Journal of Informatics and Web Engineering

Vol. 2 No. 2 (September 2023) eISSN: 2821-370X

Building Cyber Resilience: Key Factors for Enhancing Organizational Cyber Security

Thavaselvi Munusamy[1*], **Touraj Khodadadi**[2]

[1,2] School of Information Technology, Malaysia University of Science and Technology, Block B, Encorp Strand Garden Office, No. 12, Jalan PJU 5/5, Kota Damansara, 47810 Petaling Jaya, Selangor, Malaysia

**corresponding author: (thavaselvi.munusamy@phd.must.edu.my; ORCiD: 0009-0004-2807-6987)*

Abstract - The increasingly pervasive influence of technology on a global scale, coupled with the accelerating pace of organizations operating in cyberspace, has intensified the need for adequate protection against the risks posed by cyber threats. This paper aims to identify cyber resilience management attributes that can enable organizations to sustain and continually adapt in the face of evolving cyber risks and threats. The researcher explores the intersections between cybersecurity and resilience by reviewing existing frameworks, models, studies, and surveys. This study establishes the attributes of resilience with the integration of resilience theory and security theory, along with their position in the cyber domains. By proposing a converged model with fundamental factors for attaining cyber resilience, this study offers a novel contribution to cyber security management.

Keywords— Cyber Resilience, Cyber Security, Cyber Risk, Cyberattack, Organisational Resilience

Received: 14 December 2022; Accepted: 19 May 2023; Published: 16 September 2023

I. INTRODUCTION

Organizations are increasingly adopting technology to stay competitive and relevant in this era. However, increased dependence on technology and connectivity means greater exposure to cyber risk. Connecting to the internet makes organizations visible in a globalized world where disruption can come unexpectedly, causing significant damage and financial losses [1]. In addition, the Covid-19 pandemic accelerated the shift towards digital and remote working, further exacerbating the situation and leading to more vulnerabilities [2] and cyber adversaries. Technology-related risks, including cyber-related ones, are regarded as top risks, and in the latest 2023 Global Risk Report, it is one of the top 5 risks for Malaysia [3]. TAs technology continues to outpace organizations' ability to understand the environment, organizations must enforce cyber resilience to ensure that they can operate safely and effectively in the cyber realm. While cybersecurity-related studies have gained traction, scholars contend that the management approach toward security lacks clarity [4], is outdated, inadequate, and fails to comprehensively address an organization's security requirements [5]. They argue that cybersecurity frameworks primarily focus on security-related regulations and standards, adopt a traditional perspective of protection and prediction, and prove ineffective in a highly uncertain environment and a volatile cyberspace with unknown risks [6]. Hence, it prompts the question of effectively establishing cyber resilience within organizations. From these perspectives, it is evident that there is a need to explore cyber resilience. This research aims to establish a common reference point specifically related to cyber resilience in management.

Journal of Informatics and Web Engineering
https://doi.org/10.33093/jiwe.2023.2.2.5

Published by MMU Press. URL: https://journals.mmupress.com/jiwe

This research article identifies the gaps in cybersecurity and its relationship with cyber resilience within practical and theoretical domains. The study also helps to understand resilience attributes identified in the different dimensions of cyberspace domain areas to help align the industry towards cyber resilience-related attributes. By doing so, organizations can robustly meet the current cybersecurity needs and challenges. The rest of the article comprises the following sections: Section 2 briefly introduces the background of this study, exploring the concept of resilience and the rationale for cyber resilience. In Section 3, the existing frameworks and the gaps are discussed, while in Section 4, the research framework developed through the assimilation of attributes identified from existing studies along with their relevance towards achieving resilience, incorporating additional insights and enhancements. Section 5 concludes how the study can help bridge the gap. To the best of the researcher's knowledge, at the time of this study, no previous research has been undertaken to investigate the attributes of resilience by integrating resilience theory and security theory within the context of cyber domains. In this regard, this study sets the groundwork for enhancing organizations' cyber resiliency and establishing a broad framework for cyber resilience to combat cyber issues effectively.

II. BACKGROUND

The concept of "resilience" has been in use since the 1970s, when Holling first introduced it in the context of ecological systems. Since then, its application has expanded into transdisciplinary fields. The study of resilience has gained significant momentum and importance, particularly in emerging multidisciplinary fields often associated with sustainability [7],[8]. In recent years, global government and commercial sectors have introduced several cyber resilience initiatives, but it often overlaps with cyber risk management and is considered synonymous with cyber security. Currently, there is no common reference point explicitly related to cyber resilience, necessitating cyber resilience to be explored as a standalone topic. It helps to clarify the ambiguities in the taxonomy and extend the formal representation of the traits related to cyber resilience management. Given the broad scope of the resilience concept, a comprehensive understanding of existing resilience practices in various frameworks across multiple industries and technologies helps an organization advance and achieve a complete understanding. Moreover, it is necessary to comprehend the existing gaps in cybersecurity and its relationship with cyber resilience from both practical and academic perspectives to enhance cybersecurity practices to achieve resilience.

A. Cyberspace and Cyber Risk

Cyberspace is a term used metaphorically to refer to a space within the internet. It was used synonymously with the internet as a virtual networked communication [9]. However, recent definitions of cyberspace have emphasized that it is a domain characterized by the combined use of electrons and the electromagnetic spectrum for communication, and not the same as the Internet [10]. In cybersecurity, cyberspace refers to internetworked entities that facilitate information flow [11]. Cyberspace has multiple layers, with the primary simplified forms being physical (architectural/geographic), logical (software layers), and social layers [12], [13], as depicted in Figure 1. Some studies present cyber domains as physical, information, cognitive, and social domains. This study focuses on the layers of cyberspace where human and computing processes are integrated.

Initially, cyber risk was associated with threats arising from Internet use, and gradually, anywhere with the evolution of technology, cyber risk is regarded as threats arising from cyberspace [4]. Scholars contend that a uniform and broadly accepted definition of cyber risk is required as the existing ones are considered incomplete [9]. Based on existing studies, cyber risk is the potential for financial loss, disruption, or harm to an organization's reputation resulting from failures in its information technology systems [1], [4]. While the risks are within the confines of cyberspace, organizations operate in a boundaryless environment where threats can originate from the world. The rapid adoption of cloud technology and mobile computing further amplifies the risk posed by adversaries. Cyber risk is commonly classified as either malicious, arising from intentionally exploiting vulnerabilities or threats, or non-malicious, typically resulting from inadvertent exposure due to a lack of awareness or security measures.

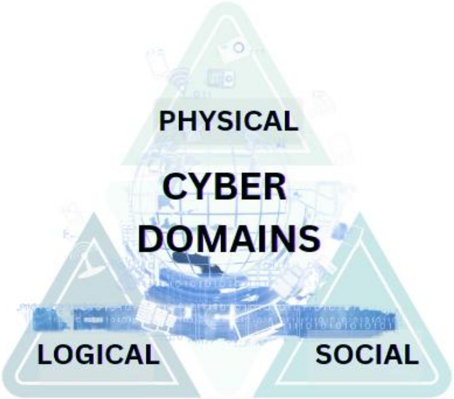

Figure 1. Cyber Domains

B. Cyber Security and Resilience

Cyber resilience refers to an organization's continuous ability to achieve its intended outcomes despite adverse cyber events [14],[15]. The NATO definition is more specific, defining cyber resilience as the ability to prepare for, adapt to, withstand, and rapidly recover from disruptions resulting from deliberate attacks, accidents, or naturally occurring threats or incidents. The World Economic Forum report [3] defines cyber resilience as the ability of systems and organizations to withstand cyber events, measured by the combination of mean time to failure and mean time to recovery. Recent research suggests that an adaptive approach and anticipating future challenges are necessary for resiliency. Some researchers define it more broadly as the ability to efficiently reduce the magnitude and duration of deviations from targeted system performance levels during a disruptive event. Despite slight variations in definitions, the concept of cyber resilience remains vital as the ability of a system to defend against cyberattack incidents, maintain critical functionality, and restore the quality of services to pre-incident levels. Overall, the main aim of cyber resiliency can be defined as the ability of the organization to prepare, defend, recover, adapt, and learn from cyber events.

C. Rationale – Why Cyber Resilience Management is needed?

With the rise of technological advances and cyber-dependency, there is a corresponding increase in cyber-related issues [16]. To address these problems, the Malaysian Communications and Multimedia Commission has urged organizations to improve security measures for users and service providers. The National Policy Document recommends implementing ISO/IEC 27001:2013 Information Security Management System (ISMS) or equivalent security best practices to reduce the risk of cybersecurity incidents. However, implementing frameworks and standards is based on organizational needs and capacity and does not explicitly include resilience. The primary challenges associated with the cyber environment include the inevitability of cyberattacks and the constantly evolving technological landscape while existing cybersecurity solutions often lack an integrated approach to addressing cyber risks. Organizations need a new resilience mindset by replacing traditional approaches using the "protection" and "prediction" concepts. Also, current security measures will degrade as technology evolves; therefore, preparation to withstand and adapt to risks is crucial. The Council of Competitiveness also echoes this view and identifies that organizations must be able to anticipate risk, limit the impact, and bounce back. Harvard Business Review reverberates as it suggests that organizations adopt a strategic resilience approach to continually develop the capacity to reinvent business models and adjust to changes or setbacks [17].

III. LITERATURE REVIEW

A. Overview

Cyber resilience is characterized by a focus not only on prevention and protection but also on reliability and the ability to recover from cyberattacks, adaptability, and learning from adversity. The methods investigated in this study aim to enhance the cyber resilience of businesses, thereby reducing the risk of significant financial loss, reputational damage, and legal consequences resulting from a cyberattack. Ultimately, a cyber resilience model can enable organizations to continually adapt to new information and adversaries to remain relevant in the fight against cyber threats. Existing resilience frameworks tend to be foundational, describing basic traits or attributes, and are focused mainly on adaptability, with the implementation providing a limited approach towards protection, mitigation, and problem-solving.

B. Theoretical Framework

The initial literature reviews on resilience in organizations mainly focused on their ability to withstand external threats [18], adapt to uncertainty, and be flexible [19]. According to Mallack, resilience is synonymous with adapting quickly to the changing environment [18]. Scholars emphasized that the key to resilience lies in adapting to new requirements [20]. However, the predominant focus of these reviews was on preparedness and adaptability, with limited attention paid to other aspects of resilience. Existing resilience frameworks are foundational, describing essential traits or attributes and focused on a single aspect, with limited implementation towards protection, mitigation, and problem-solving. A recent study strategically identified several attributes of resilience that form the building blocks of existing frameworks, including bouncing back, robustness, absorbing and thriving, learning and developing [12] [21]. Another study identified several principles that contribute to building resilient attributes, including perceiving experiences constructively, performing positive adaptive behaviours, ensuring adequate external resources, expanding decision-making boundaries, practicing bricolage, developing a tolerance for uncertainty, and building virtual role systems [18]. To further explore resilience attributes, we examined frameworks used to deploy cybersecurity or solutions and identified core attributes related to resilience.

C. Existing Cyber Security Models and Resilience Frameworks

1) Organization Resilience Frameworks – ISO22316

The International Organization for Standardization (ISO) developed ISO 22316 Security and Resilience to provide principles and guidelines for establishing organizational resilience. In this standard, organizational resilience is defined as "the ability of an organization to absorb and adapt to a changing environment, enabling it to deliver its objectives, survive, and prosper." The standard acknowledges no one-size-fits-all approach to achieving resilience [22]. The standard identifies nine attributes as depicted in Table 1, that contribute to building resilience, including a shared vision and clarity of purpose, understanding, and influencing, effective and empowered leadership, supportive culture, sharing of information and knowledge, availability of resources, development, and coordination of management disciplines, continual improvement, and the ability to anticipate and manage change. The standard's activities are primarily focused on management, organization, development, and coordination, focusing on supporting continual improvement and managing change while establishing principles and activities that promote organizational resilience.

2) Information Security Management System (ISMS) - ISO27001:2013 and ISO27001:2022

In the industry, ISO27001 is in general used to assess an organization's ability to meet information security requirements and implement a risk-based approach to cybersecurity [22] and called the "common language" for information security [23]. While the terms "information security" and "cybersecurity" are often used interchangeably, it is essential to note that there is a difference between them [1]. The ISO27001 standard focuses on preserving confidentiality, integrity, and availability of information assets by systematically managing three main components: people, process, and technology, using a risk-based approach. Several researchers have observed that ISO27001 does not indicate an acceptable level of risk, and it is up to the organization's management to decide on the type and level of security they want [5][24]. Poor risk management and low-risk awareness in the organization may result in the ineffective implementation of the cybersecurity program using ISO27001.

Table 1. ISO22316 - Security and Resilience

Attributes	Example Activities
Shared Vision and clarity of purpose	Monitor and review organizations strategies, purpose, vision, values, and objectives regularly and articulate core values to all stakeholders.
Understanding and influencing context	Think beyond current activities, organizational boundaries, interdependencies, under changing circumstances.
Effective and empowered	Empower all levels for enhanced decision making and lead under uncertainty and disruption, encourage creation and sharing lessons learnt.
Culture supportive of organizational resilience	Having a shared beliefs and values, positive attitudes, and behaviour.
Shared information and knowledge	Learning from experience and all available sources.
Availability of resources	Resources are maintained based on capacity, diversification, replication, and redundancy to avoid single point of failure.
Development and coordination of management disciplines	Design, development and coordination of management disciplines and their alignment with organization's strategic objectives.
Supporting Continual Improvement	Organization continually monitor performance against predetermined criteria to learn and improve from experience.
Ability to anticipate and managing change	Organization could anticipate, plan, and respond to change.

Table 2 depicts 14 domain areas of ISO27001:2013, with 114 controls in Annex A, which eventually revised to four main categories in ISO27001:2022 (as shown in Figure 2) with a total of 93 controls. The controls provide direction in readiness, resistance, response, and recovery. It is important to note that the controls are not mandatory, and organizations can choose to implement them based on their risk assessment and information security needs. The robustness of an organization's security depends on the organization's risk approach. For example, the standard has a control that directs the organization to learn from a past incident. However, there is no mention of adjusting to the changing nature of the organization's environment, which is one of the attributes of resilience. However, the concepts stated in the ISO27001 standard can be used to assess and manage cybersecurity risks and contribute towards cyber resilience.

Table 2. ISO27001:2013 – Information Security Management System (ISMS)

Domains	
IT security policies	Operational security
	Communications security
	System acquisition, development, and maintenance
Organisation of information	
	Supplier relationships
Human resources security	Information incident Management
Asset management	
Access control	Information aspects of business continuity management
Cryptography	
Physical and environmental security	Compliance

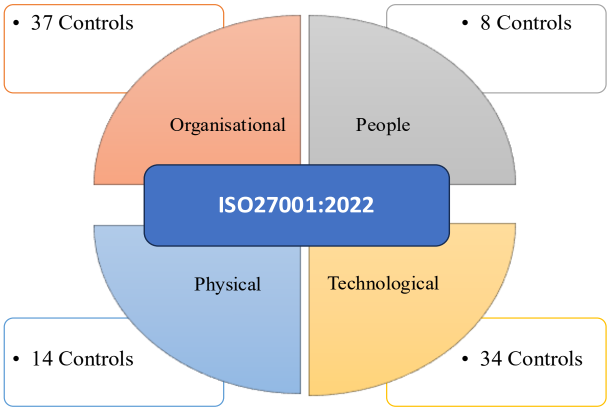

Figure 2. ISO27001:2022 – Information Security Management System (ISMS)

3) NIST

The NIST framework is a high-level, voluntary framework consisting of standards, guidelines, and practices for managing and improving critical infrastructure cybersecurity. The framework is referred to as voluntary due to the absence of enforcement or mandated controls, unlike the ISO 27001 Standard, which requires specific controls as mandatory [25]. The framework comprises three main components: the Core, Implementation Tiers, and Profiles. The Core component focuses on technical security controls, the Implementation Tiers evaluate risk assessment practices, and the Profile Tier reflects adoption within a specific industry or organization. In addition, the Core Framework consists of four elements: Functions, Categories, Subcategories, and Informative References. The five functions of NIST indicate the concept of the cybersecurity framework depicted in Figure 3. These elements operate concurrently and continually, providing a high-level, strategic view of an organization's cybersecurity risk management [26].

The NIST framework adopts a risk-based implementation, allowing organizations to select an appropriate risk management method similar to ISO 27001's approach. However, this approach earned criticism as organizations may need to be vigilant when determining the level of risk, as complacency may result in weak cybersecurity program implementation. Another important consideration is that the NIST framework is primarily developed for dealing with cyber-attacks rather than achieving resilience. Furthermore, a voluntary approach to cybersecurity guidelines may reduce investment in achieving a secured cyberspace if implementation costs are high or additional resources are required [27]. Hence, successfully implementing the NIST framework requires buy-in from the appropriate stakeholders, particularly decision-makers, to be aligned toward cyber resilience.

3) NIAC

The NIAC Resilience Model is a framework developed by the National Infrastructure Advisory Council of the United States to address the need for resilience in critical infrastructure. The council formed a working group that came up with resilience constructs identified as "robustness," "resourcefulness," "rapid recovery," and "adaptability," as shown in Table 3. However, the NIAC model's primary purpose is to determine the resilience goals from the perspective of the industry-specific sector. Therefore, the model provides a high-level resilience goal that enables the organization to interpret resilience in its business context. While this approach allows the organization to implement resilience constructs that they deem necessary, the broad approach is open to interpretation. It may defeat the purpose of cyber resilience if not rightly executed. Although the NIAC Resilience Model and cyber resilience share similar purposes of enhancing an organization's ability to withstand and recover from disruptions, they differ in their approach. The NIAC Resilience Model aims to identify resilience goals specific to industry sectors. In contrast, cyber resilience focuses on building a holistic and adaptive cybersecurity framework that can mitigate and respond to various cyber threats.

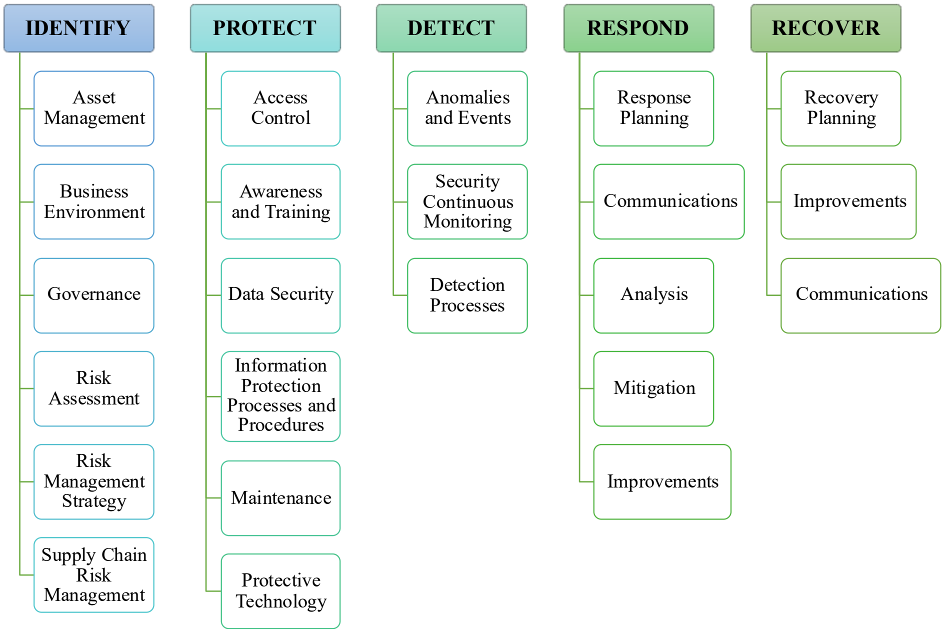

Figure 3. NIST Framework

Table 3. NIAC Resilience Framework

Resilience Construct	Description
Robustness	The ability to keep operating by having substitute or redundant systems.
Resourcefulness	Primarily on people, to skillfully manage disaster, control damage and communicating decisions.
Rapid Recovery	Capacity to get back to normal as quickly as possible after a disaster.
Adaptability	Absorb new lessons, revise plans, and introduce new tools and technologies to improve robustness, resourcefulness, and recovery capabilities.

3) Cyber resiliency engineering framework - CREF

The Cyber Resiliency Engineering Framework, also known as CREF, was developed by MITRE approximately a decade ago in 2011 to manage cyber threats. The framework comprises four main goals, including anticipating potential threats or adversaries, withstanding attacks or adversaries, recovering or restoring business functions after an attack, and adapting business functions to minimize the impact of an attack. CREF provides goals, objectives (as depicted in Table 4), practices, costs, and metrics for resilience and is designed to protect an organization against cyber threats using resilience engineering, mission assurance engineering, and cybersecurity concepts. However, recent studies have indicated that achieving cyber resiliency requires considering various aspects of adversaries within cyberspace. The model assumes that fundamental cyber security aspects exist and hence focuses on actions to ensure business continuity in the event of an attack [26]. As such, it is seen as a "complementing" model to existing cybersecurity models. CREF provides a structure for understanding the interrelated aspects of cyber resiliency rather than defining the attributes. However, compared to ISO's Security and Resilience framework, the CREF model needs more focus on leadership aspects, for example, clarity of purpose, which is necessary for decision-making at all levels to ensure resilience [5].

Table 4. CREF Framework

Objectives	Description
Understand	Maintain useful representations of mission dependencies and the status of resources with respect to possible adversity
Prepare	Maintain a set of realistic courses of action that address predicted or anticipated adversity
Prevent / Avoid	Preclude the successful execution of an attack or the realization of adverse condition
Continue	Maximize the duration and viability of essential mission / business functions during adversity
Constrain	Limit damage from adversity
Reconstitute	Restore as much mission / business functions and supporting processes to handle adversity more effectively
Transform	Modify mission/ business functions and supporting process to handle adversity more effectively
Re-architect	Modify architectures to handle adversity more effectively

D. Initial Findings and Gap

As cyber resilience is a relatively new area of study, there is limited research on the topic. Existing studies tend to focus on industry-specific needs. For example, Maziku et al. [15] developed a model to measure security scores for the smart grid domain's persistent attack, but the study lacks the relevance of security controls for resilience. Likewise, Lykou et al. [14] researched cyber resilience for airline systems without distinguishing between attributes for cyber security and those for resilience. Similarly, Babiceanu and Seker [28] assumed that preventive measures would make the industrial Internet of Things resilient but did not consider attributes such as resourcefulness. Other studies have aligned with industry-specific objectives and utilized standards such as ISO 27001 and the NIST framework. However, there is no standard approach to determine resilience attributes, and researchers have yet to demonstrate its application in policies, frameworks, or processes. Also, while some studies have presented resilience metrics for cyber systems, such as the research conducted by Linkov et al. [12], these metrics have remained focused on managing disasters and recovery.

In the earlier constructs, resilience practices related to cyber security consist of four abilities which are 1) Robustness; 2) Resourcefulness; 3) Rapid Recovery, and 4) Adaptability [29] and subsequent work by several researchers defined similar attributes from which the NIST Cybersecurity framework derived its own set of functions as an enhancement from the earlier works. ISO22316 framework emphasizes the management's role in making the organization more resilient as crucial, for example, in the attributes that mandate management's role in having a clear purpose and strategy in influencing and enhancing the organization's culture towards being resilient. On the contrary, the CREF framework, introduced in 2018, has several objectives that complement goals for achieving resilience, but the management perspective was omitted, which could be due to the framework being developed as a complementing framework. Hence, through this study, the existing gaps will be addressed by developing a model with a converged cyber resilience approach.

IV. THE RESEARCH FRAMEWORK

The constantly evolving cyberspace and technology landscape requires a multifaceted approach to cover cyber risks adequately. To survive and rebound from cyber-attacks, organizations must prioritize cyber resilience. However, "resilience" has a distinct meaning from "security”, and security alone does not guarantee resilience. This study systematically examines existing frameworks and cyber security models to identify attributes that contribute to establishing resilience. This study addresses gaps in current cybersecurity models which are currently, focusing on technical security and survivability. The challenge to develop an integrated model for cyber resiliency lies in identifying the core attributes that demonstrate resilience.

The proposed model integrates the main resilience objectives from ISO's Security and Resilience (ISO22316) and CREF's cyber security management to provide a comprehensive approach to cyber resilience as depicted in Table 5. Core resilience variables are identified based on their relevance to achieving resilience. CREF is based on three main concepts: Systems Security Engineering, Security Operations and Management, and Systems Engineering for Performance and Management, focusing on cyber threats. In contrast, ISO22316 emphasizes the critical role of management in embedding a resilient culture within the organization. The ISO22316 standard, specifically designed for organizational security resilience, complements MITRE's Cyber Resilience Engineering Framework (CREF) and serves as an ideal foundation for identifying key factors. The factors were selected based on their ability to bridge gaps in CREF and to provide a base for constructing an enhanced framework for cyber resilience. The key factors are then extended to cover the cyber domains, which are the physical, logical, and social, to provide a comprehensive approach towards achieving resilience.

Table 5. Cyber Resilience Key Factors

ISO Organizational Resilience	**CREF Resilience Objectives**	**Proposed Cyber Resilience Attributes**
Shared Vision and clarity of purpose	Maintain useful representations of mission dependencies and the status of resources with respect to possible adversity	Rationale
Understanding and influencing context	Maintain a set of realistic courses of action that address predicted or anticipated adversity	
Effective and empowered		Reliable
Culture supportive of organizational resilience		
Shared information and knowledge		Reflective
Availability of resources	Maximize the duration and viability of essential mission / business functions during adversity	Readiness
	Restore as much mission / business functions and supporting processes to handle adversity more effectively	
Development and coordination of management disciplines	Preclude the successful execution of an attack or the realization of adverse condition	Robust
Supporting Continual Improvement		Rebound
Ability to anticipate and managing change	Modify mission/ business functions and supporting process to handle adversity more effectively	Resistance
	Modify architectures to handle adversity more effectively	

A. Cyber Resilience and Rationale (Purpose Vision and Values)

ISO22316 emphasizes the importance of establishing a clearly defined objective to ensure that an organization's strategic direction, decision-making process, and activities are aligned. Accordingly, MITRE's [26] objective of cyber resiliency specifies that "anticipating" threats requires organizations to adopt a proactive approach to prevent attacks. This proactive stance encompasses identifying objectives and delineating stakeholder responsibilities, which should be integrated across various cyber domains to promote collaboration and cooperation at all levels. Hence, effective cyber resilience management requires a deep understanding of the organization's purpose, vision, and values concerning the security needs of the environment and infrastructure, as well as clarity regarding the data that the organization handles. Moreover, decision-making levels must articulate and promote the cyber resilience strategy to ensure effective implementation.

B. Cyber Resilience and Reliable (Empowered Culture)

The concept of reliability primarily pertains to the ability of a system to maintain its operational state even in the face of adverse events. However, within the cyber resilience framework, reliability expands beyond the physical system to encompass the logical and social domains. The overarching objective is establishing dependability across the entire system, including its assets and resources. Scholars highlighted in their research that reliability is determined by the likelihood of the system or network functioning as required, particularly in challenging circumstances [8]. Scholars have emphasized the need to consider degradation and the potential for failures when assessing the reliability of resources employed to safeguard the cyberspace with which organizations engage [30]. It is imperative to extend the reliability to all three cyber domains to adopt a comprehensive approach. Therefore, from a management perspective, the reliability of a team becomes crucial; an empowered and efficient team capable of making decisions amidst uncertainty and disruption significantly contributes to achieving resilience.

C. Cyber Resilience and Readiness (Availability of Resources)

Readiness is essential in cyber resilience management, which involves preparing resources and anticipating possible cyber incidents. Readiness also considers factors focusing on adapting to the constantly evolving cyberspace. Initially, readiness is associated with the coordination and availability of resources with skills and knowledge and the ability to respond quickly to threats and risks [31] and is considered one of the most important security aspects [29]. It is prevalent in most of the frameworks discussed earlier in this study. This capability is also closely tied to an organization’s ability to foresee possible threats [26] and readiness to combat the situation [12], an important aspect of resilience. The same was reiterated by research reviewing the organization context to prepare or anticipate threats [7]. This study reemphasizes and extends the attribute to physical, logical, and social domains, including the availability and functionality of systems during changes in the environment, preparedness in the event of adverse events, monitoring and evaluating changing circumstances, the ability to respond and adapt to changes, and upskilling resources to support the organization in maintaining readiness.

D. Cyber Resilience and Resistance (Avoidance of Single Point of Failure)

The idea of "resistance" was discussed in the same context as survivability in earlier studies. For an organization to be resilient, it includes capability that prevents it from being affected during adversity. Hence, to attain resistance, cyber security includes redundancy and remediation against failures [1] and the ability to prevent cyber resource attacks [32]. The general idea to attain resistive resilience is to ensure there are physical, logical, and social resources to protect and defend against attack and redundancy with remediation capabilities that enable the system to resist failures. Hence, resistance can be summarized as the ability to defend the organization against cyber threats and attacks. This study identifies "resistance" as using deterrent techniques to prevent attacks, control to limit the accessibility and readability of information, segregation of access, establishing proper roles and responsibilities, and adapting without impacting existing functions.

E. Cyber Resilience and Robust (Development and Coordination to Respond to Threat and Risks)

The derivatives of ISO's Security and resilience on being robust include its resources to respond to threats and risks [22]. Being robust also requires the management to adapt to evolving technologies [8], [15] which supports the organization to adjust to new norms. Robustness requires an organization to effectively develop and coordinate resources to respond to cyber threats and risks and ensure the capability to avoid a single point of failure. This factor assesses an organization's ability to recognize critical resources and address their weaknesses, build flexibility to absorb and enhance its capabilities, improve communication, coordination, and integration between systems, regularly assess management practices, and ensure the availability of resources to respond to incidents and changes.

F. Cyber Resilience and Rebound (Promote Continual Improvement)

ISO's standard for security resilience emphasizes the importance of ongoing enhancement, whereby organizations continuously validate their procedures and processes to ensure their relevance and suitability in response to evolving needs. From a cyber resilience standpoint, the ability to rebound signifies an organization's capacity to effectively navigate the dynamic landscape of evolving technologies and adapt to new requirements. In a challenging environment where the occurrence of cyber-attacks is deemed inevitable, the capability to "recover" or "restore" [8] remains of utmost significance. Rebound is a pivotal factor in promoting continual improvement towards achieving cyber resilience. The measure of rebound extends to the organization's ability to adapt and redeploy its capabilities considering environmental changes, as well as through a leadership review of resource appropriateness, availability, and allocation. Additionally, periodic assessments of organizational behaviour enable necessary adjustments to accommodate evolving conditions, reinforcing the purpose of cyber resilience.

G. Cyber Resilience and Reflective (Lesson learnt and Knowledge Sharing)

The factor of "reflective" plays a vital role in advancing cyber resilience by emphasizing the significance of leveraging lessons learned and facilitating knowledge sharing [22]. It entails transforming and rearchitecting objectives to align with evolving needs and understanding the necessity of adaptation [26]. This factor encompasses various elements, including establishing a knowledge base that systematically captures and preserves lessons learned within the organization. It encourages creating and disseminating insights derived from successful endeavours and failures while promoting the adoption of best practices. Additionally, it involves implementing processes for knowledge creation and sharing across all levels of the organization. The factor assesses the organization's ability to leverage past experiences and adapt to emerging technologies and new challenges. Lastly, it evaluates the organization's promptness in sharing lessons learned with all relevant parties and stakeholders.

V. CONCLUSION

Multiple studies related to the cyber security concept exist on cyber security, which emerged as a pioneering field in the era of information systems and has gained widespread adoption in the industry. Compared to the well-established concept of cybersecurity, the idea of resilience in securing cyberspace is relatively new. Understanding the similarities and differences between these two concepts can aid in identifying overlapping controls and opportunities for integration between security and resilience. Although various cyber security management frameworks exist, the literature review highlights that these models primarily centre around the principles of protection and prevention, with limited emphasis on resilience strategies. Furthermore, the current cybersecurity approach is considered inadequate for assuring cyber security. As a result, a resilient approach, with its adaptive nature, is deemed more appropriate for safeguarding cyberspace. This study examines existing frameworks, standards, and models from a resilience perspective to identify significant and relevant attributes for modelling cyber resilience and to prevent misconceptions and misrepresentations. Acquiring a comprehensive understanding of these distinctions will be invaluable in identifying shared controls, further establishing the key factors for cyber resilience, and complementing the management issues related to ever-evolving cyber risks. A resilient approach is believed to bridge the gap left by the traditional cybersecurity approach.

ACKNOWLEDGEMENT

The authors would like to thank the two anonymous reviewers who have provided valuable suggestions to improve the article.

REFERENCES

[1] R. Von Solms and J. Van Niekerk, “From information security to cyber security”, Computers & Security, vol. 38, pp. 97-102, 2013.

[2] J. Kaplan, C. Toomey and A. Tyra, “Critical resilience: Adapting infrastructure to repel cyberthreats”, McKinsey & Company, 2019.

[3] World Economic Forum, “Annual Report 2020-2021”, 2020. https://www.weforum.org/reports/annual-report-2020-2021.

[4] A. Refsdal, B. Solhaug and K. Stolen, “Cyber-risk management”, Springer Briefs in Computer Science, Springer, pp. 32 – 35, 2015.

[5] B. Dupont, “The cyber-resilience of financial institutions: significance and applicability”, Journal of Cybersecurity, vol 5, no. 1, pp. 1-17, 2019.

[6] J. F. Lai and S. H. Heng, “Secure file storage on cloud using hybrid cryptography”, Journal of Informatics and Web Engineering, vol. 1, no. 2, pp. 1–18, 2022.

[7] A. Annarelli, C. Battistella and F. Nonino, “A framework to evaluate the effects of organizational resilience on Service Quality”, Sustainability, vol. 12, no. 3, pp. 958, 2020.

[8] Z. Ma, L. Xiao and J. Yin, “Toward a dynamic model of organizational resilience”, Nankai Business Review International, vol. 9, no. 3, pp. 246-263, 2018.

[9] G. Strupczewski, “Defining cyber risk”, Safety Science, vol 135, pp. 105143, 2021.

[10] Y. I. Starodubtsev, E. V. Vershennik and E. G. Balenko, “Cyberspace: terminology, properties, problems of operation”, International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), 2020, pp. 1-3.

[11] R. Ikwu, “Identifying Data and Information Streams in Cyberspace: A Multi-Dimensional Perspective”, arXiv preprint:1906.03757, 2019.

[12] Z. Collier, I. Linkov and J. Lambert, “Four domains of cybersecurity: a risk-based systems approach to cyber decisions”, Environment Systems and Decisions, vol. 33, no. 4, pp. 469-470, 2013.

[13] Cybersecurity and Infrastructure Security Agency, "Critical Infrastructure Security and Resilience", 2022. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience

[14] G. Lykou, A. Anagnostopoulou and D. Gritzalis, “Smart airport cybersecurity: Threat mitigation and cyber resilience controls”, Sensors, vol. 19, no. 1, pp. 19, 2018.

[15] H. Maziku, S. Shetty and D. Nicol, “Security risk assessment for SDN-enabled Smart Grids”, Computer Communications, vol. 133, pp. 1–11, 2019.

[16] R. Loheswar, “Major data breaches in Malaysia in the past 24 months”, Malay Mail, https://www.malaymail.com/news/malaysia/2022/12/31/major-data-breaches-in-malaysia-in-the-past-24-months/47722, 2022.

[17] Harvard Business Review, “A Comprehensive Approach to Cyber Resilience”, https://hbr.org/2020/06/a-comprehensive-approach-to-cyber-resilience, 2020.

[18] L. A. Mallak, "Toward a theory of organizational resilience", PICMET '99: Portland International Conference on Management of Engineering and Technology. Proceedings, vol. 1, 1999, pp. 223.

[19] K. Stuermer, J. Kandt and M. Rebstock, “Resilience - A New Research Field in Business Information Systems?”, Proceedings of the 43rd Hawaii International Conference on System Sciences, 2010, pp. 1-10.

[20] A. Koziolek and R. H. Reussner, “Toward Resilience Assessment in Business Process Architectures”, IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans, vol. 41, no. 3, pp. 464-477, 2010.

[21] L. Xiao and H. Cao, “Organizational Resilience: The Theoretical Model and Research Implication”, ITM Web Of Conferences, vol. 12, 2017, pp. 04021.

[22] International Organization for Standardization, “ISO 22316:2017 Security and resilience - Organizational resilience - Principles and attributes”, 2017. https://www.iso.org/standard/60815.html.

[23] G. Disterer, "ISO/IEC 27000, 27001 and 27002 for Information Security Management”, Journal of Information Security, vol. 4, no. 2, pp. 92-100, 2013.

[24] G. Culot, G. Nassimbeni, M. Podrecca and M. Sartor, "The ISO/IEC 27001 information security management standard: Literature review and theory-based Research Agenda", The TQM Journal, vol. 33, no. 7, pp. 76–105, 2020.

[25] NIST, "Voluntary Product Standards Program", 2020. https://www.nist.gov/standardsgov/voluntary-product-standards-program.

[26] MITRE, "Cyber Resiliency Design Principles", 2017. www.mitre.org/sites/default/files/2022-09/pr-19-02172-10-cyber-resiliency-constructs-cyber-survivability.pdf.

[27] R. Gyenes, "A Voluntary Cybersecurity Framework Is Unworkable- Government Must Crack the Whip", Pittsburgh Journal of Technology Law and Policy, vol. 14, no. 2, pp. 293-314, 2014. https://doi.org/10.5195/tlp.2014.146

[28] R. F. Babiceanu and R. Seker, "Cyber resilience protection for industrial internet of things: A software-defined networking approach", Computers in Industry, vol. 104, pp. 47–58, 2019.

[29] M. P. Efthymiopoulos, "A Cyber-Security Framework for Development, Defense and Innovation at NATO", Journal of Innovation and Entrepreneurship, vol. 8, no. 1, pp. 1–26, 2019.

[30] P. Nair and R. Ross, "Malaysian agencies investigate alleged breach affecting 13M, Bank Information Security", 2023. https://www.bankinfosecurity.com/malaysian-agencies-investigate-alleged-breach-affecting-13-million-a-20839.

[31] T. Koslowski and P. Longstaff, "Resilience Undefined: A Framework for Interdisciplinary Communication and Application to Real-World Problems", Disaster Management: Enabling Resilience, pp. 3–20, 2015.

[32] J. Scott, "Toward Cyberspace: Managing Cyberattacks through Polycentric Governance.", American University Law, vol. 62, no. 5, pp. 1275 – 1360, 2013.