al., 2020). Four major issues therefore require particular attention in strengthening organisational cyber resilience.

3.1 Weak Strategic Integration of Cyber Risk Management and Governance

One significant issue is the weak integration of cybersecurity risk with organisational strategy and governance. Cybersecurity may still be viewed primarily as an information technology responsibility even though cyber incidents can affect financial performance, operations, reputation, regulatory compliance, customer relationships, and strategic objectives. Yusof and Salleh (2021) demonstrate that information security governance has shifted from a narrowly focused technical concern towards a strategic business issue with implications for senior management and boards. However, this development does not necessarily mean that cybersecurity has been effectively embedded within organisational decision making. Management may receive technical information concerning vulnerabilities without clearly understanding their potential business consequences. Goel et al. (2020) address this challenge through the PRISM framework, which emphasises prioritisation, resources, implementation, standardisation, and monitoring when evaluating an organisation's strategic cybersecurity orientation. The framework demonstrates that cybersecurity decisions require strategic consideration of organisational priorities and available resources rather than relying entirely on technical assessments. Consequently, weak integration can result in cybersecurity investments that are disconnected from critical business assets and organisational objectives. Strong cyber risk governance requires management to understand how cyber threats affect business priorities, allocate resources according to exposure, and establish clear accountability for cyber risk across organisational functions.

The governance issue becomes more difficult because cyber risks develop rapidly and can affect several organisational activities simultaneously. Strategic risk management requires organisations to determine which digital assets are most critical, which vulnerabilities create the greatest business consequences, and which security investments should receive priority. Cybersecurity frameworks may provide technical guidance, but organisational leaders still need to translate security information into strategic decisions. Schinagl and Shahim (2020) highlight continuing tensions between rapidly changing business conditions and existing approaches to information security governance, reinforcing the importance of developing governance arrangements that support both protection and digital business opportunities. Annarelli et al. (2020) similarly demonstrate that cyber resilience depends on contextual and managerial factors and identify managerial actions as important components in implementing cyber resilient systems. This suggests that cyber resilience cannot be achieved through security technology alone. Organisations need management participation, appropriate accountability, communication between technical and business functions, and clear connections between cybersecurity priorities and organisational strategy. When these elements remain weak, cyber risk assessments may become compliance activities rather than meaningful inputs into organisational decision making. Improving cyber governance therefore remains an important challenge for organisations attempting to build resilience while continuing to pursue digital transformation and business performance.

3.2 Inadequate Digital Preparedness and Human Cybersecurity Capability

A second issue concerns inadequate digital preparedness, particularly the ability of organisations and employees to recognise, understand, and respond appropriately when cyber threats emerge. Digital preparedness extends beyond the installation of security technologies because organisational protection also depends on employee knowledge, cybersecurity awareness, managerial support, communication, and clearly established response

procedures. Sepúlveda Estay et al. (2020) demonstrate that cyber resilience involves multiple assessment approaches and organisational capabilities, highlighting the complexity of preparing organisations for cyber incidents. Annarelli et al. (2020) similarly emphasise the importance of managerial actions and organisational capabilities in developing cyber resilient systems. Human capability is particularly important because employees regularly interact with information systems and can influence the effectiveness of organisational security practices. Zwilling et al. (2020) demonstrate that cybersecurity awareness, knowledge, and behaviour are interconnected, indicating that knowledge alone may not always translate into appropriate cybersecurity practices. Zhou et al. (2020) similarly highlight the importance of individual awareness and behavioural factors in strengthening secure technology practices. In addition, Torten et al. (2018) emphasise that information security awareness should be supported through organisational efforts that encourage employees to understand and adopt appropriate security behaviours. Organisations may therefore remain vulnerable despite sophisticated security technologies when employees lack sufficient awareness, responsibilities are unclear, or cybersecurity information is poorly communicated. Digital preparedness consequently requires an organisation wide approach combining technological protection with capable employees, clear responsibilities, effective communication, and management involvement.

Preparedness becomes more challenging because organisational cybersecurity capabilities must continuously develop as technologies, working arrangements, and cyber threats change. New applications, cloud services, connected devices, and digitally integrated business processes can create vulnerabilities when organisations introduce technologies more rapidly than they develop corresponding cybersecurity knowledge and practices. Sobb et al. (2020) demonstrate that Supply Chain 4.0 creates emerging operational and cybersecurity risks through increasing integration among manufacturing, telecommunications, and information technologies. Cyber preparedness should therefore develop alongside digital transformation rather than being introduced only after technologies have become embedded within organisational operations. Zhang et al. (2021) emphasise the importance of cybersecurity awareness training in strengthening employees' capacity to recognise security threats and respond appropriately, while Zhang and He (2019) highlight the need for effective organisational cybersecurity training that actively engages employees. Yusof et al. (2020) further demonstrate that cybersecurity knowledge and awareness influence security behaviour. Wiley et al. (2020) also demonstrate that employee cybersecurity behaviour is influenced by organisational and individual conditions, reinforcing the importance of developing human capability alongside technological security. These findings indicate that digital preparedness should be treated as a continuous organisational capability. Regular training, updated cybersecurity knowledge, management involvement, and clear response responsibilities can reduce confusion and strengthen the organisation's capacity to maintain critical activities when digital systems are threatened or disrupted.

3.3 Difficulty in Maintaining Cyber Resilience and Business Continuity

Another important issue involves maintaining business continuity when cyber incidents successfully disrupt organisational systems. Cybersecurity strategies traditionally place significant emphasis on preventing attacks, but complete prevention is increasingly difficult within complex digital environments. Organisations therefore need sufficient resilience to maintain critical activities, limit disruption, recover systems, and adapt after cyber incidents. Sepúlveda Estay et al. (2020) explain that cyber resilience concerns not only preventing attacks but also responding promptly and coherently when attacks occur so that operational disruption can be minimised. Yusof et al. (2020) similarly conceptualise cyber resilience through organisational adaptation and identify important managerial and contextual factors influencing cyber resilient systems. The challenge arises because cybersecurity and business continuity may be managed through separate organisational processes. Technical teams may concentrate on restoring information systems while operational managers focus on maintaining customer service, production, financial activities, or other critical functions. Without effective coordination, technology recovery priorities may not correspond with business priorities. Cyber resilience consequently requires organisations to understand which systems support critical processes and determine how essential activities can continue when those systems are temporarily unavailable. This connection between cybersecurity and operational continuity is necessary for limiting the wider consequences of cyber disruption.

Cyber resilience also requires organisations to develop adaptation and learning rather than simply restore systems to their previous condition after an incident. Cyber events may expose weaknesses in security controls, decision processes, digital architecture, employee practices, or relationships with external service providers. These weaknesses should inform future preparedness and risk management. Bøe et al. (2020) describe cyber resilience

as involving multiple organisational actors, resources, competencies, technologies, and strategic choices, demonstrating that resilience is shaped by interactions across different levels of an organisation and its environment. This perspective indicates that recovery is only one component of cyber resilience. Organisations should also examine why disruption occurred, how effectively critical activities were maintained, and what organisational changes are required to reduce future vulnerability. Annarelli et al. (2020) likewise identify organisational learning among the important elements associated with managing cyber resilient systems. Organisations that concentrate only on technical restoration may therefore lose opportunities to strengthen future resilience. The central issue is to establish continuity arrangements that support immediate recovery while also producing organisational learning and adaptation. Effective cyber resilience should consequently combine preparedness, response, recovery, learning, and strategic improvement rather than treating cyber incidents as isolated technical events.

3.4 Growing Cyber Vulnerability Across Digital Supply Chains

The final issue concerns increasing cyber vulnerability across interconnected supply chains and digital business ecosystems. Organisations increasingly depend on suppliers, cloud providers, logistics partners, digital platforms, software vendors, and other external organisations to support their operations. These relationships create efficiency and flexibility but also extend cybersecurity exposure beyond the direct control of individual firms. Sobb et al. (2020) demonstrate that Supply Chain 4.0 combines manufacturing, telecommunications, and information technologies in ways that create unique and emerging operational and cyber risks. Masip-Bruin et al. (2021) similarly identify cybersecurity challenges in ICT supply chains characterised by distributed, dynamic, heterogeneous, and potentially insecure infrastructures. Their work emphasises the need for coordinated cyber resilience across interconnected supply chain environments. This creates an important strategic challenge because an organisation may implement strong internal security controls while remaining vulnerable through weaknesses in suppliers or digital service providers. Cybersecurity risk assessment should therefore consider external dependencies and understand how incidents affecting third parties could interrupt organisational activities. However, organisations may have limited visibility into the security practices and vulnerabilities of external partners, making cyber supply chain risk particularly difficult to assess and control.

Increasing digital integration also creates challenges in determining how cybersecurity responsibilities should be shared across supply chain relationships. A cyber incident originating from one organisation can create consequences for multiple connected parties through disrupted information, systems, services, or operational flows. Masip-Bruin et al. (2021) emphasise that complex ICT supply chains require coordinated frameworks for cyber resilience because individual approaches may be insufficient within distributed digital infrastructures. Sobb et al. (2020) similarly identify the need for stronger cybersecurity approaches as Supply Chain 4.0 expands technological interdependence. Additional research on blockchain adoption for cyber supply chain risk management demonstrates that growing Industry 4.0 connectedness has intensified cyber risks and created demand for more secure mechanisms for managing supply chain relationships (Shojaei et al., 2021). Nevertheless, technological solutions alone cannot resolve weaknesses in governance, communication, or accountability among supply chain partners. Organisations need greater visibility of critical digital dependencies, appropriate assessment of third party security, and clearer arrangements for coordinating responses when external cyber incidents occur. The growing interdependence of digital supply chains consequently means that cyber resilience should be evaluated not only at organisational level but also across the broader network on which business continuity depends.

4. DISCUSSION ON STRATEGIC RISK MANAGEMENT AND DIGITAL PREPAREDNESS FOR CYBER RESILIENCE

Cyber resilience requires organisations to integrate cybersecurity with strategic risk management, organisational preparedness, business continuity, and external digital relationships. The issues identified indicate that technological controls alone cannot provide sufficient protection when cyber threats affect employees, strategic decisions, operations, and interconnected supply chains. Existing research supports a broader organisational approach in which cybersecurity governance, readiness, resilience, and coordinated risk management operate together to protect critical business activities (Schinagl & Shahim, 2020; Annarelli et al., 2020).

4.1 Integrating Cyber Risk Management with Strategic Governance

The weak strategic integration of cyber risk identified earlier demonstrates that cybersecurity should be positioned within organisational governance and strategic decision making rather than remaining primarily within information technology functions. Cyber threats can generate consequences for operations, financial resources, customers, reputation, and strategic objectives, requiring management to understand cybersecurity from a broader business perspective. Schinagl and Shahim (2020) demonstrate that information security has developed from a narrowly focused technical issue into a strategic business concern with direct implications for senior management and boards. This transition indicates that cyber risk decisions should involve managers who understand both technological vulnerabilities and their potential organisational consequences. AlGhamdi et al. (2020) similarly identify alignment between information security policies and organisational objectives as an important requirement of effective information security governance. Organisations should therefore integrate cybersecurity considerations into strategic planning, investment decisions, digital transformation initiatives, and resource allocation. Risk priorities should be established according to the importance of digital assets, potential operational disruption, stakeholder consequences, and organisational exposure rather than primarily according to technical severity. Such integration can improve management understanding of cyber risk and create stronger accountability for decisions concerning cybersecurity resources, responsibilities, and acceptable levels of organisational exposure.

Cyber governance should also establish clear connections between strategic oversight and operational cybersecurity activities. Senior management cannot manage every technical vulnerability directly, but it should ensure that appropriate structures exist for communicating significant cyber exposures and determining when strategic intervention is required. Yusof and Abd Wahab (2020) identify top management support, strategic alignment, control, regulation, and continuous evaluation as important components of effective information security governance. This demonstrates that cybersecurity governance should not be limited to approving security policies because implementation, monitoring, and organisational accountability are equally important. Schinagl and Shahim (2020) further emphasise that digitalisation creates tension between protecting organisations and enabling them to pursue digital opportunities, requiring governance mechanisms capable of balancing security and business development. Strategic cyber risk management should consequently enable management to distinguish between risks that require additional protection and risks that can be accepted within established organisational tolerances. This approach avoids treating cybersecurity as an objective of eliminating every possible vulnerability, which may be economically or operationally unrealistic. Instead, cyber governance should guide decisions concerning which assets require the strongest protection, which vulnerabilities create strategic consequences, and how cybersecurity investments support wider organisational objectives. Effective governance can therefore transform cybersecurity from reactive technical protection into an integrated component of strategic risk management.

4.2 Strengthening Digital Preparedness and Human Cybersecurity Capability

The issue of inadequate digital preparedness demonstrates that organisations require cybersecurity readiness across technological, organisational, and human dimensions. Installing sophisticated security technologies cannot provide effective protection when organisational processes are unclear or employees lack the knowledge required to recognise and respond appropriately to cyber threats. Hasan et al. (2021) provide important empirical evidence by demonstrating that cybersecurity readiness is influenced by technological, organisational, and environmental factors. Their findings further show that cybersecurity readiness positively influences organisational security performance, which subsequently contributes to financial and nonfinancial performance. This indicates that preparedness should be developed as an organisational capability rather than measured simply through the number of security technologies implemented. Organisations need appropriate information technology infrastructure, management support, security policies, employee awareness, external knowledge, and processes for recognising emerging cyber risks. Yusof et al. (2020) similarly find that organisations demonstrating stronger cyber resilience invest in employee learning alongside technological capabilities. Consequently, digital preparedness should involve regular assessment of whether employees understand security responsibilities, whether managers possess sufficient information to coordinate responses, and whether organisational systems can detect and respond to cyber incidents. Combining technological readiness with organisational capability can create a stronger security environment and reduce dependence on preventive technology alone.

Human capability should receive particular attention because cybersecurity preparedness depends substantially on how employees interact with digital systems and organisational information. Employees can strengthen organisational protection when they understand cybersecurity responsibilities, but they can also create vulnerabilities when security requirements are misunderstood, ignored, or inconsistently applied. Annarelli et al. (2020) identify employee training and organisational learning as important managerial actions associated with cyber resilient systems, demonstrating that human capability should be incorporated directly into cybersecurity management. Digital preparedness should consequently move beyond occasional awareness programmes and become a continuous organisational learning process. Employees should understand the security requirements associated with their responsibilities, while managers should ensure that cybersecurity information is communicated clearly across organisational levels. Hasan et al. (2021) further demonstrate that organisational cybersecurity readiness depends on multiple internal and external conditions rather than isolated technical measures. Their findings support a holistic approach in which employee capability operates alongside infrastructure, organisational resources, management support, and environmental awareness. Cyber preparedness should therefore be regularly reviewed as technologies and working practices change. New digital systems can create new security exposures, requiring organisations to update employee knowledge and organisational procedures accordingly. Strengthening human cybersecurity capability can ultimately improve detection, response, communication, and the overall capacity to limit the consequences of cyber incidents.

4.3 Advancing Cyber Resilience and Business Continuity

The difficulty of maintaining business continuity during cyber incidents demonstrates why organisations should extend cybersecurity beyond prevention and develop stronger cyber resilience capabilities. Preventive controls remain essential, but organisations cannot assume that every cyberattack will be successfully prevented. Sepúlveda Estay et al. (2020) explain that cyber resilience includes the capacity to respond promptly and coherently when cyberattacks occur so that their disruptive effects on operations can be minimised. Their systematic review further demonstrates that cyber resilience has been addressed across numerous industries and research contexts, indicating that resilience represents a broader organisational concern rather than a narrowly technical concept. Yusof and Razali (2020) similarly identify contextual conditions and managerial actions as important elements in implementing cyber resilient systems. These perspectives suggest that cybersecurity should be directly connected with business continuity planning. Organisations need to determine which digital systems support critical business processes, how long those processes can tolerate interruption, and which alternative arrangements are available when important technologies become unavailable. Cyber response priorities should consequently be determined according to business criticality rather than technical considerations alone. Linking cybersecurity with business continuity can enable organisations to protect essential operations, coordinate recovery priorities, and reduce the wider organisational consequences of successful cyberattacks.

Cyber resilience should also include organisational learning and adaptation after incidents because returning systems to their previous condition does not necessarily strengthen future preparedness. Cyber incidents can expose weaknesses in security technologies, communication, employee behaviour, managerial decisions, and business continuity arrangements. Organisations should therefore examine incidents systematically and determine which vulnerabilities or organisational weaknesses contributed to disruption. Annarelli et al. (2020) identify learning by employees and technologies as significant actions in managing cyber resilient systems, highlighting the importance of improving capabilities through experience. Sepúlveda Estay et al. (2020) similarly demonstrate that cyber resilience frameworks extend across preparation, response, and recovery considerations, reinforcing the need for organisations to assess resilience comprehensively. Business continuity plans should consequently be treated as dynamic organisational arrangements that can be improved when new vulnerabilities or dependencies become visible. Organisations should assess whether critical processes were adequately protected, whether response responsibilities were clear, whether communication was timely, and whether resources were sufficient to support recovery. Lessons identified through these reviews should subsequently influence cybersecurity investment, employee preparation, system design, and continuity arrangements. This learning orientation can transform cyber incidents from isolated disruptions into opportunities for strengthening future organisational resilience and reducing vulnerability to similar events.

4.4 Managing Cyber Risk Across Digital Supply Chains

The growing cyber vulnerability of digital supply chains demonstrates that organisational resilience cannot be developed exclusively within individual organisational boundaries. Businesses increasingly rely on interconnected suppliers, logistics providers, cloud services, software systems, and digital platforms, creating dependencies through which cyber threats can affect multiple organisations. Sobb et al. (2020) demonstrate that Supply Chain 4.0 combines manufacturing, telecommunications, and information technologies while simultaneously generating distinctive operational and cyber risks. Their findings indicate that digital integration creates substantial efficiency opportunities but also expands the environment in which vulnerabilities may emerge. Ghadge et al. (2021) further demonstrate that cyber risks can propagate through supply chain information, material, and financial flows, illustrating how digital vulnerabilities can extend beyond conventional information systems. Organisations should therefore identify which external relationships and digital services are critical to operational continuity and assess how disruption affecting those parties could influence their own activities. Internal cybersecurity may be insufficient when critical suppliers or service providers maintain weaker security capabilities. Strategic cyber risk management consequently requires greater visibility of external dependencies, appropriate assessment of third party vulnerabilities, and mechanisms for communicating significant cybersecurity concerns across business relationships. Cyber resilience should therefore be understood partly as a network capability rather than solely as an internal organisational characteristic.

Digital supply chain resilience also requires coordinated approaches because individual organisations may have limited ability to control cybersecurity across complex networks. Masip-Bruin et al. (2021) demonstrate that ICT supply chains consist of distributed, dynamic, heterogeneous, and potentially insecure infrastructures, creating a need for coordinated cyber resilience frameworks. Their research highlights that trustworthy supply chains require security arrangements capable of addressing vulnerabilities across interconnected technological environments. Ghadge et al. (2021) similarly show that cyber risks can enter and propagate through different supply chain flows, reinforcing the need to understand cybersecurity beyond direct organisational boundaries. Organisations should therefore establish cybersecurity expectations for important external partners, identify critical data and system connections, and determine how cyber incidents affecting third parties will be communicated and managed. Sobb et al. (2020) further demonstrate that increasingly integrated Supply Chain 4.0 environments create new cybersecurity challenges that require solutions capable of addressing technological interdependence. Effective cyber supply chain risk management should consequently combine technological controls with governance, communication, relationship management, and coordinated response capability. Organisations that understand their digital dependencies and maintain stronger collaboration with critical partners are better positioned to manage cyber incidents that originate outside their direct control and protect business continuity across interconnected digital ecosystems.

5. SUGGESTIONS FOR STRENGTHENING CYBER RESILIENCE THROUGH STRATEGIC RISK MANAGEMENT AND DIGITAL PREPAREDNESS

Organisations should strengthen cyber resilience through an integrated approach that combines strategic governance, digital preparedness, business continuity, and supply chain cybersecurity. Cybersecurity should be embedded within organisational decision making rather than treated only as a technical responsibility. The following suggestions address the four major areas identified in the discussion and provide practical directions for improving organisational preparedness and resilience against evolving cyber risks.

5.1 Strengthening Strategic Cyber Risk Governance

Organisations should strengthen cyber risk governance by integrating cybersecurity responsibilities directly into strategic management and organisational decision making. Cybersecurity should be considered when organisations evaluate digital investments, business expansion, operational priorities, information systems, and other strategic activities that increase dependence on digital resources. Schinagl and Shahim (2020) demonstrate that information security governance has developed from a narrowly focused technical issue into a strategic business concern with implications extending to senior management and boards. Organisations should therefore establish clear accountability for cyber risk at different management levels and ensure that significant cybersecurity exposures are communicated to decision makers in understandable business terms. Management should receive information concerning the potential operational, financial, reputational, and strategic consequences of important cyber risks rather than relying primarily on technical descriptions. Cyber risk assessment should also identify critical digital assets and determine which systems, information, and business

processes require the greatest level of protection. Goel et al. (2020) similarly emphasise prioritisation, resource allocation, implementation, standardisation, and monitoring as important components of strategic cybersecurity risk management. Organisations can consequently improve cyber governance by connecting security priorities with organisational objectives and ensuring that cybersecurity resources are directed towards vulnerabilities capable of producing the most significant business consequences.

Cyber governance should also establish stronger coordination among senior management, risk professionals, information technology specialists, and operational managers. Cybersecurity decisions frequently involve trade offs between security, cost, operational efficiency, digital innovation, and business opportunities. These decisions should therefore incorporate different organisational perspectives rather than being determined entirely within technical functions. Schinagl and Shahim (2020) emphasise that digitalisation creates a governance challenge because organisations must protect themselves while remaining capable of benefiting from digital opportunities. Management should consequently establish regular cyber risk reviews that evaluate significant vulnerabilities, emerging threats, critical digital dependencies, and the effectiveness of existing controls. These reviews should be connected with broader organisational risk management so that cybersecurity exposures can be considered together with operational and strategic consequences. Organisations should also establish clear criteria for determining when cyber risks require escalation to senior management and when existing controls remain sufficient. Such governance arrangements can prevent cybersecurity from becoming an isolated compliance exercise and encourage management to treat cyber risk as part of normal strategic decision making. Stronger governance can ultimately improve accountability, resource prioritisation, communication, and organisational understanding of how cybersecurity contributes to business continuity and long term resilience.

5.2 Developing Continuous Digital Preparedness and Human Capability

Organisations should develop digital preparedness as a continuous capability involving technology, employees, management, and organisational processes. Cybersecurity readiness cannot be achieved through security technologies alone because employees and managers influence how effectively organisations identify and respond to digital threats. Hasan et al. (2021) demonstrate that cybersecurity readiness is shaped by technological, organisational, and environmental factors and that stronger readiness contributes to organisational security performance. Organisations should therefore regularly assess whether security technologies remain appropriate, employees understand their responsibilities, management provides sufficient support, and organisational procedures reflect changing digital conditions. Digital preparedness should develop alongside the introduction of new technologies rather than being considered only after systems have been implemented. This is particularly important because increased digitalisation can create additional vulnerabilities and dependencies. Organisations should identify cybersecurity requirements when adopting cloud services, connected technologies, digital platforms, and other new systems. Employee preparation should also be aligned with actual responsibilities because cybersecurity risks differ across organisational roles. Continuous security education, clear communication, practical awareness activities, and accessible reporting processes can strengthen employees' ability to recognise and communicate potential threats. Digital preparedness can consequently become an organisation wide capability rather than a responsibility concentrated primarily within information technology departments.

Preparedness should also include regular evaluation of organisational readiness to respond when cybersecurity controls fail. Organisations should determine whether employees know how to communicate suspicious activities, whether managers understand their responsibilities during incidents, and whether appropriate resources are available for coordinated response. Sepúlveda Estay et al. (2020) emphasise that organisations dependent on information technology gain value not only from preventing cyberattacks but also from responding promptly and coherently when incidents occur. This indicates that preparedness should incorporate response capability alongside preventive security. Organisations should periodically review cybersecurity procedures, communication responsibilities, critical system dependencies, and recovery priorities so that weaknesses can be identified before serious disruption occurs. Digital preparedness should also evolve as organisational technologies and business practices change. Sobb et al. (2020) demonstrate that Supply Chain 4.0 introduces distinctive operational and cyber risks through greater integration of manufacturing, telecommunications, and information technologies. Organisations should therefore avoid treating cybersecurity readiness as a one time achievement. Continuous assessment, employee learning, management involvement, and technological review can enable organisations to

maintain preparedness as digital environments evolve and strengthen their capacity to respond effectively when cyber threats affect organisational activities.

5.3 Integrating Cyber Resilience with Business Continuity

Organisations should integrate cybersecurity response and recovery arrangements directly with business continuity management. Cyber incidents can affect more than information systems because prolonged digital disruption may interrupt customer service, financial activities, communication, production, logistics, and other critical operations. Organisations should therefore identify which digital systems support essential business activities and determine how operations can continue when those systems become unavailable or compromised. Sepúlveda Estay et al. (2020) explain that cyber resilience requires organisations to respond promptly and coherently to cyber incidents in order to minimise disruption to operations. This perspective demonstrates that cybersecurity priorities should be connected with business priorities. Organisations should identify critical processes, determine acceptable interruption periods, establish recovery priorities, and develop alternative operating arrangements where appropriate. Cyber response responsibilities should also be clearly coordinated between technical teams and operational managers because restoring a system does not necessarily mean that the most important business activity has been restored. Business continuity planning should therefore incorporate cybersecurity scenarios and evaluate whether existing arrangements provide sufficient support when critical digital resources are disrupted. Integrating cyber resilience with continuity management can improve organisational coordination and ensure that limited recovery resources are directed towards activities with the greatest strategic and operational importance.

Cyber resilience should also incorporate systematic learning because recovery without improvement may leave organisations exposed to similar future incidents. Following significant cybersecurity disruptions, organisations should evaluate the effectiveness of their response, communication, decision making, recovery arrangements, and continuity processes. The objective should be to identify weaknesses and improve future preparedness rather than merely restore previous operating conditions. Cyber resilience assessment research demonstrates that resilience extends beyond prevention and incorporates organisational response and recovery capabilities (Sepúlveda Estay et al., 2020). Lessons identified after cyber incidents should consequently be incorporated into revised risk assessments, employee preparation, system protection, response responsibilities, and business continuity arrangements. Management should also determine whether disruption revealed previously unidentified dependencies between technology and critical operations. Such reviews can provide useful information for future cybersecurity investment and resource allocation. Organisations should additionally conduct periodic exercises that evaluate whether continuity arrangements remain appropriate as technologies and business processes change. Cyber resilience can therefore become a continuous organisational learning capability in which preparation, response, recovery, and improvement reinforce each other. Stronger integration between cybersecurity and business continuity can reduce operational disruption while improving the organisation's ability to adapt after significant cyber events.

5.4 Strengthening Cyber Resilience Across Digital Supply Chains

Organisations should extend cyber risk management beyond internal systems and strengthen cybersecurity arrangements across critical digital supply chain relationships. Digital supply chains increasingly involve interconnected suppliers, service providers, platforms, cloud systems, and communication technologies, meaning that vulnerabilities outside an organisation can influence its own business continuity. Sobb et al. (2020) demonstrate that Supply Chain 4.0 creates distinctive cybersecurity risks because manufacturing operations are increasingly integrated with telecommunications and information technologies. Organisations should therefore identify external partners whose systems, services, information, or technologies are critical to business operations and prioritise these relationships within cyber risk assessments. Digital preparedness should include understanding how external disruption could affect internal activities and determining whether alternative arrangements are available for particularly important services. Cybersecurity expectations should also be communicated clearly to critical partners so that responsibilities concerning information protection, incident communication, and digital access are understood. Organisations do not need identical security arrangements for every supplier because cyber risk exposure differs according to the importance of the relationship and the level of digital access involved. A risk based approach can enable management to concentrate assessment and monitoring resources on external relationships capable of creating significant organisational consequences.

Cyber supply chain resilience should also be strengthened through coordinated communication and shared preparedness among important business partners. Individual organisations may have limited ability to manage vulnerabilities across complex digital networks, making cooperation particularly important for critical dependencies. Masip Bruin et al. (2021) demonstrate that ICT supply chains involve distributed, dynamic, heterogeneous, and potentially insecure infrastructures and emphasise the need for coordinated frameworks capable of supporting cyber resilience across these environments. Organisations should consequently establish arrangements for communicating significant cyber incidents with critical partners and determine how responses will be coordinated when disruption affects interconnected operations. Such arrangements can include clear contact responsibilities, agreed communication procedures, assessment of critical digital connections, and periodic review of major third party dependencies. Cyber supply chain resilience should also be considered when organisations introduce new digital technologies because greater connectivity can create additional external vulnerabilities. Sobb et al. (2020) emphasise that increasing technological integration creates emerging cybersecurity challenges requiring stronger approaches to supply chain protection. Strengthening visibility, communication, partner assessment, and coordinated preparedness can therefore reduce external cyber vulnerability and improve the organisation's ability to maintain business continuity when cybersecurity incidents originate elsewhere within the digital ecosystem.

6. CONCLUSION

Cybersecurity has become an important strategic concern as organisations increasingly depend on digital technologies, interconnected information systems, cloud services, and external digital partners. This article establishes that building cyber resilient organisations requires more than the implementation of technical security controls. Effective cyber resilience depends on the integration of strategic risk management, digital preparedness, human capability, business continuity, and coordinated management of external cyber dependencies. Cyber risk can affect strategic objectives, operational activities, financial resources, organisational reputation, and stakeholder relationships, making cybersecurity an important responsibility for senior management and organisational governance. Strategic cyber risk management can strengthen this responsibility by enabling organisations to identify critical digital assets, understand the business consequences of cyber threats, prioritise vulnerabilities, and allocate cybersecurity resources according to organisational exposure and strategic importance.

Digital preparedness is equally important because organisational cybersecurity depends on the interaction between technology, employees, management, and organisational processes. Sophisticated security technologies may provide limited protection when employees lack cybersecurity awareness, responsibilities are unclear, or organisations are unable to coordinate effective responses during cyber incidents. The analysis demonstrates that digital preparedness should therefore be developed continuously as technologies, working practices, and cyber threats evolve. Cyber resilience should also be closely connected with business continuity because complete prevention of cyber incidents cannot always be achieved. Organisations need the capability to maintain critical activities, limit disruption, recover essential systems, and adapt after cyber incidents occur. This requires stronger coordination between cybersecurity and operational functions, supported by organisational learning that enables weaknesses identified during incidents to improve future preparedness and resilience.

The increasing interdependence of digital business environments further demonstrates that cyber resilience cannot be developed solely within organisational boundaries. Suppliers, logistics providers, cloud services, software systems, and other external partners can create vulnerabilities through which cyber risks spread across interconnected operations. Effective cyber resilience therefore requires organisations to understand critical external dependencies, assess third party vulnerabilities, establish appropriate cybersecurity expectations, and coordinate responses with important business partners. Organisations should consequently adopt an integrated approach that strengthens strategic cyber risk governance, develops continuous digital and human preparedness, connects cybersecurity with business continuity, and extends cyber risk management across digital supply chains. Through these interconnected capabilities, organisations can move from reactive cybersecurity towards a more resilient approach that supports preparedness, effective response, organisational adaptation, and the protection of long term business performance in an increasingly digital environment.

7. ACKNOWLEDGEMENT

The authors would like to express their sincere appreciation to Universiti Poly-Tech Malaysia (UPTM) for providing the academic environment and institutional support that facilitated the development of this article. The authors also acknowledge the valuable contributions of scholars and researchers whose published works provided the intellectual foundation for examining strategic risk management, digital preparedness, and organisational cyber resilience. Their scholarly contributions have significantly enriched the conceptual analysis and strengthened the academic foundation of this study.

8. CONFLICT OF INTEREST

The authors declare that there are no financial, professional, institutional, or personal conflicts of interest that could have influenced the development, analysis, interpretation, or publication of this article. The study was conducted independently, and all arguments, interpretations, and conclusions were developed in accordance with established principles of academic integrity, scholarly objectivity, and responsible research practice.

9. AUTHOR CONTRIBUTION STATEMENT

Shahri Abu Seman contributed to the conceptualisation of the study, development of the article framework, critical analysis of the literature, and preparation of the original manuscript.
Azahari Jamaludin contributed to the literature review, synthesis of scholarly evidence, analysis of strategic cyber risk management and digital preparedness, and development of the discussion and recommendations.
Ahmad Fauzi Ahmad Zaini contributed to the critical review of the manuscript, interpretation of the literature, refinement of the academic arguments, and editorial revision.
All authors participated in reviewing and improving the manuscript and approved the final version for publication.

10. ETHICS STATEMENT

This study is conceptual in nature and is based exclusively on the review, critical analysis, and synthesis of previously published academic literature and secondary scholarly sources. It did not involve human participants, personal or confidential data, clinical interventions, experimental procedures, or animal subjects. Therefore, institutional ethical approval and informed consent were not required. Throughout the preparation of the article, established principles of research ethics, academic integrity, responsible authorship, appropriate attribution of scholarly sources, and ethical publication practices were strictly observed.

REFERENCES

Abdullah, F. I., Yusof, M. S., & Abu Seman, S. (2020). Strategic Warehouse Management and Supply Chain Performance in a Changing Business Environment. *The Asian Journal of Professional & Business Studies*, *1*(2), 73–89. https://doi.org/10.61688/ajpbs.v1i2.155

Abd Wahab, N. S., & Yusof, M. S. (2020). Ergonomic Work Design and Its Influence on Healthcare Professionals' Well-being and Performance. *The Asian Journal of Professional & Business Studies*, *1*(2), 90–107. https://doi.org/10.61688/ajpbs.v1i2.298

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

Anderson, R., & Moore, T. (2006). The economics of information security. *Science, 314*(5799), 610–613. https://doi.org/10.1126/science.1130992

Andersson, J., de Lemos, R., Malek, S., & Weyns, D. (2021). Software engineering for self adaptive systems: Research challenges in the provision of assurances. In R. de Lemos et al. (Eds.), *Software engineering for self adaptive systems III: Assurances* (pp. 3–30). Springer.

Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of cyber resilient systems. *Computers & Industrial Engineering, 149*, 106829. https://doi.org/10.1016/j.cie.2020.106829

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons, 63*(4), 531–540. https://doi.org/10.1016/j.bushor.2020.03.010

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation, 34*(7), 342–353. https://doi.org/10.1016/j.technovation.2014.02.001

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. *Long Range Planning, 48*(4), 265–276. https://doi.org/10.1016/j.lrp.2014.07.005

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–548. https://doi.org/10.2307/25750690

Callahan, C., & Soileau, J. (2017). Does enterprise risk management enhance operating performance? *Advances in Accounting, 37*, 122–139. https://doi.org/10.1016/j.adiac.2017.01.001

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of Internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers. *International Journal of Electronic Commerce, 9*(1), 70–104. https://doi.org/10.1080/10864415.2004.11044320

Colicchia, C., Creazza, A., & Menachof, D. A. (2019). Managing cyber and information risks in supply chains: Insights from an exploratory analysis. *Supply Chain Management: An International Journal, 24*(2), 215–240. https://doi.org/10.1108/SCM-09-2017-0289

D'Arcy, J., & Teh, P. L. (2019). Predicting employee information security policy compliance on a daily basis: The interplay of security related stress, emotions, and neutralization. *Information & Management, 56*(7), 103151. https://doi.org/10.1016/j.im.2019.02.006

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security, 29*(2), 196–207. https://doi.org/10.1016/j.cose.2009.09.002

Duchek, S. (2020). Organizational resilience: A capability based conceptualization. *Business Research, 13*, 215–246. https://doi.org/10.1007/s40685-019-0085-7

Dupont, B. (2019). The cyber resilience of financial institutions: Significance and applicability. *Journal of Cybersecurity, 5*(1), tyz013. https://doi.org/10.1093/cybsec/tyz013

Florio, C., & Leoni, G. (2017). Enterprise risk management and firm performance: The Italian case. *The British Accounting Review, 49*(1), 56–74. https://doi.org/10.1016/j.bar.2016.08.003

Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2020). Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal, 25*(2), 223–240. https://doi.org/10.1108/SCM-10-2018-0357

Goel, S., Williams, K., & Dincelli, E. (2020). Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems, 21*(1), 22–44.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security, 5*(4), 438–457. https://doi.org/10.1145/581271.581274

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy, 22*(6), 461–485. https://doi.org/10.1016/j.jaccpubpol.2003.09.001

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications, 58*, 102726. https://doi.org/10.1016/j.jisa.2020.102726

Heidt, M., Gerlach, J. P., & Buxmann, P. (2019). Investigating the security divide between SME and large companies: How SME characteristics influence organizational IT security investments. *Information Systems Frontiers, 21*, 1285–1305. https://doi.org/10.1007/s10796-019-09959-1

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Hillmann, J., & Guenther, E. (2021). Organizational resilience: A valuable construct for management research? *International Journal of Management Reviews, 23*(1), 7–44. https://doi.org/10.1111/ijmr.12239

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. In I. Linkov & A. Kott (Eds.), *Cyber resilience of systems and networks* (pp. 1–25). Springer. https://doi.org/10.1007/978-3-319-77492-3_1

Malik, M. F., Zaman, M., & Buckby, S. (2020). Enterprise risk management and firm performance: Role of the risk committee. *Journal of Contemporary Accounting & Economics, 16*(1), 100178. https://doi.org/10.1016/j.jcae.2019.100178

Masip Bruin, X., Marín Tordera, E., Ruiz, J., Jukan, A., Ren, G. J., Zhu, J., & Farré, J. (2021). Cybersecurity in ICT supply chains: Key challenges and a relevant architecture. *Sensors, 21*(18), 6057. https://doi.org/10.3390/s21186057

Mikes, A., & Kaplan, R. S. (2015). When one size doesn't fit all: Evolving directions in the research and practice of enterprise risk management. *Journal of Applied Corporate Finance, 27*(1), 37–40. https://doi.org/10.1111/jacf.12102

Nurse, J. R. C., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R. T., & Whitty, M. (2014). Understanding insider threat: A framework for characterising attacks. In *2014 IEEE Security and Privacy Workshops* (pp. 214–228). IEEE. https://doi.org/10.1109/SPW.2014.38

Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: Conceptual framework. *Journal of Global Operations and Strategic Sourcing, 13*(1), 103–128. https://doi.org/10.1108/JGOSS-05-2019-0042

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly, 34*(4), 757–778. https://doi.org/10.2307/25750704

Radanliev, P., De Roure, D., Nurse, J. R. C., Montalvo, R. M., Cannady, S., Santos, O., Maddox, L. T., & Burnap, P. (2020). Future developments in cyber risk assessment for the Internet of Things. *Computers in Industry, 117*, 103172. https://doi.org/10.1016/j.compind.2020.103172

Schinagl, S., & Shahim, A. (2020). What do we know about information security governance? From the basement to the boardroom: Towards digital security governance. *Information & Computer Security, 28*(2), 261–292. https://doi.org/10.1108/ICS-02-2019-0033

Scholz, R. W., Czichos, R., Parycek, P., & Lampoltshammer, T. J. (2020). Organizational vulnerability of digital threats: A first validation of an assessment method. *European Journal of Operational Research, 282*(2), 627–643. https://doi.org/10.1016/j.ejor.2019.09.020

Sepúlveda Estay, D. A., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). A systematic review of cyber resilience assessment frameworks. *Computers & Security, 97*, 101996. https://doi.org/10.1016/j.cose.2020.101996

Shojaei, A., Wang, J., & Fenner, A. (2020). Exploring the feasibility of blockchain technology as an infrastructure for improving built asset sustainability. *Built Environment Project and Asset Management, 10*(2), 184–199.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487–502. https://doi.org/10.2307/25750688

Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply Chain 4.0: A survey of cyber security challenges, solutions and future directions. *Electronics, 9*(11), 1864. https://doi.org/10.3390/electronics9111864

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awareness on information technology professionals' behaviour. *Computers & Security, 79*, 68–79.

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and information security awareness. *Computers & Security, 88*, 101640. https://doi.org/10.1016/j.cose.2019.101640

Yusof, M. S. (2022). Strengthening warehouse operations through Integrated Safety Management Practices: bi. *The Asian Journal of Professional & Business Studies*, *1*(2), 56–72. https://doi.org/10.61688/ajpbs.v1i2.150

Yusof, M. S., & Abd Wahab, N. S. (2020). Advancing Sustainable Healthcare Workplaces Through Human Centred Ergonomic Work Design. *The Asian Journal of Professional & Business Studies*, *1*(2), 108–126. https://doi.org/10.61688/ajpbs.v1i2.330

Yusof, M. S., & Abd Wahab, N. S. (2020). Transforming Healthcare Work Systems Through Human-Centred Ergonomic Innovation. *The Asian Journal of Professional & Business Studies*, *1*(1), 93–110. https://doi.org/10.61688/ajpbs.v1i1.134

Yusof, M. S., & Abd Wahab, N. S. (2020). Strengthening Hospital Management Through Ethical Leadership and Professional Integrity. *The Asian Journal of Professional & Business Studies*, *1*(1), 59–75. https://doi.org/10.61688/ajpbs.v1i1.8

Yusof, M. S., & Abd Wahab, N. S. (2021). Balancing technology and ethics in the transformation of modern hospital healthcare. *The Asian Journal of Professional & Business Studies*, *2*(1), 16–34. https://doi.org/10.61688/ajpbs.v2i1.146

Yusof, M. S., & Razali, H. (2020). Navigating Organisational Uncertainty Through Risk Perception and Managerial Judgement. *The Asian Journal of Professional & Business Studies*, *1*(1), 76–92. https://doi.org/10.61688/ajpbs.v1i1.69

Yusof, M. S., Salleh, M. N., & Zahari, F. M. (2020). The Relationship between Information Technology Capability and New Product Development Success: A Conceptual Framework. *International Journal of Business and Technology Management*, 2(1), 98-112.

Yusof, M. S., Salleh, M. N., & Zahari, F. M. (2020). The Relationship between NPD Process and NPD Strategy toward NPD Success in Malaysian Automotive Industry. *Asian Journal of Research in Business and Management*, 2(1), 11-26.

Yusof, M. S., & Salleh, M. N. (2021). Beyond manufacturing towards innovation-driven new product development in Malaysia's automotive industry. *The Asian Journal of Professional & Business Studies*, *2*(1), 35–52. https://doi.org/10.61688/ajpbs.v2i1.152

Zhang, J., & He, W. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational and End User Computing, 31*(4), 1–18.

Zhang, T., Tao, D., Qu, X., Zhang, X., Zeng, J., Zhu, H., & Zhu, H. (2020). Automated vehicle acceptance in China: Social influence and initial trust are key determinants. *Transportation Research Part C: Emerging Technologies, 112*, 220–233.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Çetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269