Open Access Library Journal
2023, Volume 10, e9882
ISSN Online: 2333-9721
ISSN Print: 2333-9705

Literature Review on Building Cyber Resilience Capabilities to Counter Future Cyber Threats: The Role of Enterprise Risk Management (ERM) and Business Continuity (BC)

Awini Thomas Assibi

College of Business, Westcliff University, Irvine, CA, USA
Email: a.assibi.113@westcliff.edu

How to cite this paper: Assibi, A.T. (2023) Literature Review on Building Cyber Resilience Capabilities to Counter Future Cyber Threats: The Role of Enterprise Risk Management (ERM) and Business Continuity (BC). *Open Access Library Journal*, **10**: e9882.
https://doi.org/10.4236/oalib.1109882

Received: February 16, 2023
Accepted: April 18, 2023
Published: April 21, 2023

Abstract

The primary purpose of this paper is to critically explore the importance of building cyber resilience capabilities in organizations to counter future cyber threats. With the increasing sophistication and frequency of cyber-crimes, traditional security systems and techniques are no longer sufficient to combat them. To maintain business operations during and after a cyber-attack, it is essential to adopt a holistic approach to IT risks and create a robust cyber resilience program. The methodology adopted involved a systematic literature review on how Enterprise Risk Management (ERM) and Business Continuity (BC) contribute to building cyber resilience capabilities. The results showed that ERM and BC are critical components of cyber resilience and can help organizations identify, evaluate, and manage interruption risks. The paper concludes that organizations must maintain cyber resilience with efficient business continuity management and enterprise risk management frameworks as cyber hazards continue to increase.

Subject Areas

Business Management, Information Management

Keywords

Enterprise Risk Management, ERM, Business Continuity, BC, Risk Assessment, Risk Mitigation, Risk Monitoring, Risk Reporting, Risk Culture, Crisis Management, Disaster Recovery, Business Resilience, Risk Governance, Risk Framework

1. Introduction

In recent years, cyber threats have become increasingly sophisticated and prevalent, posing significant risks to organizations across various industries. As such, building cyber resilience capabilities has become a critical priority for organizations looking to protect their assets and reputation. To maintain company operations both during and after a cyberattack, it is essential for IT and information security leaders to adopt a holistic approach to IT risks and create a robust cyber resilience program (Goel *et al.*, 2020) [1]. This is primarily because they are now having trouble deciding which technological fields to invest their limited funds in. Information Technology may take the initiative in forging relationships with business executives and collaborating with them to confidently progress their journey toward digital transformation in a cyber-resilient environment (Goel *et al.*, 2020) [1].

Errors or external factors, such as business mergers, acquisitions, and divestitures, business unit operations and outsourcing, operational and regulatory compliance, financial and accounting operations, information technology systems, communication systems, and procedures, as well as concerns about the law, morality, and reputation, can all result in risk (Quinn *et al.*, 2022) [2]. ERM is a thorough framework for identifying and managing the risks that a company confronts. All the processes, tools, and people that make up an organization are included. Because of its robust functionality, standardization of data and processes, and customized approach to risk management that may help reduce financial risk, enterprise risk management best practices can help mitigate the hazards encountered (Quinn *et al.*, 2022) [2]. ERM is an essential component of today's businesses. Investors want it, corporate boards and top executives expect it, and customers are becoming increasingly adamant about it. Implementing ERM makes it much simpler to adhere to governmental rules for company governance and public reporting (Quinn *et al.*, 2022) [2]. The necessity for leadership at all levels of a firm to adopt resilience as a proactive strategy for managing risk across an organization is also under public scrutiny (Goel *et al.*, 2020) [1]. The purpose of this research is to examine the potential of ERM and BC in addressing cyber threats and to provide insights into how organizations can leverage these capabilities to strengthen their cyber resilience. Moreover, the paper also critically discusses how organizations can build cyber resilience capabilities to counter future Cyber Threats with a particular focus on the role of Enterprise Risk Management (ERM) and Business Continuity (BC). Specifically, this paper seeks to answer the following research questions:

1) What is the current state of cyber threats and the need for cyber resilience capabilities?

2) How can ERM be used to identify, assess, and manage cyber risks?

3) How can BC be used to ensure business continuity in the face of cyber disruptions?

4) What are the benefits and challenges of integrating ERM and BC to enhance cyber resilience capabilities?

2. How Enterprise Risk Management (ERM) and Business Continuity Contribute to Cyber Resilience

Both Enterprise Risk Management (ERM) and Business Continuity play a critical role in building an organization's cyber resiliency capabilities, thereby enabling it to counter future cyber Threats. Enterprise risk management is the strategic management of systematic risk inside a company (ERM) (Quinn *et al.*, 2022) [2]. In the last decade, there has been significant interest in digital transformation across nearly all industries. Businesses have automated more tasks, moved their servers and networks off-site, and moved their data to the cloud, but they have mostly maintained their antiquated cybersecurity practices (Carcary *et al.*, 2019) [3]. Although conditions are still not optimal, as was the case previously, the idea of cyber resilience is starting to gain momentum as an addition (or upgrade) to traditional business continuity (BC) and disaster recovery methods (Stine *et al.*, 2020) [4]. Building resilience can provide tangible advantages beyond business continuity, such as lower costs from process disruption, lower liability risk, fewer service interruptions, or better system performance. It creates a new problem for industry and the larger global community, as well as a new task for risk managers (Andronache, 2019) [5]. Many businesses had engaged in thorough crisis management plans prior to the pandemic, but they did not account for a catastrophic occurrence that would be on a worldwide scale (Carcary *et al.*, 2019) [3].

Enterprise risk management includes business continuity management as a critical component. They are complementary, and both are essential in the high-risk business world of today (Klučka & Grünbichler, 2020) [6]. The unifying objectives of ERM and BCM are to identify, evaluate, and manage interruption risks that can prohibit the attainment of their strategic goals (Klučka & Grünbichler, 2020) [6]. Business continuity management strengthens enterprise resilience and aids companies in responding to and recovering from both planned and unforeseen business disruptions. In contrast, enterprise risk management improves an organization's capacity to make risk-informed choices. When implementing an ERM and resilience plan, businesses must employ a wider range of tools to determine which risks are most crucial to their long-term well-being and then take proactive measures to increase resilience (Ghadge *et al.*, 2019) [7].

Moreover, businesses that incorporate business continuity management (BCM) into their strategic planning processes have discovered that it advances both their value generation and protection goals (Klučka & Grünbichler, 2020) [6]. Their ability to recognize and effectively manage interruption risks gives them the assurance they need to execute those strategic initiatives more audaciously. But to get that trust, ERM and BCM programs must be combined (Stine *et al.*, 2020) [4]. Organizations must maintain cyber resilience with efficient business continuity management (BCM) and enterprise risk management (ERM) frameworks as cyber hazards continue to increase (Niemimaa *et al.*, 2019) [8].

3. Role of Enterprise Risk Management (ERM) in Building Cyber Resiliency

Corporate risk management must take cybersecurity into account as businesses continue their digital transformation. In the absence of a comprehensive ERM program, organizations lack the ability to identify and assess the relationship between cyber risk and its impacts on the firm. According to (Antonucci, 2017) [9], this is why the new strategy for reducing the risks that a firm faces integrated risk management is increasingly preferred by both business leaders and security managers. It is critical to understand that cybersecurity is a risk that must be managed rather than an issue that can be fixed. Cyber risk is now a concern for the whole company in the digital era, not just the tech or IT department (Lee, 2021) [10]. Executives may make decisions with both protection and operational success in mind by approaching risks from a business viewpoint. An individual must comprehend each impact in order to assess the cyber threats that a firm may face (Stine *et al.*, 2020) [4]. Moreover, organizations may more effectively prioritize risks and next measures by including the important business context in their study of cyber hazards. According to Hopkin (2018) [11], cybersecurity has become crucial to complete corporate risk management as businesses depend more and more on technology for day-to-day operations.

Integrating cyber risk management programs with business requirements may be challenging since they are frequently created around adhering to compliance standards and laws. Security and business executives may develop an ERM that more effectively supports the larger objectives of the corporation by making cybersecurity a business problem (Niemimaa *et al.*, 2019) [8]. The data needed to establish a business environment inside of a company is already there in many businesses. Threats and their possible effects are highlighted by initiatives including achieving regulatory standards, business continuity, catastrophe recovery, and data security (Klučka & Grünbichler, 2020) [6]. The issue occurs when businesses attempt to effectively manage all of that data and transform it into useful insight. By consolidating all of the information required for risk evaluation in one location, a cyber-risk management platform may aid in this process, making it simpler to spot links between risks and estimate the size of the effect. When developing an enterprise risk management program, quantification is crucial (Niemimaa *et al.*, 2019) [8]. An organization must be able to quantify the cyber threats affecting the firm in terms of precise statistics, figures, and percentages because it is impossible to manage what cannot be measured. For the whole C-Suite and stakeholders to quickly evaluate pertinent insights and ensure everyone is aligned, the data should be devoid of jargon and easy to comprehend (Antonucci, 2017) [9].

A program for enterprise risk management that does not use all the available data will not be as effective in reducing risk. Silos of information might create unanticipated dangers or misjudged risk exposure (Andronache, 2019) [5]. As a result of combining all the data, security managers may highlight opportunities

and linkages across the company with full visibility. The organization may assess the effectiveness of the organization's risk management program by contrasting it with those of its rivals. In this way, it may investigate any problems affecting the sector and do its best to avoid having them affect the way the firm is run (Antonucci, 2017) [9].

An ERM platform should enable businesses to take a proactive approach to cybersecurity and use all current and historical threat intelligence to spot attacks and other unwanted behaviour. An organization can construct a solid, well-informed basis for its ERM program by having a thorough grasp of what has and has not worked in the past and what risks are typical within the firm or sector (Antonucci, 2017) [9]. A cyber-risk management platform should gather the information required creating an efficient enterprise risk management program from both business and IT sources. Security managers may use Security Scorecard to draw the dots between risk and impact across the company using security ratings, threat reconnaissance, compliance requirements, and vendor risk management. According to Varga *et al.* (2021) [12], this enables security managers to prioritize vulnerabilities and gives them the information they need to decide what to do next. A data-centric approach to enterprise risk management fosters cooperation throughout the business by giving executives and security manager's common ground (Varga *et al.*, 2021) [12].

Defining the fundamental company goals and then identifying the risks associated with those goals and strategies is the first stage in developing an ERM plan; the ERM plan will aid in reducing such risks. Nevertheless, it is crucial to remember that every company now confronts digital risk, which is the most significant threat (Hunziker, 2021) [13]. Businesses now face additional cybersecurity challenges due to the rising requirement to alter their operations, which has increased the number of digital data breaches. Digital contact is the primary means of internal and external communication for businesses. Companies will continue to devote more time and resources to digital transformation as digital processes continue to grow (Antonucci, 2017) [9].

4. Role of Business Continuity in Building Cyber Resiliency

Business continuity planning is a critical process of developing a strategy to identify key business risks that might result in severe disruption, preventing them where practical, and planning to enable crucial activities to continue when practical. A business continuity strategy should list a variety of hazards, such as supply chain interruption, cyberattacks, and physical occurrences (Goldstein & Flynn, 2022) [14]. The potential impact of business interruption is routinely underestimated, and cyber risk is frequently ignored. An organization can identify various cyber risks with a cyber-security business continuity strategy, which can also specify ways to avoid or lessen incidents when feasible (Carcary *et al.*, 2019) [3]. An incident response plan or cybersecurity business continuity plan has several advantages, such as minimizing business interruption by defining clear stages, actions, and responsibilities and raising overall company knowledge of

cyber hazards that can help stop events from happening. A company may ensure its incident response complies with GDPR and regulations by preparing it in advance (Goldstein & Flynn, 2022) [14].

For risks requiring coordinated responses across organizational departments, business continuity has a defined function in cyber resilience plans and has merged with cyber security (Ali *et al.*, 2020) [15]. This is extremely significant since there has been a surge in cyberattacks and the creation of new cyber threats that can seriously harm businesses, including severe financial and reputational repercussions that jeopardize their survival. The cost of cyberattacks in terms of money is rising. After last year's events, when widespread cyberattacks cost businesses millions of euros worldwide, this outcome is not unexpected (Goldstein & Flynn, 2022) [14].

Additionally, cyber security events may no longer be categorized as non-physical occurrences. Due to the complexity and quick change of the current cyber threat landscape, it is now obvious that business continuity is essential to the organization's ability to respond to incidents, manage disruptions, and avoid crises (Antonucci, 2017) [9]. Building cyber resilience still depends on business continuity, which must work with information security and cyber departments to better how businesses respond to interruptions brought on by cyber security events. When it comes to cyber security, the same rules that apply to any business continuity or disaster recovery plan should be followed, but with a knowledge of the particular risks of a cyber-attack or breach (Petrenko, 2022) [16]. The first stage in a cyber-resilience program is assessing cybersecurity risks that might disrupt crucial company processes and assets. This requires knowing and managing the threats to the company's network, IT infrastructure, and information systems (Ali *et al.*, 2020) [15].

The next step is implementing the necessary technologies, tools, and security safeguards to protect the systems, applications, and data. This component includes identity management and access control, information security policies, awareness-raising activities, and IT infrastructure maintenance (Petrenko, 2022) [16]. The final task is to search for weaknesses and questionable activity and assess how they could affect the company. This stage entails ongoing monitoring to spot cybersecurity risks and anomalies in order to safeguard sensitive data and systems against hacker assaults, hardware failures, and unauthorized access (Ali *et al.*, 2020) [15].

A strong BCM program lowers exposure to significant business interruptions and promotes enterprise-wide resilience. The program plans for disruptive events that may result in material harm and provides mitigating measures to respond to them, such as; natural or man-made catastrophes, cyberattacks, and pandemics that affect the whole world (Ghelani, 2022) [17]. Business continuity planning is becoming a crucial tool in an organization's toolbox for enhancing cyber resilience. However, to reduce cyberattacks and guarantee a quick recovery, joint solutions are required (Ali *et al.*, 2020) [15]. Breach incidents coming from a third-party provider can cause significant losses for businesses. To

achieve economies of scale, relatively few organizations choose to operate independently; instead, they choose an outsourcing model, with several suppliers helping to bring goods and services to market (Parraguez-Kobek, n.d.) [18]

Cyber resilience is made up of several different elements, including security software (antivirus and anti-malware), local machine and network policies to enforce strong passwords that are updated on a regular basis, delegated folder access privileges, and physical access security measures. Generally, business continuity normally seeks to keep a business from shutting down in an emergency (Kure *et al.*, 2018) [19]. System images, off-site data backups, redundant and remote co-located servers, plans to operate from other facilities, and redundant and remote co-located servers should all be included. Service providers must assist clients in realizing that cyber resilience is a continual process of development rather than a finished good or even a one-time service (Ghelani, 2022) [17]. Threats are ever-evolving; therefore, any strategy to counter them must, by necessity, constantly advance in each of the three crucial pillars of cyber resilience: people, processes, and technology (Parraguez-Kobek, n.d.) [18].

Companies should have a specialized talent pool to sustain the cyber resilience process, according to security experts. While many small to medium-sized companies (SMBs) find this to be unfeasible, it is at this point that MSPs may help customers buy into the notion of a continuous and committed cyber resilience strategy (Bellini *et al.*, 2021) [20]. MSPs have the chance to design ongoing security programs for cyber resilience that will empower their clients and provide recurring, highly profitable income (Bellini *et al.*, 2021) [20]. Service providers nowadays frequently create cyber resilience strategies for their own businesses to mitigate the effects of situations like ransomware or data theft (Lee, 2020) [21]. The benefit is that MSPs are already specialists due to their own internal efforts; it is not just about evangelizing a service they may be able to offer to clients (Ghelani, 2022) [17]. This information may go a long way toward convincing client firms that their MSP, who already has a thorough understanding of the client company's IT processes, is the appropriate person to handle cyber resilience (Bellini *et al.*, 2021) [20].

Small and medium-sized firms may not be aware of how widespread the threat of an attack is if they lack professional cybersecurity specialists who maintain a constant watch on adjusting to threat potentials (Kure *et al.*, 2018) [19]. Customers need to understand that although having a product in place may provide them with a sense of security about their cyber resilience, the term "people, processes, and technology have" technology in italics for a reason (Bellini *et al.*, 2021) [20]. In the end, cyber resilience is driven by people relying too much on automation, and a solution can be a fatal mistake without human intelligence to modify the technology and procedures to respond to changing threats (Bellini *et al.*, 2021) [20].

Threat-monitoring personnel need to be educated about threats, competent, and trained in the best procedures. One of the best ways to help customers appreciate the need for an ongoing cyber resilience program is to offer to do a

threat analysis (Lee, 2020) [21]. In order to identify any potential gaps and a lack of failover capabilities, the client's cybersecurity postures will be assessed as part of this vulnerability review. According to Ghelani (2022) [17], this audit may be performed by MSP personnel directly or by CISA, the Cybersecurity and Infrastructure Security Agency. After an evaluation is finished, firms are in a good position to explain to clients why more personnel, procedures, and technological advancements are required to bring a business up to the level of cyber resilience. This can entail updating firewalls, VPNs, anti-malware programs, patching and firmware, remote monitoring and administration, and a specialized team of staff that can make sure that technology and procedures are as reliable as possible (Kleij & Leukfeldt, 2019) [22].

There are a number of cybersecurity risks which are growing as a result of globalization and market demand—including interruptions to ICT continuity, cyberattacks, customer expectations, market shifts, and regulatory compliance requirements (Lee, 2020) [21]. In order to ensure that businesses have business resilience and the capacity to swiftly adjust to risks and interruptions while sustaining essential business activities and protecting personnel, assets, and brand reputation BRM was created. Business resilience is the capacity to run a company under challenging and unpredictable circumstances (Goldstein & Flynn, 2022) [14]. In addition to the traditional risks like fires, floods, economic and financial uncertainty, terrorist attacks, epidemics or pandemics like Covid 19, the most frequent risks to organizations include; IT system or service failures caused by human error, cyber-attacks, sabotage, equipment failure, and power failures. The ability to bounce back rapidly from adversity or difficulties and resume a regular condition is referred to as resilience. Therefore, resilience is the cornerstone for maintaining operations and minimizing the effects of any type of economic disruption at the corporate, regional, national, or international levels (Kleij & Leukfeldt, 2019) [22]. An organization must be able to identify all forms of risks and implement controls to lower those risks, and where those controls fall short of eliminating the risks, the organization must possess the flexibility and processes to adapt to any change in circumstances so that regular business operations can continue with little to no disruption (Lee, 2020) [21].

5. Importance of Building Cyber Resilience Capabilities to Counter Future Cyber Threats

The primary aim of cyber resilience is to provide minimally disruptive operational continuation. Instead of concentrating entirely on prevention, companies may make strategic decisions to limit disruption and shorten the cleanup period when a breach happens by preparing for an attack in advance (Papathanasiou *et al.*, 2022) [23]. Complacency has no place in the dynamic environment of today (Kure *et al.*, 2018) [19]. To make sure that their security system is impenetrable both now and in the future, organizations must change their technology, policies, and business models to concentrate on fast cyber resilience (Petrenko, 2022) [16]. One successful cyberattack is all it takes to cause mayhem, suffer sig-

nificant financial losses, or in the worst situations, completely shut down the company. In order to recognize, evaluate, manage, mitigate, and recover from harmful assaults, cyber resilience is crucial (Radanliev *et al.*, 2018) [24].

In addition to assisting in the protection of crucial systems, applications, and data, a sound cyber resilience plan also facilitates rapid recovery and business continuity in the event of disruptive cyber disasters (Radanliev *et al.*, 2018) [24]. A company will be able to continue operating normally and survive crises with the aid of a thorough cyber resilience program. Because standard security measures are insufficient to guarantee proper information security, data security, and network security, cyber resilience is crucial (Ghelani, 2022) [17]. Nowadays, a lot of CISOs and IT security teams believe that hackers will ultimately acquire access to their companies without authorization. Every day, adverse cyber occurrences have a detrimental influence on an organization's availability, confidentiality, and integrity (Radanliev *et al.*, 2018) [24].

Cyber resilience is useful for more than just defending against and surviving attacks. Additionally, it may assist the company in creating plans to enhance IT governance, increase safety and security across crucial assets, strengthen data protection initiatives, mitigate the effects of natural catastrophes, and lower human error (Kure *et al.*, 2018) [19]. Over the past ten years, third-party risk management frameworks have received a lot of attention, and for good reason. Trust, however, is a two-way street. Before requesting that the vendors implement cyber resilience plans, it is imperative that the company do so. Customer and vendor reputations may suffer if the company lacks effective cyber resilience (Settembre-Blundo *et al.*, 2021) [25].

Cyber resilience reduces the risks associated with lapses in cyber security and intrusions by online criminals. Making an interface hard to tear down is what it means when viewed through the perspective of resilience. Cyber resilience ultimately focuses on reducing risks and recovering fast in the event of an attack (Settembre-Blundo *et al.*, 2021) [25]. It enables a holistic approach to security and recognizes that there will eventually be a compromise of some kind; when taken into account, it is possible to start preparing for the worst-case situations and setting up a mechanism to drive intruders out of the data centres (Keskin *et al.*, 2021) [26]. Those in charge of cyber security should continually update their practices and adjust to new potential threats. In general, cyber resilience alerts three crucial areas for security (Keskin *et al.*, 2021) [26]. These include information security, organizational sturdiness, and operational continuity. On the other hand, technological safeguards, integrations, and preventative procedures are all part of cyber security. When businesses prepare for breaches, they will be better equipped to design robust features that enable rapid recovery and the restoration of ongoing operations (Ghelani, 2022) [17].

Without strong cyber resilience, a company would have to stop its key operating operations in the event of a cyberattack (Papathanasiou *et al.*, 2022) [23]. As a result, cyber resilience enables an organization to both combat infections and continue performing its operational tasks in the face of a cyberattack. Addi-

tionally, a far wider range of cognitive processes and interconnections are covered by cyber resilience (Kure *et al.*, 2018) [19]. Businesses and organizations are able to reinforce their systems and become more dependable by planning for the future and taking all dangers into consideration. It could also explain a change in a company's broader culture, necessitating the organization to make the appropriate adjustments in advance (Petrenko, 2022) [16]. Positive effects on an organization's regular business operations may also result from these adjustments.

According to Papathanasiou *et al.* (2022) [23], cyber resilience is concerned with what occurs if cybersecurity defences are breached as well as when systems are affected by unforeseen events like human error, power outages, and weather. Resilience considers the areas of an organization's activities that depend on technology, the locations of vital data storage, and the potential effects of interruption in those areas. The next step is to put strategies in place to lessen the effect of such interruptions (Althonayan & Andronache, 2019) [27]. A resilience strategy could include, for instance, steps to adhere to in the event of a system breach. It must first recognize where risk is present in the increasing digital ecosystem, including on-premises, on the cloud, and across business units and countries, in order to be ready for an attack and, ideally, prevent one (Lamine *et al.*, 2020) [28].

Any cyber resilience structure must include incident response teams. According to Settembre-Blundo *et al.* (2021) [25], they provide the ability to lessen the effects of cyberattacks, promptly restore services, and stop additional harm. However, it is necessary to include partners and vendors in the response activities. In the wake of a breach, hackers frequently travel laterally across the connected supply chain in search of sensitive information while also spreading malware and encrypting computers. An organization can recover from a cyberattack and guarantee company continuity by using a cyber-resilience structure (Papathanasiou *et al.*, 2022) [23]. This necessitates intensive preparation, which includes understanding system dependencies, making sure the most important data is safe and simple to recover, running attack simulations, and testing recovery procedures (Marotta & McShane, 2018) [29]. But part of rehabilitation is making sure that the same thing does not happen again. To achieve this, an organization must identify the breach's underlying cause and take appropriate action to fix it. Many businesses manage their cyber risk by looking for vulnerabilities, applying patches, and moving on to the next blaze (Lamine *et al.*, 2020) [28].

In order to prevent the types of catastrophic failures that can happen when an all-or-nothing approach to security is adopted, companies need to pay attention to cyber resilience. For instance, such a strategy can presuppose that all threats can be halted at a company's perimeter, negating the need for interior controls (Marotta & McShane, 2018) [29]. Giving users full access to an internal network just because they have a working login and password might have the same negative effects. A resilience strategy will therefore take into account activities and results before, during, and after an incident (Marotta & McShane, 2018) [29]. It

is quite probable that a company's networks will be penetrated if persistent threat actors target that organization. A company must thus be prepared to survive such attacks. A company may achieve this by being resilient, which lessens the effect of chronic threats. Resiliency in an organization's information architecture will reduce the likelihood of an attack's success and, in the event that it does, limit the damage (Jarjoui & Murimi, 2021) [30].

Redesigning and modernizing an organization's systems to be more resilient can make an enemy costlier and unpredictable, which frequently discourages cybercriminals from attacking since they want to spend as little time and money as possible. Reduced long-term risk profiles for particular enterprises and society as a whole are another benefit of resilience (Goldstein & Flynn, 2022) [14]. Businesses can only combat present risks and potential ones associated with emerging technologies, such as; quantum computing, artificial intelligence, and the Internet of Things, by considering total network resilience (Jarjoui & Murimi, 2021) [30].

6. Conclusion

In conclusion, it is crucial for organizations to adopt a comprehensive approach to IT risks and develop a strong cyber resilience program in order to preserve business operations both during and after a cyberattack. While the paper provides valuable insights on the importance of adopting a comprehensive approach to IT risks and developing a strong cyber resilience program to preserve business operations, there are some potential shortcomings that need to be considered. Firstly, the paper lacks empirical evidence and relies heavily on theoretical arguments, making it difficult to gauge the effectiveness of the proposed cyber resilience program in practice. Secondly, the paper does not provide detailed guidance on how organizations can implement the recommended approach and how to overcome potential challenges in the process. Finally, the paper does not consider the financial costs associated with building and maintaining a cyber resilience program, which could be a significant challenge for smaller organizations with limited resources.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] Goel, R., Kumar, A. and Haddow, J. (2020) PRISM: A Strategic Decision Framework for Cybersecurity Risk Assessment. *Information & Computer Security*, **28**, 591-625. https://doi.org/10.1108/ICS-11-2018-0131

[2] Quinn, S., Ivy, N., Chua, J., Barrett, M., Feldman, L., Topper, D. and Gardner, R.K. (2022) Using Business Impact Analysis to Inform Risk Prioritization and Response (No. NIST Internal or Interagency Report (NISTIR) 8286D (Draft)). National Institute of Standards and Technology, Gaithersburg. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=935699

https://doi.org/10.6028/NIST.IR.8286D.ipd

[3] Carcary, M., Doherty, E. and Conway, G. (2019, July) A Framework for Managing Cybersecurity Effectiveness in the Digital Context. *European Conference on Cyber Warfare and Security*, Coimbra, 4-5 July 2019, 78-86. https://books.google.com/books?hl=en&lr=&id=b8-hDwAAQBAJ&oi=fnd&pg=PA78&dq=cybersecurity+and++ERM+and+business+continuity&ots=KPTYyCKryo&sig=Jin0UKnI_HZ5VhAG0Tn5WU0eKgs

[4] Stine, K., Quinn, S., Witte, G. and Gardner, R. (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM). National Institute of Standards and Technology, NIST Internal or Interagency Report (NISTIR), Gaithersburg, 8286. https://complexdiscovery.com/wp-content/uploads/2020/03/NIST.IR_.8286.pdf https://doi.org/10.6028/NIST.IR.8286

[5] Andronache, A. (2019) Aligning Cybersecurity Management with Enterprise Risk Management in the Financial Industry. Doctoral Dissertation, Brunel University, London. https://bura.brunel.ac.uk/bitstream/2438/19040/1/FulltextThesis.pdf

[6] Ghadge, A., Weiß, M., Caldwell, N.D. and Wilding, R. (2019) Managing Cyber Risk in Supply Chains: A Review and Research Agenda. *Supply Chain Management: An International Journal*, **25**, 223-240. https://doi.org/10.2139/ssrn.3426030 https://www.researchgate.net/profile/Dr-Abhijeet-Ghadge/publication/334736415_Managing_cyber_risk_in_supply_chains_A_review_and_research_agenda/links/62040b49075f695e892d54d9/Managing-cyber-risk-in-supply-chains-A-review-and-research-agenda.pdf

[7] Klučka, J. and Grünbichler, R. (2020) Enterprise Risk Management-Approaches Determining Its Application and Relation to Business Performance. *Quality Innovation Prosperity*, **24**, 51-58. https://doi.org/10.12776/qip.v24i2.1467 https://www.qip-journal.eu/index.php/QIP/article/view/1467/1218

[8] Niemimaa, M., Järveläinen, J., Heikkilä, M. and Heikkilä, J. (2019) Business Continuity of Business Models: Evaluating the Resilience of Business Models for Contingencies. *International Journal of Information Management*, **49**, 208-216. https://jyx.jyu.fi/bitstream/handle/123456789/66650/1/bc%20for%20bmshare.pdf https://doi.org/10.1016/j.ijinfomgt.2019.04.010

[9] Antonucci, D. (2017) The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities. Wiley, Hoboken. https://doi.org/10.1002/9781119309741 https://www.wiley.com/en-us/The+Cyber+Risk+Handbook:+Creating+and+Measuring+Effective+Cybersecurity+Capabilities-p-9781119308805

[10] Lee, I. (2021) Cybersecurity: Risk Management Framework and Investment Cost Analysis. *Business Horizons*, **64**, 659-671. https://e-tarjome.com/storage/btn_uploaded/2021-06-15/1623738581_11813-etarjome%20English.pdf https://doi.org/10.1016/j.bushor.2021.02.022

[11] Hopkin, P. (2018) Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management. Kogan Page Limited, London. http://dspace.vnbrims.org:13000/xmlui/bitstream/handle/123456789/5077/Fundamentals%20of%20Risk%20Management.pdf?sequence=1

[12] Varga, S., Brynielsson, J. and Franke, U. (2021) Cyber-Threat Perception and Risk Management in the Swedish Financial Sector. *Computers & Security*, **105**, Article ID: 102239. https://www.sciencedirect.com/science/article/pii/S0167404821000638 https://doi.org/10.1016/j.cose.2021.102239

[13] Hunziker, S. (2021) Enterprise Risk Management: Modern Approaches to Balancing Risk and Reward. Springer, Berlin. https://doi.org/10.1007/978-3-658-33523-6 https://link.springer.com/content/pdf/10.1007/978-3-658-33523-6.pdf

[14] Goldstein, M. and Flynn, S. (2022) Business Continuity Management Lessons Learned from COVID-19. *Journal of Business Continuity & Emergency Planning*, **15**, 360-380. https://www.ingentaconnect.com/content/hsp/jbcep/2022/00000015/00000004/art00007

[15] Ali, J.A., Nasir, Q. and Dweiri, F.T. (2020) Business Continuity Framework for Internet of Things (IoT) Services. *International Journal of System Assurance Engineering and Management*, **11**, 1380-1394. https://doi.org/10.1007/s13198-020-01005-7 https://link.springer.com/article/10.1007/s13198-020-01005-7

[16] Petrenko, S. (2022) Cyber Resilience. CRC Press, Boca Raton. https://www.routledge.com/Cyber-Resilience/Petrenko/p/book/9788770221160 https://doi.org/10.1201/9781003337775

[17] Ghelani, D. (2022) Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. *American Journal of Science*, *Engineering and Technology*, **3**, 12-19. https://doi.org/10.22541/au.166385207.73483369/v1 https://d197for5662m48.cloudfront.net/documents/publicationstatus/90321/preprint_pdf/bcff668d616b9c43ffde5be665cea136.pdf

[18] Parraguez-Kobek, L., Stockton, P. and Houle, G. (2022) Cybersecurity and Critical Infrastructure Resilience in North America. In: Long, T. and Bersin, A., Eds., *Forging a Continental Future*, The North American Institutes, Washington DC, 217. https://www.researchgate.net/profile/Penny-Bamber/publication/363863410_North_America_in_Global_Value_Chains/links/6332ed0886b22d3db4e880df/North-America-in-Global-Value-Chains.pdf#page=228

[19] Kure, H.I., Islam, S. and Razzaque, M.A. (2018) An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System. *Applied Sciences*, **8**, 898. https://www.mdpi.com/2076-3417/8/6/898 https://doi.org/10.3390/app8060898

[20] Bellini, E., Sargsyan, G. and Kavallieros, D. (2021) Cyber-Resilience. In: Shiaeles, S. and Kolokotronis, N., Eds., *Internet of Things*, *Threats*, *Landscape*, *and Countermeasures*, CRC Press, Boca Raton, 291-333. https://doi.org/10.1201/9781003006152-8 https://www.taylorfrancis.com/chapters/edit/10.1201/9781003006152-8/cyber-resilience-bellini-sargsyan-kavallieros

[21] Lee, I. (2020) Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet*, **12**, 157. https://www.mdpi.com/1999-5903/12/9/157 https://doi.org/10.3390/fi12090157

[22] Kleij, R.V.D. and Leukfeldt, R. (2019, July) Cyber Resilient Behavior: Integrating Human Behavioral Models and Resilience Engineering Capabilities into Cyber Security. In: Ahram, T. and Karwowski, W., Eds., *International Conference on Applied Human Factors and Ergonomics*, Springer, Berlin, 16-27. http://activiteitgerichtwerken.nl/resources/publications/Kleij-Leukfeldt2020_Chapter_CyberResilientBehaviorIntegrat.pdf https://doi.org/10.1007/978-3-030-20488-4_2

[23] Papathanasiou, J., Belioka, M.P., Digkoglou, P. and Zopounidis, D. (2022, May) ERM-POP Model: Improving Government Initiatives towards Enterprise Risk

Management Implementation. *Proceedings of the* 8*th International Conference on Decision Support System Technology ICDSST* 2022 *on Decision Support Addressing Modern Industry*, *Business and Societal Needs*, Vol. 8, 124. https://books.google.co.ke/books?hl=en&lr=&id=7Kl3EAAAQBAJ&oi=fnd&pg=PA124&dq=Enterprise+Risk+Management+(ERM)+and+Business+Continuity++to+counter+future+Cyber+Threats&ots=ozC9t4sbeM&sig=CM42-guvokrG1wTPc0rSerNv_Qk&redir_esc=y#v=onepage&q&f=false

[24] Radanliev, P., De Roure, D., Cannady, S., Montalvo, R.M., Nicolescu, R. and Huth, M. (2018) Economic Impact of IoT Cyber Risk-Analysing Past and Present to Predict the Future Developments in IoT Risk Analysis and IoT Cyber Insurance. In: *Living in the Internet of Things*: *Cybersecurity of the IoT*—2018, Institution of Engineering and Technology, London, 1. https://doi.org/10.1049/cp.2018.0003 https://arxiv.org/ftp/arxiv/papers/1810/1810.10322.pdf

[25] Settembre-Blundo, D., González-Sánchez, R., Medina-Salgado, S. and García-Muiña, F.E. (2021) Flexibility and Resilience in Corporate Decision Making: A New Sustainability-Based Risk Management System in Uncertain Times. *Global Journal of Flexible Systems Management*, **22**, S107-S132. https://link.springer.com/content/pdf/10.1007/s40171-021-00277-7.pdf?pdf=button https://doi.org/10.1007/s40171-021-00277-7

[26] Keskin, O.F., Caramancion, K.M., Tatar, I., Raza, O. and Tatar, U. (2021) Cyber Third-Party Risk Management: A Comparison of Non-Intrusive Risk Scoring Reports. *Electronics*, **10**, 1168. https://doi.org/10.3390/electronics10101168 https://www.mdpi.com/2079-9292/10/10/1168/pdf?version=1620961080

[27] Althonayan, A. and Andronache, A. (2019) Resiliency under Strategic Foresight: The Effects of Cybersecurity Management and Enterprise Risk Management Alignment. 2019 *International Conference on Cyber Situational Awareness*, *Data Analytics and Assessment* (*Cyber SA*), Oxford, 3-4 June 2019, 1-9. https://www.researchgate.net/profile/Alina-Andronache-2/publication/332094387_Resiliency_under_Strategic_Foresight_The_effects_of_Cybersecurity_Management_and_Enterprise_Risk_Management_Alignment/links/5d02be77a6fdccd130991fd7/Resiliency-under-Strategic-Foresight-The-effects-of-Cybersecurity-Management-and-Enterprise-Risk-Management-Alignment.pdf https://doi.org/10.1109/CyberSA.2019.8899445

[28] Lamine, E., Thabet, R., Sienou, A., Bork, D., Fontanili, F. and Pingaud, H. (2020) BPRIM: An Integrated Framework for Business Process Management and Risk Management. *Computers in Industry*, **117**, Article ID: 103199. https://www.sciencedirect.com/science/article/abs/pii/S0166361520300890 https://doi.org/10.1016/j.compind.2020.103199

[29] Marotta, A. and McShane, M. (2018) Integrating a Proactive Technique into a Holistic Cyber Risk Management Approach. *Risk Management and Insurance Review*, **21**, 435-452. https://doi.org/10.1111/rmir.12109 https://www.researchgate.net/profile/Michael-Mcshane-4/publication/329709919_Integrating_a_Proactive_Technique_Into_a_Holistic_Cyber_Risk_Management_Approach_A_Holistic_Cyber_Risk_Management_Approach/links/5efca43392851c52d60cc56f/Integrating-a-Proactive-Technique-Into-a-Holistic-Cyber-Risk-Management-Approach-A-Holistic-Cyber-Risk-Management-Approach.pdf

[30] Jarjoui, S. and Murimi, R. (2021) A Framework for Enterprise Cybersecurity Risk

Management. In: Daimi, K. and Peoples, C., Eds., *Advances in Cybersecurity Management*, Springer, Berlin, 139-161. https://doi.org/10.1007/978-3-030-71381-2_8
https://www.researchgate.net/profile/Renita-Murimi/publication/352435737_A_Framework_for_Enterprise_Cybersecurity_Risk_Management/links/629f40696886635d5cc6fdd0/A-Framework-for-Enterprise-Cybersecurity-Risk-Management.pdf