Article

Not peer-reviewed version

Enhancing Cyber Security in Organisations by Establishing Attributes Towards Achieving Cyber Resilience

Thavaselvi Munusamy , Touraj Khodadadi * , Mazdak Zamani *

Posted Date: 11 August 2023

doi: 10.20944/preprints202308.0901.v1

Keywords: cyber resilience; cyber security; cyber risk; cyberattack; cyber domains

Article

Enhancing Cyber Security in Organisations by Establishing Attributes towards Achieving Cyber Resilience

Thavaselvi Munusamy [1], Touraj Khodaadi [1,*] and Mazdak Zamani [2,*]

[1] School of Information Technology, Malaysia University of Science & Technology, Petaling Jaya, Malaysia; thavaselvi.munusamy@phd.must.edu.my

[2] School of Business and Information Sciences, Felician University, Rutherford, NJ 07070, USA

* Correspondence: touraj@must.edu.my (T.K.); zamanim@felician.edu (M.Z.)

Abstract: The rapid changes in technology on a global scale, combined with the widespread adoption of business operations in cyberspace, have intensified the need for robust protection against escalating risks posed by cyber threats. This research paper aims to identify fundamental cyber resilience management attributes that enable organizations to manage cybersecurity, sustain, and adapt amidst evolving cyber risks and threats. By integrating resilience theory and security theory, this study establishes the attributes for resilience within cyber domains, making a novel contribution to cyber resilience management in organizations. The study introduces a model featuring seven main variables: Rationale, Reliable, Readiness, Resistance, Robust, Rebound, Reflective, and sub-variables across the Physical, Logical, and Social cyber domains, providing a converged framework for achieving cyber resilience. The findings of the study highlight the significance of fundamental attributes for enhancing cyber resilience management in organizations, such as clarity in purpose, vision, and values for security management, an empowered culture, availability of resources, avoidance of single points of failure, development, and coordination of resources to respond to threats and risks, promotion of continual improvement, and the sharing of information and knowledge. In conclusion, this research paper presents a model for managing cybersecurity in organizations by identifying key attributes for achieving cyber resilience.

Keywords: cyber resilience; cyber security; cyber risk; cyberattack; cyber domains

I. INTRODUCTION

The expanding number of organizations relying on technology and embracing internet connectivity amplifies their exposure to cyber risks and renders them susceptible to cybercriminal activities. In addition, the Covid-19 pandemic accelerated the shift towards digital, further intensifying the situation and leading to more vulnerabilities (McKinsey, 2020). According to a cybersecurity solutions provider, Malaysia records an average of 84 million cyberattacks in the fourth quarter of 2022 (Bernama, 2023). Some of the notable cyber-attacks are related to a major e-commerce platform (The Star, 2022), ransomware and breach on budget airlines system, data leakages from the Malaysian National Registration Department and Malaysian Election Regulatory, and civil servant e-payslip system breach (Malay Mail, 2022) and Malaysian Armed Force web portal defacement (The Straits Times, 2022). The problem is not confined solely to Malaysia, as research indicates a substantial increase in cyberattack attempts per organization worldwide, reaching a weekly average of 925 (Zurier, 2022).

To tackle these challenges, the Malaysia National Security Council recommends implementing ISO/IEC 27001:2013 Information Security Management System (ISMS) or equivalent security best practices to mitigate the risk of cybersecurity-related incidents (MKN, 2020). Also, it is common for security experts to utilize risk management models and cybersecurity frameworks to evaluate and develop security strategies for organizations to manage their cyber risk. Some commonly used frameworks are the NIST framework aligning organizational activities with business requirements, risk tolerances, and resources; the ISO 27001 standard providing industry best practices and methodology for cybersecurity implementation and the Cloud Security Alliance's Cloud Control Matrix, offering guidelines for securing and assessing cloud security in organizations. However, scholarly studies contend that the approach toward managing security lacks clarity (Shackelford, 2013), is outdated and inadequate, and falls short of comprehensively addressing an organization's security requirements (Dupont, 2019; Woods & Hollnagel, 2017). They argue that most cybersecurity frameworks focus on security-related regulations and standards, use the traditional outlook of protection and prediction, and are ineffective in a highly uncertain environment (B Dupont, 2019) and volatile cyberspace with unknown risks (World Economic Forum, 2023). This brings forth the inquiry of how to establish cyber resilience within organizations effectively.

Over the past several years, research studies have consistently highlighted the inevitability of cyberattacks, necessitating adopting resilience strategies (Dupont, 2019) and revisiting the approach toward protecting organizations (National Competitiveness Forum, 2021). Also, researchers agree that cyber resilience is still a new concept and are calling for ways to develop resilience to tackle cyber security from management point of view (Dacorogna et al., 2023). Despite the growing research focus on cyber security, there still needs to be more exploration and investigation into cyber resilience. Government and commercial sectors globally have introduced several cyber resilience initiatives in the last few years, either complementing or alternative to existing cyber security practices. However, it often overlaps with cyber risk management and is synonymous with cyber security (Siegel, 2020). Since the concept of resilience itself is broad, it is necessary to comprehensively analyse existing resilience practices in various frameworks across diverse industries and technologies to understand the concept and identify ways to build it into the organization.

From these various perspectives, it is evident that there is a need to explore cyber resilience on its own. This research aims to establish a common reference point specifically related to cyber resilience in management. This research article identifies the gaps in cybersecurity and its relationship with cyber resilience within practical and theoretical domains. It offers valuable insights by clarifying the ambiguities in the cyber resilience taxonomy by exploring interpretations in different contexts and highlighting the distinguishing elements of cyber resilience compared to cybersecurity. The study also helps to understand resilience attributes identified in the different dimensions of cyberspace domain areas. The significant characteristics that help align the industry towards cyber resilience-related attributes are grouped into a basic model, which can be incorporated into building a converged and integrated approach toward effectively dealing with evolving cyber risks. By doing so, organizations can robustly meet the current cybersecurity needs and challenges.

The rest of the article comprises the following sections: Section 2 provides an overview of the concept of resilience and the study's rationale. Section 3 discusses the existing frameworks and the gaps, while Section 4 presents the research framework developed using attributes and its relevance towards achieving resilience, expanding from previous models and incorporating additional insights and enhancements. Section 5 presents the findings, and lastly, Section 6 concludes by discussing the research perspectives and future direction. As far as the researcher is aware, until this study, no prior research has been conducted to examine the characteristics of resilience by incorporating both resilience theory and security theory in the context of cyber domains. Therefore, this study lays the foundation for strengthening organizations' cyber security by establishing a comprehensive "cyber resilience" framework to reduce financial losses, mitigate reputational damage, and effectively address cyber challenges.

II. OVERVIEW OF RESILIENCE AND SECURITY

A. Concept of Resilience

Holling (1973) first introduced “resilience” in the context of ecological systems referring to the ability of the system to absorb changes in the surroundings and remain persistent. Almost three decades later, Richardson (2002) defined resilience as "the process of reintegrating from disruptions

doi:10.20944/preprints202308.0901.v1

in life' (p.307). From the perspective of both researchers, resilience is strongly associated with coping mechanisms in the event of adversity. However, Hartmann et al. (2020) discussed the concept of resilience as more complex than a regular coping process. He emphasized the resilience process involves the interplay of traits covering the cognitive, affective, and behavioural elements that make an entity (individual or organization) able to fare well when facing adversity. Acknowledging the expanding dynamic business environment and cross-national interdependencies, the focus on resilience also heightened. The Council on Competitiveness (2007), a non-profit organization in the United States with aims to drive economic growth, began advocating resilience as a critical component for organizations to address the challenges of globalization and the ever-changing business landscape. Resilience gained significant momentum and importance in addressing the phenomenon of increasing integration of humans and machines (Dupont, 2019), particularly in emerging multidisciplinary fields (Annarelli et al., 2020; Ma et al., 2018). According to the Council of Competitiveness (2007), resilience includes the ability of individuals, organizations, and systems to anticipate, adapt, and recover from disruptive events or challenges. However, according to Vogelgesang et al. (2021), although various studies are emerging, they are disconnected from various subconstructs resulting in a fragmented understanding surrounding the concept of resilience. Considering the setbacks, the concept of resilience provides insights into the state of resilience in cybersecurity. It turns the attention to improving understanding and assisting in identifying the right attributes collectively.

B. What is Cyberspace?

Cyber resilience is closely linked to cyberspace as it focuses on an organization's resilience in the face of adverse cyber events and cyber risks within the digital realm. Cyberspace can be interpreted in varied ways (Fedorov et al., 2021). ISO (2012) defined cyberspace as a multifaceted environment where individuals, software, and services interact through technology devices and interconnected networks on the Internet. Some recent definitions of cyberspace have emphasized that it is a domain characterized by the combined use of electrons and the electromagnetic spectrum for communication (Cybersecurity Intelligence, 2020) and refers to internetworked entities that facilitate information flow (Ikwu, 2019). Cyberspace has multiple layers, with the primary simplified forms being physical (architectural/geographic), logical (software layers), and social layers (Collier et al., 2013; Kott et al., 2018; Steed, 2019) as depicted in Figure 1. This study focuses on the layers of cyberspace where human and computing processes are integrated. The physical domain refers to the computer system comprising hardware, software, and network infrastructure for the system to function (Lee, 2015). The logical domain attributes are the building blocks that support cyberspace infrastructure (Ikwu, 2019) in which the raw data are generated, processed, and analysed. From the aspect of social, the people in the organization and their interaction in cyberspace integration of human social behaviour, such as adherence to policies, regulations, and requirements as a crucial part (Ikwu, 2019; Linkov et al., 2018).

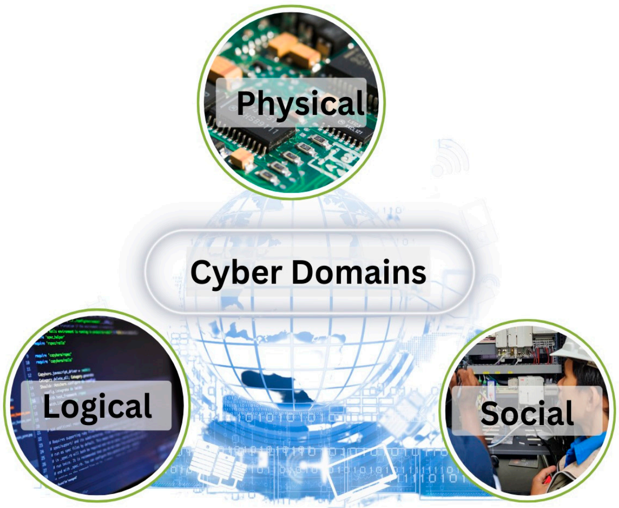


Figure 1. Cyber Domains.

C. Understanding Cyber Resilience

Cyber resilience involves surviving significant challenges that present a substantial and fundamental threat to the operational function of a system, be it individuals, teams, or organizations (Hartmann et al., 2020). Some scholars criticized the existing definitions of cyber resilience for their lack of specificity, general assumption (Annareli et al., 2020), vagueness, ambiguity, and reliance on self-explanatory concepts (Dupont, 2019). One of the existing definitions provided by the Cooperative Cyber Defence Centre of Excellence, as cited by Foale (2018), characterized 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." Likewise, The World Economic Forum (2012) defined it as the capability of systems and organizations to withstand cyber events, measured by the combination of mean time to failure and time to recovery. From scholars' perspective, resilience refers to an organization's continuous ability to achieve its intended outcomes despite adverse cyber events (Chhetri et al., 2018), while some suggest that an adaptive approach and anticipating future challenges (Haque et al., 2019), and the capability to efficiently reduce the magnitude and duration of deviations from targeted system performance levels during a disruptive event (Vugrin & Turgeon, 2013) are crucial for building resilience. Despite slight variations in definitions, we can agree with the concept of cyber resilience as a system's ability to defend against cyberattack incidents, maintain critical functionality, and restore the quality of services to pre-incident levels. Cyber resiliency can be summarized as the process to ensure organization's ability to prepare, defend, recover, adapt, and learn from cyber events.

III. LITERATURE REVIEW

A. Identifying Cyber Resilience Attributes in Existing Studies

With the complexity of securing cyberspace, some researchers have stated that cyber resilience is more important than cyber security (Linkov et al., 2018). Cyber resilience focuses not only on prevention (Babiceabu et al., 2019) and protection but also on reliability and the ability to recover from cyberattacks (Hutschenreuter et al., 2021; Linkov et al., 2019; Perrett et al., 2022; Ross et al., 2019), adaptability; and learning from adversity (Dupont, 2019; Hartmann et al., 2020). Scholars have also identified risk mitigation (Foale, 2018; Lykou et al., 2018), managing resources (Linkov et al.; Maziku, 2019), resilience culture (Harris, 2019), built-in security architecture and intelligence (Harris, 2019 Yogi, 2022) as a crucial aspect in cultivating cyber resilience. 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. Cyber resilience can enable organizations to continually adapt to new information and adversaries to remain relevant in the fight against cyber threats.

Table 1. Existing Research on Cyber Resilience.

Research Title	Cyber Resilience Attributes / Objectives	Author	Year
Cyber Resilience of Systems and Networks	plan, absorb, recover, adapt, robust	Linkov et. al	2018
Resilience Reboot: Rethinking the Cyber Strategy	compulsory intrusion reporting, Bayesian risk assessment, improved risk communications, self-assessment, cyber standards, cyber insurance, risk assessment	E Foale	2018
Smart airport cybersecurity: Threat mitigation and cyber resilience controls	threats, assets infected, cascading effects, mitigation actions, resilience measures	Lykou et. al	2018
Fundamental Concepts of Cyber Resilience: Introduction and Overview	manage complexity, choose topology, add resources, design for reversibility, control propagation, provide buffering, prepare active agents, build agent capabilities, consider adversary, and conduct analysis.	Kott & Linkov	2018
Cyber resilience protection for industrial internet of things: A software-defined networking approach	preventive cybersecurity and equilibrium resilience	Babiceanu & Seker	2019
Security risk assessment for SDN-enabled smart grids.	resource monitoring, threat detector, map the security requirements to mitigate the risk.	Maziku et. al	2019
Exploring the Agile System Development Best Practices Cybersecurity Leaders Need to Establish A Cyber-Resilient System: A Phenomenological Study	a) conducting early involvement; (b) baking in cybersecurity; (c) reducing bureaucracy and organizational impediments; (d) addressing concerns with organizing, training, and equipping; (e) understanding Agile is not a panacea; (f) assessing, understanding, and managing risk; (g) driving acquisition with timely, relevant intelligence; and (h) understanding the need for a culture shift	AB Harris	2019
Developing Cyber Resilient Systems: A Systems Security Engineering Approach	anticipate, withstand, recover, and adapt; prevent / avoid, prepare, continue, constrain, reconstitute / understand, transform / rearchitect., safety, system resilience, survivability, reliability, and security.	Ross et al.	2019
Resilient Machine Learning for Networked Cyber Physical Systems: A Survey for Machine Learning Security to Securing Machine Learning for CPS	machine learning, adversarial attack	Olowononi et al.	2021
Ontology-based cybersecurity and Resilience Framework	identify, protect, detect, respond, recover, sustain, change management, continuous improvement, and centralized management.	Hutschenreuter et al.	2021

The Threat of Cyber-Terrorism & Security in Intelligent Transportation Systems Architecture	three-layer architecture, risk, and vulnerabilities management	Yogi Chakravarthy, 2022	2022
A Cyber Resilience Analysis Case Study of an Industrial Operational Technology Environment	preparedness, prevention, detection, and response.	Perrett & Wilson, 2022	2022

B. Theoretical Framework

To further understand resilience attributes, the study explores frameworks utilized for deploying cyber security or resilience solutions, examining the core attributes specified in the research to establish shared traits and gaps related to resilience. An initial study by Mallack (1998) identified several principles for developing resilience attributes, including perceiving experiences constructively, engaging in positive adaptive behaviours, ensuring adequate external resources, expanding decision-making boundaries, practicing bricolage, developing a tolerance for uncertainty, and building virtual role systems. Earlier scholarly reviews described resilience synonymously with an organization's ability to adapt effectively and respond swiftly to external environmental threats. However, scholars emphasize the ability to navigate high uncertainty and the importance of adapting to new requirements as a critical aspect of resilience (Koslowski, 2017; Koziolek & Reussner, 2011). These reviews predominantly highlighted preparedness and adaptability as the core traits of resilience. Several attributes drawn upon earlier literature studies include bouncing back (Hale et al., 2006), robustness (Tierney, 2003), absorbing and thriving (Berkes, 2007; Seville et al., 2013), and learning and developing (Xiao & Cao, 2017). While the existing resilience frameworks can be categorized as foundational, underlining specific traits, they provide foundational concepts towards resilience.

C. Existing Cyber Security Models and Resilience Frameworks

1) *Organization Resilience Frameworks – ISO22316*

The International Organization for Standardization (ISO) established the ISO 22316 Security and Resilience standard emphasized no universally applicable approach to attaining resilience (ISO, 2017). The standard included nine attributes, as depicted in Table 2, where the activities focus on four primary areas: management, organization, develop guided by fundamental principles for fostering organizational resilience strategically. A key aspect of these activities is empowering individuals at all levels through effective leadership. Additionally, allocating resources to strengthen organizational resilience, promoting continuous improvement, and fostering resilient practices by learning from experiences and encouraging knowledge sharing are highlighted as important components. The ISO standards emphasize the importance of these activities and shed light on resource allocation strategies like diversification, replication, and redundancy. The implementation minimizes the risk of relying solely on a single point of failure. In conclusion, the ISO standards provide valuable guidance for developing resilience within an organization, thereby improving its capacity to withstand and recover from adversarial in a dynamic environment.

Table 2. 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.

doi:10.20944/preprints202308.0901.v1

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.

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

ISO 27001 is a globally recognized standard for information security management systems (ISMS) that helps organizations manage and protect their information assets (Dupont, 2019). The standard was first introduced in 2005 and was revised multiple times to keep up with the changing technology landscape and evolving cyber threats. The recent update was in 2021, known as ISO27001:2022. One of the key differences between ISO 27001:2013 and ISO 27001:2022 is the structure of the standard. ISO 27001:2022 version of the standard includes updated terminology, enhanced guidance on risk management, and a greater emphasis on the importance of leadership and commitment to information security. While ISO 27001:2013 contains 114 controls categorized under 14 control domains, as depicted in Figure 2, the latest version of ISO 27001:2022 maintains similarities to those in the previous standard but reduced to a total of 93 controls categorized into four distinct themes: people, organizational, technological, and physical as shown in Figure 3. Some controls from the earlier versions were merged, and newer controls were introduced mainly to safeguard cloud computing services (Malatji, 2023). Although ISO27001 is a renowned standard for information security, implementing it can be challenging due to the generic guidelines (Culot G. et al., 2021). Numerous researchers have noted that ISO27001 lacks a precise indication of scope (Alshar'e, 2023), an explicitly defined acceptable level of risk. Instead, the organization's management is responsible for determining the type and extent of security (Dupont, 2019). Consequently, inadequate awareness of risks within the organization can lead to a suboptimal implementation of the cybersecurity program based on ISO27001.

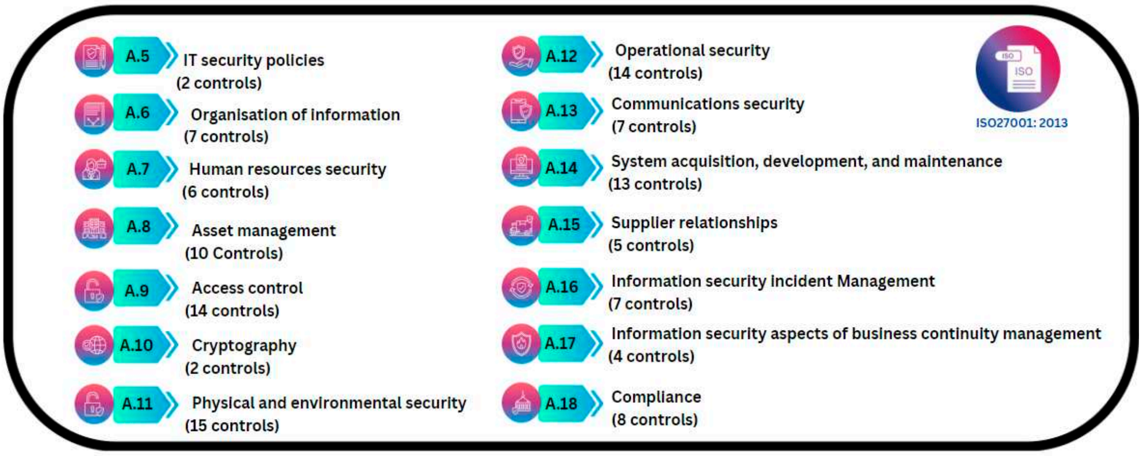


Figure 2. ISO27001:2013 Domains.

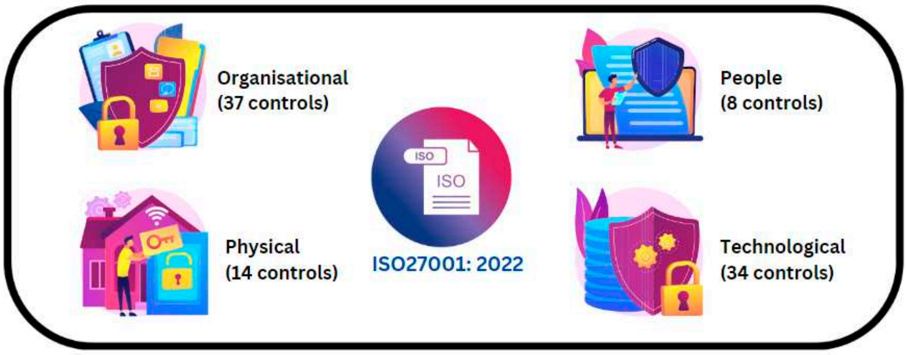
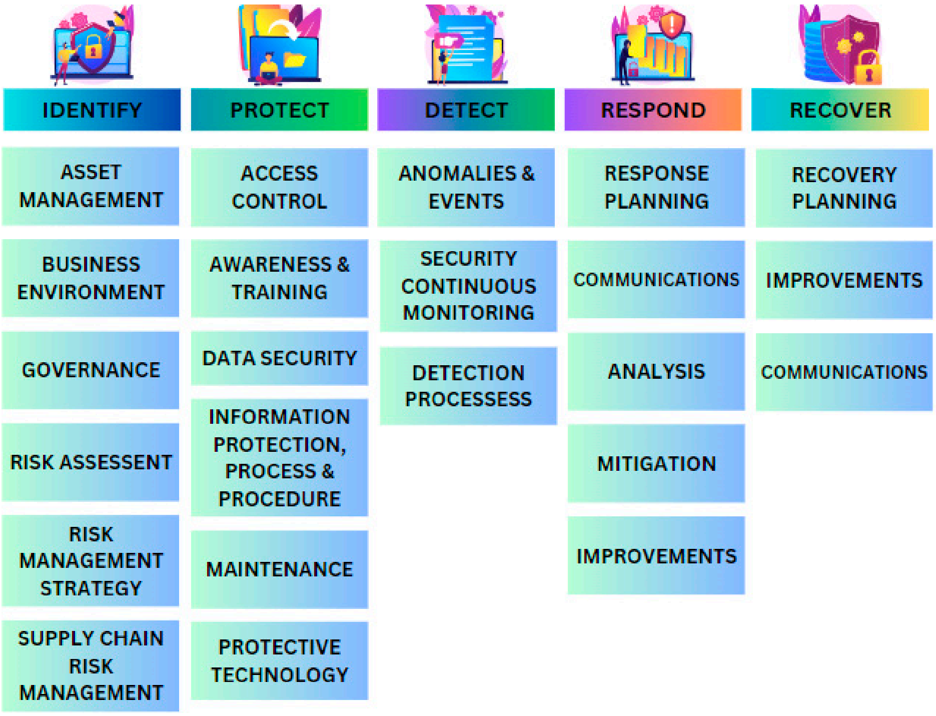


Figure 3. ISO27001: 2022 Domains.

3) NIST

The NIST framework is a widely adopted approach to managing and enhancing cybersecurity within organizations providing high-level standards, guidelines, and practices for managing and improving critical infrastructure cybersecurity. The NIST framework does not enforce or mandate controls, unlike the ISO 27001 Standard (NIST, 2020). It incorporates a risk-based approach, enabling organizations to adopt a risk management methodology akin to the approach taken by ISO 27001. Nevertheless, this method has faced criticism; embracing a voluntary stance towards cybersecurity guidelines might reduce investments in securing cyberspace, mainly when implementation costs are significant or additional resources are required (Dupont, 2019; Gyenes, 2014). It is worth noting that the primary design of the NIST framework focuses on addressing cyber-attacks rather than explicitly aiming to achieve resilience. Additionally, successful implementation of the NIST framework necessitates supporting and aligning relevant stakeholders, particularly decision-makers, in the pursuit of cyber resilience.



IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
ASSET MANAGEMENT	ACCESS CONTROL	ANOMALIES & EVENTS	RESPONSE PLANNING	RECOVERY PLANNING
BUSINESS ENVIRONMENT	AWARENESS & TRAINING	SECURITY CONTINUOUS MONITORING	COMMUNICATIONS	IMPROVEMENTS
GOVERNANCE	DATA SECURITY	DETECTION PROCESSESS	ANALYSIS	COMMUNICATIONS
RISK ASSESSENT	INFORMATION PROTECTION, PROCESS & PROCEDURE		MITIGATION	
RISK MANAGEMENT STRATEGY	MAINTENANCE		IMPROVEMENTS	
SUPPLY CHAIN RISK MANAGEMENT	PROTECTIVE TECHNOLOGY			

Figure 4. NIST Framework.

4) NIAC

The NIAC Resilience Model, by the National Infrastructure Advisory Council of the United States, is specifically designed to address the critical need for resilience in critical infrastructure. The framework's strength lies in its flexibility, allowing organizations to implement resilience constructs (as depicted in Table 3) that align with their specific needs and operational context. However, this broad approach is also open to interpretation, which may pose challenges in its proper execution. While the NIAC Resilience Model shares a common goal with cyber resilience - enhancing an organization's ability to withstand and recover from disruptions - it differs in its approach. The model focuses on identifying sector-specific resilience goals; meanwhile, cyber resilience aims to build a holistic and adaptive cybersecurity framework capable of mitigating and responding to diverse cyber threats across all sectors.

Table 3. NIAC Model attributes and description.

NIAC Resilience Model	
Resilience Construct	*Description*
Robustness	The ability to keep operating by having substitute or redundant systems.
Resourcefulness	Primarily on people, to skilfully 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.

D. Cyber resiliency engineering framework - CREF

MITRE developed the "Cyber Resiliency Engineering Framework," also known as CREF, a decade ago with the intent to evolve as the discipline of cyber resilience matures (MITRE, 2013). The framework was developed comprehensively, mainly focussing on survivability, dependability, fault tolerance, business continuity, and contingency resulting in a large and complex model. Though the CREF Model is comprehensive, it is narrowed towards "defending" against adversaries. It highlights the goals, objectives, practices, costs, and metrics for resilience and to protect organizations against cyber threats using resilience engineering, mission assurance engineering, and cybersecurity concepts. One of the drawbacks of CREF is that it assumes existing conventional cyber security exists and focuses on actions to ensure business continuity in an attack (MITRE, 2013). CREF provides a structure for understanding the interrelated aspects of cyber resiliency rather than defining the attributes. Furthermore, recent studies have indicated that cyber resiliency requires consideration of various aspects of adversaries within cyberspace (Dupont, 2019) and multiple processes (Harmann, 2020) for which the CREF framework lacks sufficient coverage.

Table 4. Cyber Resiliency Engineering Framework Objectives (CREF).

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

E. Initial Findings and Gaps

Multiple studies related to the cyber security concept exist as it was a pioneering subject in the wake of information systems and is used widely in the industry. In contrast with cyber security, cyber resilience is considered in its early stage of development; hence there is a limited exploration of this topic in general. Although the resilience concept has existed for three decades, the existing studies focus on industry-specific needs rather than exploring the traits. Numerous cyber security management frameworks exist, yet a comprehensive literature review reveals a prevailing focus on protection and prevention, with limited attention given to resilience strategies. Scholars have delved into cyber resilience from a process perspective, focusing on the cognitive, affective, and behavioural mechanisms when facing adversity. These mechanisms determine an entity's capacity to achieve a resilient outcome (Hoegl & Hartmann, 2020). From this perspective, current studies lack several aspects that are deemed crucial for cyber resilience, such as considering attributes in establishing direction and purpose (ISO,2017), the process for adaptation (Linkov, 2019), resourcefulness (Koslowski, 2020), the process for dependable systems (Enisa, 2018), and preparation towards threat anticipation (Annarelli et al., 2020). Also, while there are studies on resilience metrics for cyber systems (Linkov et al.,2013), they remained focused on managing disasters and recovery. Consequently, the current cybersecurity approach must be revised to safeguard businesses against evolving threats.

IV. THE RESEARCH FRAMEWORK

A. The Proposed Framework

Cybersecurity continually evolves, with previous studies focusing on prevention and detection mechanisms proven insufficient in effectively addressing the dynamic landscape of cyber threats. Given the widely acknowledged potential of the resilience approach to bridge the gaps in traditional cybersecurity methods, it becomes imperative to explore the specific requirements for implementing a business-oriented resilience strategy to tackle the challenges posed by evolving cybersecurity threats. Nevertheless, resilience in cybersecurity needs clear and widely agreed-upon definitions and characteristics. This lack of consensus hampers the development of a cohesive understanding of the attributes that contribute to cybersecurity resilience. By drawing insights from existing security research, models, and frameworks, the literature review aids in identifying crucial attributes that lays the foundation for a comprehensive conceptual model organizations can use to enhance cyber resilience.

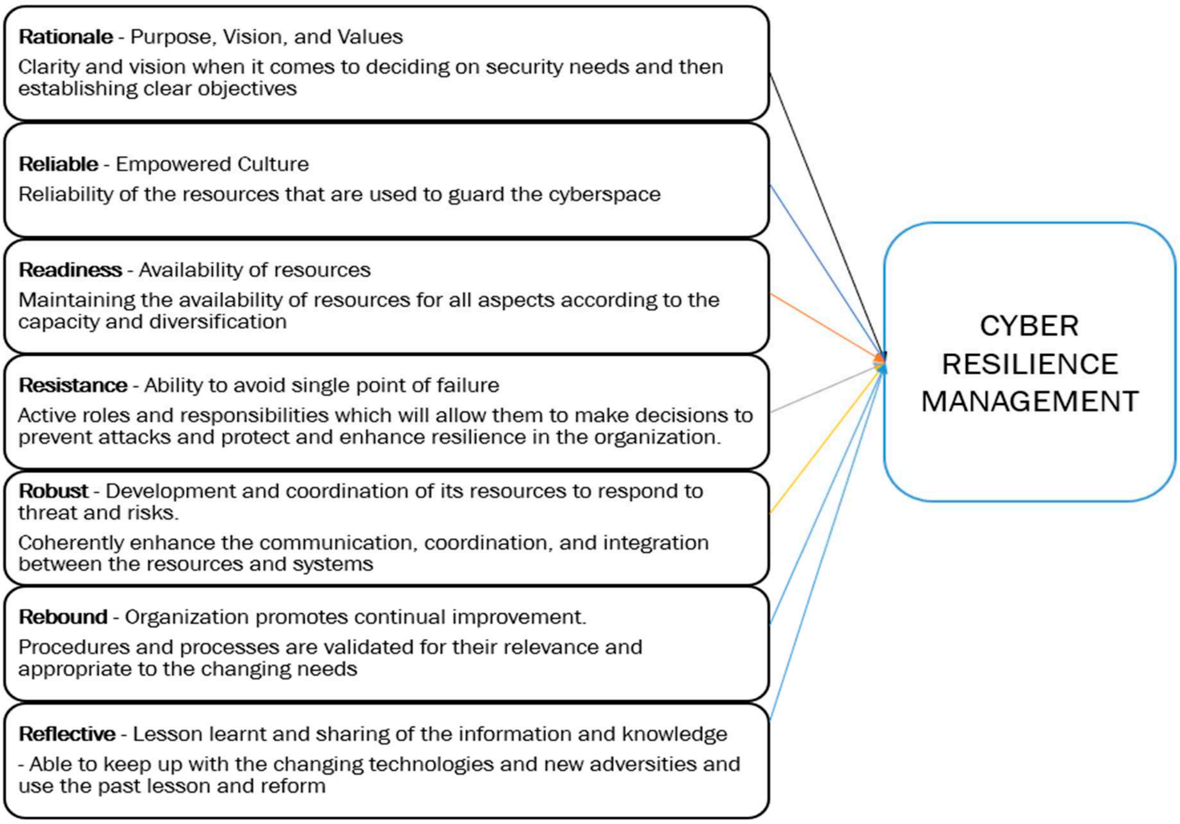
This research examines various common cybersecurity frameworks and models to discern the essential attributes contributing to the establishment of resilience. Subsequently, an integrated model for cyber resiliency is proposed.

The suggested model incorporates key resilience objectives drawn from ISO's Security and Resilience (ISO22316) and CREF's cyber security management, resulting in a comprehensive approach to cyber resilience, as outlined in Table 5. Core resilience variables are identified based on their significance in achieving resilience. CREF is built on concepts related to systems security engineering, security operations and management, and systems engineering for performance and management, primarily centred on addressing cyber threats. Contrarily, ISO22316 places significant emphasis on management's pivotal role in fostering a resilient culture within the organization. As a standard designed explicitly for organizational resilience, ISO22316 complements MITRE's Cyber Resilience Engineering Framework (CREF) and provides an ideal foundation for identifying key factors towards cyber resilience. These selected factors are strategically chosen to bridge the gaps in CREF and lay the groundwork for constructing an enhanced framework for cyber resilience. Furthermore, the key factors are extended to encompass the physical, logical, and social cyber domains, thus offering a comprehensive approach to achieving resilience.

doi:10.20944/preprints202308.0901.v1

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 Restore as much mission / business functions and supporting processes to handle adversity more effectively	Readiness
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 Modify architectures to handle adversity more effectively	Resistance



Rationale - Purpose, Vision, and Values

Clarity and vision when it comes to deciding on security needs and then establishing clear objectives

Reliable - Empowered Culture

Reliability of the resources that are used to guard the cyberspace

Readiness - Availability of resources

Maintaining the availability of resources for all aspects according to the capacity and diversification

Resistance - Ability to avoid single point of failure

Active roles and responsibilities which will allow them to make decisions to prevent attacks and protect and enhance resilience in the organization.

Robust - Development and coordination of its resources to respond to threat and risks.

Coherently enhance the communication, coordination, and integration between the resources and systems

Rebound - Organization promotes continual improvement.

Procedures and processes are validated for their relevance and appropriate to the changing needs

Reflective - Lesson learnt and sharing of the information and knowledge

- Able to keep up with the changing technologies and new adversities and use the past lesson and reform

Figure 5. Proposed Cyber Resilience Management Framework.

B. Research Design & Analysis

This study investigates a phenomenon related to the real-world problem, the rise in cyber risk, and the increasing need for cyber resiliency. Exploratory research is "the preliminary research to clarify the exact nature of the problem to be solved" and provides insight into the phenomenon studied (Sekaran & Bougie, 2016, pp. 81-82). The utilization of the exploratory approach is motivated by the scarcity of research studies on cyber resilience and the complex and evolving nature of the subject being studied.

1) Research Methodology & Sampling

The current study adopts a novel approach by employing observed variables derived from previous research and existing models to create a comprehensive framework that accounts for the complexities of the cyber domain. Questionnaires using the identified variables are subsequently utilized to survey information security or cyber security practitioners. The objective is to collect valuable feedback regarding cyber resilience attributes. The participants selected for this study represent a diverse range of industries and possess varying levels of professional experience, spanning from a minimum of three years to over ten years. The Cronbach Alpha method is employed on the collected data to ensure data reliability. Cybersecurity Malaysia estimates a population of approximately 10,733 cybersecurity knowledge workers (The Star Online, 2020). Given the limitations of resources and the challenges posed by the Covid-19 pandemic during the survey's administration, including restricted face-to-face communication with potential respondents, the research aims to secure a sample size that allows for reliable statistical analysis by Cohen's rule, selecting a minimum sample size with a 7% margin of error and a 95% confidence level, determined based on a table published by Glenn (1992) that corresponds to the specified criteria. For instance, considering a population size of 10,000, the table recommends a minimum sample size of 200.

2) Analysis Methodology

In this study, the research data will be subjected to multivariate data analysis to validate the hypotheses derived from the proposed research model. The statistical software package SPSS will be employed to analyse the collected data, enabling the researcher to confirm the identified cyber resilience attributes. Data cleanup and validation will be conducted before the data analysis using an Excel spreadsheet. SPSS software will be utilized to perform reliability analysis, assessment of normality, and descriptive statistics, which includes Cronbach's Alpha and Exploratory Factor Analysis. AMOS software will be used for Structural Equation Modelling (SEM) to enable the researcher to effectively examine the relationships and validate the proposed research model.

V. THE RESEARCH FINDINGS

3) Preliminary Analysis

The survey was distributed to 300 participants, and a satisfactory response rate of approximately 68% was achieved, with 204 participants providing responses. This response rate meets the required minimum sample size for the study, ensuring a robust dataset for analysis. Regarding the distribution characteristics of the collected data, skewness and kurtosis values are important indicators. In this study, an acceptable skewness range is between -3 and +3, while an appropriate range for kurtosis is between -1.5 and <10. Notably, all the values obtained in this study fall within these acceptable ranges, signifying that the data is suitable and valid for further analysis. Furthermore, the reliability of the measurement scale used in the study was assessed using the Cronbach's alpha test. The obtained Cronbach's alpha value was 0.8 or higher, which falls within the acceptable range for reliability. This suggests that the measurement items demonstrate strong internal consistency and reliability. In addition, suitability for factor analysis (as indicated by the KMO coefficient yielded a value greater than 0.5) and overall significance of the correlation matrix (as indicated by Bartlett's test with test results indicated statistical significance, with a p-value of less than 0.05.), are all within acceptable parameters. Overall, the findings of this study suggest that the survey responses, in terms of sample size, distribution characteristics, and measurement reliability, are all within acceptable parameters. This provides a solid foundation for conducting further analysis and drawing valid conclusions from the data.

4) *Results and Discussion*

Based on the test results, the chi-square to degrees of freedom ratio (χ^2/df) was less than 3, indicating a good model fit. The comparative fit index (CFI), Tucker-Lewis index (TLI), and incremental fit index (IFI) were all greater than 0.9, demonstrating a high degree of model fit. The root mean square error of approximation (RMSEA) was 0.000, indicating an excellent fit. These findings confirm the convergent validity of all the variable constructs. The research model examined the relationship between independent variables and cyber resilience management.

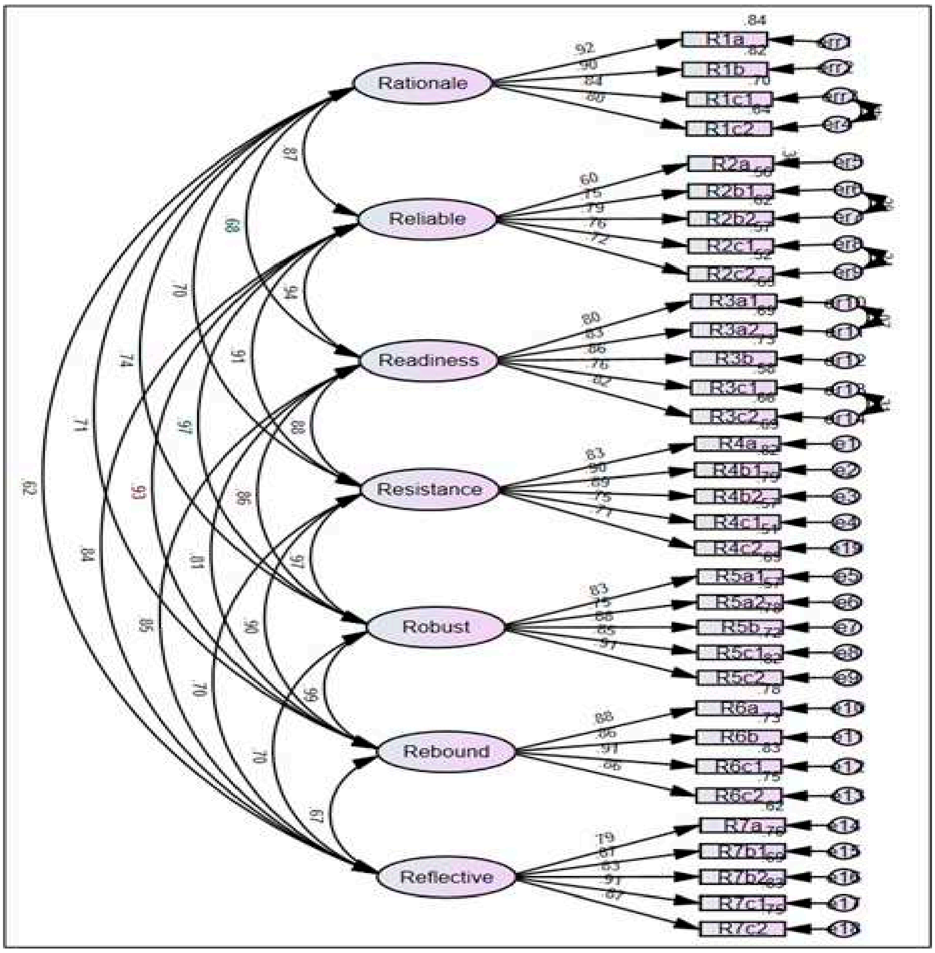


Figure 6. Factor Model Analysis Result.

The results revealed a significant positive correlation ($p < 0.001$) between all the independent variables and cyber resilience management. The factor loadings, ranging from $\beta = 0.9$ to 0.8, indicate a substantial and statistically significant positive relationship with cyber resilience management. Notably, the attribute "Rebound" exhibited the highest factor loading, ranging from $\beta = 0.91$ to 0.85, indicating that promoting continual improvement significantly contributes to cyber resilience. Other attributes, such as Rationale, Readiness, Resistance, Robustness, and Reflective, also demonstrated significant positive relationships with cyber resilience, as evidenced by large factor loadings ranging from $\beta = 0.9$ to 0.8. The attribute "Reliable" and having an organization with an empowered culture showed a slightly lower but still significant factor loading of $\beta = 0.72$. The findings of this study highlight the importance of a combination of factors, including Rationale, Resistance, Robustness, Readiness, Rebound, Reflection, and Reliable, in enhancing cyber resilience. These factors collectively contribute to the improvement of cyber resilience in organizations. In conclusion, the results support the hypothesized positive relationships between the independent variables and cyber resilience management. The attributes identified in this study provide valuable insights into the essential factors necessary for enhancing cyber resilience.

The results findings are discussed in order of strongest importance:

5) Rebound

The concept of "rebound" emphasizes the continuous improvement of cybersecurity activities within an organization, enabling them to bounce back from adversities and enhance their resilience effectively. The study's findings highlight the significance of leadership's regular review of cyber security solutions, systems, infrastructure, and resources as the most substantial factor in achieving cyber resilience. Given the rapidly evolving technological and threat landscape, organizations must adopt a proactive approach to security to achieve resilience (MITRE, 2018). It involves the capability to modify and redeploy resources, accommodate changing security needs, and adapt operational structures. These adjustments include revalidating processes and procedures and aligning with ISO's resilience requirement of proactive awareness and process revalidation (ISO, 2017).

6) Rationale

The study findings demonstrate the significance of rationale in cyber resilience, as indicated by favourable ratings for all the related factors. This attribute reflects the organization's clarity of vision and purpose in addressing its security needs from factors impacting its environment and infrastructure (physical factor) followed by the data and information (logical) it is dealing with and people (social) at the decision-making level's ability to articulate their cyber security strategy to provide a clear direction to all level. The research reveals that a well-defined rationale is pivotal in fostering effective communication and collaboration among various stakeholders, including senior management, IT personnel, and third parties. This alignment of efforts towards established objectives significantly enhances cyber resilience within an organization. Moreover, organizations with a clear vision and purpose, as outlined in ISO (ISO, 2017), can establish a solid foundation for making effective and strategic decisions, a viewpoint supported by MITRE (2013) concerning resilience activities.

7) Reflective

MITRE (2017) mentioned understanding the need to evolve, transform, and modify current architectures to improve cyber resilience as a critical aspect. The reflective factor in this study achieves that by emphasizing implementing lessons learned and sharing of knowledge through an established system and shared as part of organizational learning. Several researchers argue that the ability to reflect and learn is one of the crucial factors in organizations building resilience (Haque et al., 2019; Chhetri et al., 2018). The result shows a positive inclination towards establishing a process for knowledge creation and communication at all levels, particularly from the social aspect, where using the knowledge and lesson to reform an organization to keep up with the evolving threats has one of the highest ratings. Promoting better practices helps the organization identify potential vulnerabilities and develop strategies to prevent future attacks by employing a proactive approach. Conclusively, the attribute "reflective" can help reduce the risk of cyber incidents and minimize the impact of any attacks, therefore navigating the organization toward being more resilient.

8) Robust

The robust attribute focus on an organization's commitment to protection, performance, and adaptability, underscoring the importance of effective communication, coordination, and regular assessments to foster a coherent and resilient cybersecurity approach. The study identifies the robust attribute as significant aspect related to cyber resilience, particularly concerning the social factor, which involves regularly assessing the organization's management discipline in terms of commitment to protection, risk and threat management, and adaptability to changes in the cyber landscape. Such assessments enable organizations to pinpoint gaps and areas for improvement and implement appropriate measures to address them. Robustness also encompasses understanding critical resources, such as information systems, data, and cyber security resources, and ensuring the availability of adequate personnel, technology, and processes for cyber-related activities. Moreover, building flexibility into the organization's resources facilitates adaptation to change, enhances responsiveness to threats and risks, and enables swift recovery from cyber incidents, in line with MITRE's insights (2018). Effective communication, coordination, and integration between systems and resources, as emphasized by ISO (2017), play a vital role in maintaining organization services at an optimal level during cyber incidents.

9) Resistance

The study's resistance attribute underscores a preventive approach from social, physical, and logical perspectives. The results indicate that physical and logical factors hold slightly greater importance compared to the social aspect, highlighting the significance of securing data and information through techniques like encryption, access controls, and data masking, as well as implementing well-defined access control measures, such as segregation of access, to restrict unauthorized personnel. The physical aspect of resistance emphasizes resource allocation, capacity planning, diversification, replication, and redundancy techniques to enhance an organization's ability to withstand and recover from cyber-attacks with minimal impact, contributing to cyber resilience. This finding aligns with prior research emphasizing redundancy's importance in achieving resistance (Khan et al., 2015).

10) Readiness

The attributes of readiness in the context of cyber resilience highlight the importance of a proactive approach to cybersecurity, including investment in employee training and development, proactive system design and maintenance, risk assessment and scenario planning, monitoring of the external environment, leadership adaptability and collaboration, and valuing diversity in the workforce. The readiness attribute is essential as it allows the organization to anticipate possible threats (MITRE, 2018) and combat adverse situations (Kott & Linkov, 2018). In this study, the readiness aspect highlights the importance of monitoring and evaluating the organization's information context, including interdependencies, political and regulatory environment, and competitor activities under changing circumstances. It requires organizations to understand the external environment and its impact on cybersecurity deeply. Other aspects include the importance of maintaining a set of realistic courses of action that address predicted or anticipated adversity and selecting and developing employees with diverse skills, knowledge, and behaviour that can contribute to the organization's ability to respond and adapt to change.

11) Reliable

The findings reveal the importance of collaboration with stakeholders, including interested parties, suppliers, and vendors, to enhance cyber security, regarded as an essential aspect supporting the previous ISO's security resilience objectives (ISO, 2017). Other relevant factors include the organization understanding the internal and external environment and catering to the need based on the relevance of the availability and effectiveness of resources; while empowering all levels of the organization to make decisions that protect and enhance the resilience of the organization. Among all the factors, prioritizing, monitoring, and evaluating the interdependencies of data and information shows a slightly lower rating but with significant importance, which still warrants inclusion towards the reliability attribute. It helps to comprehensively understand the interdependencies of systems resources and information to identify potential vulnerabilities and develop strategies to mitigate them, therefore approaching cyber resilience holistically.

VI. CONCLUSION

In conclusion, organizations seeking to enhance cyber resilience should implement several key practices. Firstly, promote continual improvement by regularly evaluating and improving its cybersecurity measures. Secondly, an organization must clearly understand its environment, purpose, vision, and values, align its cybersecurity strategy with its overall goals, and provide clear directives. Also, encouraging the sharing of knowledge and lessons learned within the organization will enhance its cyber resilience by having an established process regarding its knowledge creation, use, and communication. Furthermore, to avoid having a single point of failure, they need to consider the development and coordination of resources to respond to threats and risks effectively, the availability of resources, adequate personnel and skills, and upskilling to function in a new or updated environment by validation and periodic assessments, and finally promote an empowerment culture to enable effective decision-making at all organizational levels during uncertainty and disruption by designation of roles and responsibilities. In a nutshell, this study enhances the understanding of cyber resilience by identifying pertinent traits through exploring various methodologies and practices while addressing the gaps between cybersecurity and cyber resilience in practical and academic contexts. Also, the study helps to understand resilience attributes identified in the established framework on the different dimensions of cyberspace domain areas adding scientific evidence to the theoretical basis of the cyber resilience model.

The result of this study can be used to improve cyber resilience implementation for organizations as it approaches resilience by considering all the cyber-domain aspects in which the organization operates, providing comprehensive coverage of all the possible factors that may lead to cyber risk exploitation. The study highlights the importance of the physical domain, where the infrastructure and all the related components are considered when strategizing for cyber security, then moves to the logical aspects, where it emphasizes that the information stored is not limited to business purposes but extends to cover information that is required to ensure the infrastructure and systems (physical components) can function and continue to work, and finally, the social factor on the awareness and skills of the personnel running the system to ensure they are equipped with suitable skills and knowledge. In a nutshell, integrating all the crucial elements paves the way for an organization to achieve resilience.

References

Annarelli, A., Battistella, C., &amp; Nonino, F. (2020). A framework to evaluate the effects of organizational resilience on Service Quality. Sustainability, 12(3), 958.

Babiceanu, R. F., & Seker, R. (2019). Cyber resilience protection for industrial internet of things: A software-defined networking approach. Computers in Industry, 104, 47–58. https://doi.org/10.1016/j.compind.2018.10.004

Chartered Institute of IT, (Bcs,2020). Retrieved 28 March 2020, from https://www.bcs.org/content-hub/why-iso-27001-is-not-enough/

Collier, Z., Linkov, I. and Lambert, J., 2013. Four domains of cybersecurity: a risk-based systems approach to cyber decisions. Environment Systems and Decisions, 33(4), pp.469-470.

Culot, G. et al. (2021) 'The ISO/IEC 27001 information security management standard: Literature review and theory-based Research Agenda', The TQM Journal, 33(7), pp. 76–105. doi:10.1108/tqm-09-2020-0202.

Cyber Resiliency Design Principles. (2017). [Ebook]. MITRE

Cybersecurity and Infrastructure Security Agency. (n.d.). Critical Infrastructure Security and Resilience. Retrieved Feb 12, 2022, from https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. Journal of Cybersecurity, 5(1).

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (2018). doi: 10.6028/nist.cswp.04162018

G. Disterer, "ISO/IEC 27000, 27001 and 27002 for Information Security Management," Journal of Information Security, Vol. 4 No. 2, 2013, pp. 92-100. doi: 10.4236/jis.2013.42011.

Gyenes, R. (2014). A Voluntary Cybersecurity Framework Is Unworkable- Government Must Crack the Whip. Pittsburgh Journal Of Technology Law And Policy, 14(2), 293-314. doi: 10.5195/tlp.2014.146

Harvard Business Review. (2020). A Comprehensive Approach to Cyber Resilience. Harvard Business Review. Retrieved from https://hbr.org/2020/06/a-comprehensive-approach-to-cyber-resilience

Hoegl, M. and Hartmann, S. (2020) 'Bouncing back, if not beyond: Challenges for research on resilience', Asian Business &amp; Management, 20(4), pp. 456–464. doi:10.1057/s41291-020-00133-z. https://doi.org/10.3390/su12030958

Ikwu, R. (2019). Identifying Data And Information Streams In Cyberspace: A Multi-Dimensional Perspective. ArXiv, abs/1906.03757.

International Organization for Standardization. (2017). ISO 22316:2017 Security and resilience - Organizational resilience - Principles and attributes. Retrieved from https://www.iso.org/standard/60815.html

Khan, Y.I., Al-shaer, E. and Rauf, U. (2015) "Cyber resilience-by-construction," Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense [Preprint]. Available at: https://doi.org/10.1145/2809826.2809836.

Koziolek, A., Koziolek, H., & Reussner, R. H. (2011). Toward Resilience Assessment in Business Process Architectures. IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans, 41(3), 464-477. https://doi.org/10.1109/TSMCA.2010.2087310

L. A. Mallak, "Toward a theory of organizational resilience," PICMET '99: Portland International Conference on Management of Engineering and Technology. Proceedings Vol-1: Book of Summaries (IEEE Cat. No.99CH36310), Portland, OR, USA, 1999, pp. 223 vol.1-, doi: 10.1109/PICMET.1999.808142.

Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2018). Smart airport cybersecurity: Threat mitigation and cyber resilience controls. Sensors, 19(1), 19. https://doi.org/10.3390/s19010019

Ma, Z., Xiao, L., & Yin, J. (2018). Toward a dynamic model of organizational resilience. Nankai Business Review International, 9(3), 246-263. doi: 10.1108/nbri-07-2017-0041

Malatji, M. (2023). Management of enterprise cyber security: A review of ISO/IEC 27001:2022. 2023 International Conference On Cyber Management And Engineering (CyMaEn), 117-122. https://doi.org/10.1109/CyMaEn57228.2023.10051114.

Maziku, H., Shetty, S. and Nicol, D.M. (2019) "Security risk assessment for SDN-enabled Smart Grids," Computer Communications, 133, pp. 1–11. Available at: https://doi.org/10.1016/j.comcom.2018.10.007.

McKinsey & Company. (n.d.). Cybersecurity in a digital era. McKinsey & Company. Retrieved from https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity-in-a-digital-era

NIST, Voluntary Product Standards Program. (2020). Retrieved 23 March 2020, from https://www.nist.gov/standardsgov/voluntary-product-standards-program

Stuermer, K., Kandt, J., & Rebstock, M. (2010). Resilience - A New Research Field in Business Information Systems? Proceedings of the 43rd Hawaii International Conference on System Sciences, 1-10. https://doi.org/10.1109/HICSS.2010.366

Techopedia. (n.d.). Cyberspace. Techopedia. Retrieved from https://www.techopedia.com/definition/2493/cyberspace

The Difference Between Cyberspace & The Internet. (2020). Retrieved 4 May 2020, from https://www.cybersecurityintelligence.com/blog/the-difference-between-cyberspace-and-the-internet-2412.html

The Star Online (2019) Universiti Malaya E-Pay Portal is down after being defaced, The Star. Available at: https://www.thestar.com.my/tech/tech-news/2019/10/18/universiti-malaya-e-pay-portal-is-down-after-being-defaced (Accessed: April 29, 2023).

The Star Online, (2019) Websites hacked after Flag Blunder, The Star. Available at: https://www.thestar.com.my/news/nation/2017/08/22/websites-hacked-after-flag-blunder/ (Accessed: April 29, 2023).

The Star Online: In Need of Cybersecurity Experts. (2020, March 22). The Star Online. https://www.thestar.com.my/news/focus/2020/03/22/in-need-of-cybersecurity-experts

The U.S. Army Concept Capability Plan for Cyberspace Operations 2016-2028. (2020). Retrieved May 4, 2020, from https://www.army.mil/article/37870/the_u_s_army_concept_capability_plan_for_cyberspace_operations_2016_2028.

U.S. Army Concept Capability Plan for Cyberspace Operations 2016-2028. (2020). Retrieved 4 May 2020, from https://www.army.mil/article/37870/the_u_s_army_concept_capability_plan_for_cyberspace_operations_2016_2028

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97-102. doi: 10.1016/j.cose.2013.04.004

World Economic Forum. (2021). The Global Risks Report 2021. Retrieved from https://www.weforum.org/reports/the-global-risks-report-2021

Xiao, L., & Cao, H. (2017). Organizational Resilience: The Theoretical Model and Research Implication. ITM Web Of Conferences, 12, 04021. doi: 10.1051/itmconf/20171204021

Yogi, M.K. and Chakravarthy, A.S. (2022) 'Application of temporal logic for construction of threat models for intelligent Cyber-Physical Systems', Intelligent Cyber-Physical Systems Security for Industry 4.0, pp. 159–176. doi:10.1201/9781003241348-9.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.