Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

The Impact of Cybersecurity Strategy on Information System Effectiveness: Conceptual Paper

Oraib Al Hyasat[1], Mohammad Falahat[2]

[1]Ph.D. Student in Management, Asia Pacific University of Technology and Innovation (APU), Jalan Teknologi 5, Taman Teknologi Malaysia, 57000 Kuala Lumpur, Wilayah Persekutua Kuala Lumpur, Malaysia, Oraibhyasat@gmail.com
[2]Professor of International Entrepreneurship and Business Management School of Marketing and Management, Asia Pacific University of Technology and Innovation (APU), Jalan Teknologi 5, Taman Teknologi Malaysia, 57000 Kuala Lumpur, Wilayah Persekutuan Kuala Lumpur, Malaysia.

Cyber security has become a critical issue for organizations, especially in public and private sectors where sensitive information is stored and processed. This study aims to examine the impact of cyber security strategy on information systems effectiveness, through a comprehensive literature review. The primary outcome reveals a positive association between effective cybersecurity practices and the success of information systems, highlighting cybersecurity's management vital role in controlling and protecting information within organizations in the private and public sectors. Additionally, the research emphasizes the importance of using new tools and mechanisms to search the sources and causes of cyber threats and attacks and to abandon traditional mechanisms to identify them, perhaps those related to information systems and methods to manage and protect information systems and information within organizations. Key recommendations include that developing a strategy for cybersecurity is crucial for ensuring the resilience of an organization against cyber risks, and essential to protecting institutions' systems and users' data from theft and exposure to risks. This investigation enriches the academic dialogue on cyber security's strategic value and provides actionable insights for entities seeking to improve their systems and maintain the privacy of their data and information through reinforcement cybersecurity measures.

Keywords: Cyber Security, Cybersecurity Strategy, Cybersecurity Risk Management, Information System Effectiveness, Cybersecurity Success.

1. Introduction

The rapid environmental changes and developments have led business organizations to rely on modern technology using applications, technologies, and modern information networks [i] [ii]. as well as relying on cloud computing [iii], which helped organizations store a huge amount of

their data on the cloud within the digital space or cyberspace to develop their performance and make them more efficient and effective. And then stay and carry on.

The increasing use of technologies such as social media, the Internet of Things, mobility, and cloud computing has led to an expansion of sources of potential cyber risks. this leads to the emergence and continuation of cybersecurity risks in any place or location where such data is located [iv]. Here organizations, companies, and individuals face different types of cyber security risks. Organizations that face challenges and risks in the work environment, especially those related to information and information technology, must follow specific frameworks to implement an approach that is aware of those risks and threats, rather than focusing on identifying areas that must be addressed to avoid those unsafe risks and threats that can cause losses. huge investments.

Using a framework that covers the fully functional areas of business and information technology responsibility helps organizations avoid many of the risks and threats faced by their information systems projects. Cybersecurity concentrates on protecting information systems from cyber threats [v].

The research significant:

The significance of the current research is highlighted by researching and learning more about cyber security and information system effectiveness to contribute to bridging the knowledge gap for these variables by clarifying their concepts and the sub-dimensions of each approach and providing results that can be used in future studies. This is reflected in expanding the range of visions towards more future studies and research in analyzing the topics of the current study and linking them with other variables that have a reflection on the effectiveness and efficiency of information systems of organizations in general. The significance of the current research stems from the increasing prevalence of cyber threats, understanding how a well-defined cybersecurity strategy framework affects information systems success is crucial for ensuring the resilience of organizations against potential cyber-attacks.

The research problem:

Despite some research developments in the subject of cybersecurity, the volume of academic research work focused on cybersecurity is still relatively small, which makes the scope of cybersecurity unclear and many gaps must be filled. Theoretically and practically.

Hence, the features of the current problem in its two dimensions can be summarized as follows:

- The theoretical dimension of the problem

The literature and previous studies did not provide a comprehensive framework for formulating a strategy for cybersecurity in organizations that helps them to reduce cyber risks, and threats and manage and safeguard their information systems and information in them, as well as help understand how the practices of cybersecurity can help organizations manage to direct and control their information technology departments and develop strategic plans for them in line with their overall strategy.

- Practical dimension of the problem:

The need to direct the attention of decision-makers in their positions in the organizations to the need to search for sources and causes of cybersecurity risks and to abandon traditional mechanisms in identifying and clarifying cybersecurity risks, their nature, and ways to confront them by developing a clear strategy for cybersecurity, as they must realize that the foundations of survival Modern continuity are based on new tools and mechanisms, perhaps the most important of which are those related to information systems and methods of protecting them and protecting information in them.

The issue of how the organizations develop a cybersecurity strategy to confront cyber risks and how to reduce them and their impact on the effectiveness of their information systems is still under discussion and is not clear to the administrations of the organizations, and those departments do not have an understanding and awareness of the fact that the cybersecurity strategy is related to methodological alignment planned information systems strategy with the general and main objectives of the organization.

The research objectives:

The primary objective of this research is to explore the impact of cyber security on information system effectiveness. Through a comprehensive literature review, this study aims to anatomy the fundamental concepts and consequences of cyber security and its influence on information system effectiveness. Furthermore, it seeks to inflame interest among researchers in the momentous variables under investigation, emphasizing the significance of leveraging the findings and recommendations derived from this study. This research endeavors not only to chart the topography between cyber security and information system effectiveness but also to serve as a stimulus for future investigations, promoting a deeper exploration into how cyber security strategies can be enhanced to increase the effectiveness of information systems.

2. Methodology:

Literature Review:

Cyber Security.

ISO/IEC 27032:2012 defines cybersecurity as “Preservation of the confidentiality, integrity, and availability of information within complex environments, which arise from the interaction of individuals, software, and services on the internet through technological devices and connected networks” [iii] [vi]

Cybersecurity is defined as a set of informational, organizational, and technical measures designed to protect information systems, communications, and networks from activities or events that could cause damage, destruction, alteration, or disruption of their operations [vii].

Ensuring the continuity of cybersecurity necessitates several requirements, including confidentiality, integrity, and availability. These requirements guarantee that only authorized users have access to the information or resources used or stored within the organization's information systems [vii]. This is because the data is integral to all operations within an organization, preserving it necessitates adherence to specific procedures and rules. These

include determining access permissions to ensure only authorized individuals can access the data, thereby maintaining confidentiality. This approach ensures the credibility, reliability, and availability of the data. Data loss can lead to organizational failure [viii].

Cybersecurity strategy.

Cybersecurity strategy is defined as "Investigating security threats to an organization involves identifying security weaknesses, locating vulnerabilities and breach points, and making informed decisions about managing the cyber risk landscape" [ii]. It has also been defined as "the measure, techniques, and policies involved in cybersecurity risk management" [ix].

The National Institute of Standards and Technology (NIST) defines cyber risk management as "a framework for enhancing the security of cyberinfrastructure" [x]. It was explained that "The Cyber Risk Management (CRM) framework encompasses three interconnected processes: cyber risk assessment, identified risk analysis, and regular evaluation of cyber risks" [i] [ii].

Cybersecurity risk management (CRM) is the "The process involves detecting an organization's security threats, identifying vulnerabilities to pinpoint potential attack vectors, and making decisions on how to address the cybersecurity risk" [ii]. Where defined as "the process of managing cybersecurity risk" [ix].

Implementing comprehensive organizational risk management has become a standard practice, yielding both tangible and intangible benefits. These include enhanced performance across all management operations, bolstered organizational reputation, increased competitiveness, and mitigation of damages resulting from threats and risks through systematic risk identification, assessment, analysis, response, and control [ii].

The framework for the cyber security management model is crucial and indispensable for organizations, aiding in the protection of cyber security and the reduction of cyber risks and threats within their operations [ii] [iii] [xi].

Cyber Risk Assessment.

Cyber risk assessment is a foundational and crucial initial process within the broader domain of cybersecurity and cyber risk management [xii] [xiii]. It is considered as an integral component of the organization's enterprise risk management process [xiv]. It entails systematically assessing the organization's information technology (IT) infrastructure, identifying potential cyber threats, analyzing system vulnerabilities susceptible to these threats, evaluating the potential impact of these threats if realized, and assessing the likelihood of their occurrence [xiii].

[xii] explained risk assessment involves identifying assets and systems that require protection and evaluating potential threats, vulnerabilities, and risks to the organization's core services and operations. Various methodologies and techniques exist for conducting risk assessments. One approach integrates results from threat assessments, vulnerability assessments, and impact assessments to quantify the risk level for each asset-threat pair.

Cyber Risk Analysis.

[xv] identified Cyber risk analysis involves conducting a thorough examination of potential threats to an organization's information systems, devices, and data security, aiming to prevent

cyber-attacks. It includes a detailed exploration and understanding of identified risks to discern their nature, potential consequences, and the most effective strategies for managing or mitigating them [xvi].

[xvii] stated that "Cyber risk analysis involves assessing the likelihood of threat events and identifying vulnerable conditions that could adversely affect system assets. The analysis evaluates the impact of these events and calculates risk exposure using methodologies outlined in the organization's risk strategy. Results are documented in rating column reports under Likelihood, Impact, and Exposure".

Respond to Cyber Risk.

[xvxv] highlighted the essential for effectively responding to cyber risks, emphasizing proactive planning, prompt detection, and efficient containment strategies. They underscored the importance of incident response plans that include isolating affected systems, analyzing attacks, mitigating damage, and restoring systems.

[xviii] addressed the need to address cyber risks by implementing measures such as deploying security protocols, updating software, training employees in cybersecurity best practices, and regularly assessing and adapting security measures to evolving threats. The objective is to minimize the impact of cyber threats and uphold the integrity, confidentiality, and availability of critical data and systems.

Recovery Cyber Risk.

According to [xix] "The goal of recovery is to restore systems to their normal state after a security incident. This involves taking specific actions once the threat has been eliminated". Based on [xx] the recovery phase in cyber risk management encompasses post-incident activities such as data restoration, system reconfiguration, and service reinstatement. It also involves implementing enhanced security measures to mitigate the risk of similar incidents in the future.

Activity Control.

Previous studies showed the concept of activity control in cybersecurity and its importance in mitigating cyber risks within the organization. [xxi] [xxii] demonstrated that "Activity control involves managing, monitoring, and organizing user activities within the information system or network to ensure security, integrity, and compliance. This includes implementing measures to restrict and monitor user actions and enforcing policies to prevent malicious activities."

According to [xxiii]activity control "This involves implementing access controls, authentication mechanisms, and authorization protocols to manage and oversee user interactions with digital resources. It includes granting appropriate permissions to users and defining their roles to monitor and review activities".

Information System Effectiveness.

IS a set of components to collect, manipulate, store, and disseminate information, aiming to achieve organizational goals, this is what Zemmouchi-Ghomari defined in the book "Current Issues in Information Systems – A Global Perspective" by its author, [xxiv]. "The significance of information security for organizations lies in their focus on safeguarding confidentiality,

privacy, and integrity of their most critical asset: data and information" [xxv].

[xxvi]outlined three dimensions of information system effectiveness, based on the Delone and Mclean model these dimensions are as follows:

System Quality.

System quality is "Desirable attributes of an information system include ease of use, system flexibility, reliability, ease of learning, intuitiveness, sophistication, and response time" [xxvii]. According to [xxviii] "System quality a metric used to assess the quality of an IT system".

Information Quality.

According to [xxix], information quality is a critical factor in the success of an information system model, defined as the suitability of information characteristics for information users. Meanwhile, as explained in [xxx], information quality refers to the degree to which data or information is accurate, reliable, timely, relevant, consistent, and usable for its intended purposes. This ensures that information is trustworthy, comprehensible, and valuable for decision-making and other organizational functions.

Service Quality.

High service quality has emerged as a distinctive strategy in recent times. To meet the diverse needs of stakeholders, many organizations have developed websites that offer high-quality information and services. Consequently, there has been a growing emphasis among service providers on improving service quality as a pivotal strategy for enhancing stakeholder satisfaction [xxxi].

Other studies, such as [xxxii], view service quality through the lens of customer perceptions regarding the quality of products or services and their alignment with expectations. According to another study [xxxiii], there is consensus that service quality is determined by comparing expectations with perceptions of performance.

Supporting Theories of Study:

This study used some theories and conceptual frameworks such as Resource-Based View (RBV), and NIST Cybersecurity Framework that helped link cybersecurity strategy and information system effectiveness and clarify the relationship between them.

- Resource-Based View (RBV)

The Resource-Based View (RBV) was originally formulated by [xxxiv] in his influential 1991 paper titled "Firm Resources and Sustained Competitive Advantage." He introduced the VRIN criteria, asserting that resources must be valuable, rare, inimitable, and non-substitutable to provide a sustained competitive advantage. [xxxv] later expanded on evaluating firms based on their resource profiles. The RBV theory posits that a firm's resources and capabilities, meeting the VRIN criteria, are pivotal in achieving competitive advantage. These resources form the foundation of the firm's strategy and performance [xxxiv].

Cybersecurity as a Strategic Resource

- Valuable: Effective cybersecurity measures protect the organization's information assets, ensure compliance with regulations, and maintain the trust of the organization.

- Rare: Advanced cybersecurity capabilities, such as cutting-edge technologies and highly skilled cybersecurity professionals, are not easily available to all organizations.
- Inimitable: The specific combination of cybersecurity policies, practices, and technologies tailored to an organization's needs makes it difficult for competitors to replicate.
- Non-substitutable: No other resource can fully replace the need for robust cybersecurity measures in protecting information systems.

Information System Effectiveness as a Strategic Resource

- Valuable: Effective information systems enhance operational efficiency, support the organization's processes, and improve decision-making.
- Rare: Information systems that are perfectly aligned with the strategic goals of organizations and that operate seamlessly are unique.
- Inimitable: The integration of information systems with organizations -specific workflows and data makes them hard to replicate.
- Non-substitutable: Effective information systems are essential for the digital functioning of organizations, and there are no perfect substitutes for their role.

- NIST Cybersecurity Framework

The NIST Cybersecurity Framework (NIST) comprises guidelines and best practices aimed at assisting organizations in managing and mitigating cybersecurity risks. Developed by the National Institute of Standards and Technology (NIST), an agency within the U.S. Department of Commerce, the framework was initially released in February 2014. It was created in response to an executive order from former President Barack Obama, aimed at enhancing cybersecurity for critical infrastructure.

Many studies have employed the NIST Cybersecurity Framework in their research. For study [xxxvi] utilized the framework to investigate the impacts of cyber regulations and security policies on organizational outcomes, focusing on the Protect function. The study presented empirical evidence demonstrating how the NIST Framework assists organizations in improving their cybersecurity readiness and resilience. Furthermore, the research referenced NIST standards to analyze the impact of cybersecurity policies on knowledge management processes, exploring how adherence to NIST guidelines can enhance the security and efficiency of knowledge management systems.

A study by [xxxvii] utilized the NIST Cybersecurity Framework to assist Italian SMEs in navigating digital transformation while managing cybersecurity risks. The study underscored the implementation of the Detection and Protection functions through technologies such as encryption and access controls. It emphasized the significance of the Respond and Recover functions in developing incident response plans and ensuring rapid recovery from cybersecurity incidents. The research applied the framework to establish continuous improvement processes, enabling organizations to adapt to evolving cyber threats. Additionally, the study referenced NIST standards to evaluate the effectiveness of cybersecurity practices in organizations using big data analytics, illustrating how adherence to NIST guidelines enhances the safeguarding of knowledge assets.

In another study by [xxii], the NIST Cybersecurity Framework was utilized to enhance cybersecurity practices within organizations in Bahrain. The study employed the Identify function for Risk Assessment, assessing and identifying cybersecurity risks to gain a comprehensive understanding of potential threats and vulnerabilities. It also utilized the Protect function to implement Security Measures, deploying tools like firewalls, encryption, and access controls to safeguard critical infrastructure and sensitive information. Additionally, the study incorporated the Detect and Respond functions for Incident Detection and Response, establishing processes to swiftly identify and mitigate cybersecurity incidents, thereby reducing their impact. Lastly, the study employed the Recover function for Recovery Planning, creating and executing plans to restore any capabilities or services affected by cybersecurity incidents promptly.

While study of [xxxvii] utilized the NIST Cybersecurity Framework to bolster cybersecurity practices in Kenyan SMEs. The study focused on employing specific functions of the framework, including Identifying Risks (NIST Identify Function), Implementing Protective Measures (NIST Protect Function), Detecting and Responding to Incidents (NIST Detect and Respond Functions), and Recovery Planning (NIST Recover Function). These efforts were aimed at strengthening cybersecurity resilience and readiness among small and medium-sized enterprises in Kenya.

These studies underscore the versatility and effectiveness of the NIST Cybersecurity Framework across diverse sectors. They emphasize its ability to establish governance frameworks, conduct comprehensive risk assessments, implement protective measures, and facilitate ongoing enhancements in cybersecurity practices.

This study implements the NIST Cybersecurity Risk Management Framework within organizational settings. The framework aids in establishing a cybersecurity governance structure by forming a committee comprising IT professionals and other pertinent stakeholders. It also delineates roles and responsibilities for cybersecurity across the organization. Utilizing this framework, organizational management can evaluate risks to their systems and infrastructure and deploy proactive measures such as firewalls, intrusion detection systems, and encryption. Furthermore, it facilitates the development of policies and procedures for managing access to sensitive information and systems, along with conducting regular cybersecurity training and awareness programs for staff members.

By employing this framework, organizations can strengthen their capability to detect threats, identify potential cybersecurity incidents, and develop response and recovery plans accordingly. The framework facilitates ongoing evaluation and enhancement of cybersecurity measures, safeguarding infrastructure and fostering a secure environment. Consequently, organizations can leverage the NIST Cybersecurity Framework to fortify their cybersecurity posture, safeguard sensitive information, and bolster the resilience of their operations.

Based on RBV, and NIST Cybersecurity Framework the researcher developed a conceptual framework that illustrates the relationships between variables in this study by the following:

Hypothesis development:

Cybersecurity Strategy and Information System Effectiveness.

The relationship between cybersecurity strategy and information system effectiveness is

considered complex and interconnected within the organizational context. [xxxviii]confirms the prerequisites for attaining cybersecurity in management information systems within select Arab countries. The study's findings delineate cybersecurity prerequisites pertinent to administrative information systems, underscoring how this security significantly influences the efficiency and overall functionality of information systems by guaranteeing continuous operation.

The study by [xxxix] demonstrated the correlation between the effectiveness of information security and the prevalence of information security threats. A robust cybersecurity strategy emphasizes safeguarding digital assets, systems, and information against cyber threats. When implemented adeptly, it fortifies the security stance of information systems, safeguarding them from unauthorized access, data breaches, malware, and other risks.

[xl] explores the tactics employed by leaders of small financial institutions in Qatar to safeguard their information systems against cyber threats, driven by the expanding reliance on computer networks in their business's trading and governance facets. The findings underscore that these leaders protect their information systems by proficiently overseeing information security practices, establishing robust cybersecurity policies, identifying, assessing, and mitigating cybersecurity risks, and implementing a comprehensive organizational strategy.

[xli] aimed to identify the primary cybersecurity risks (CSR) encountered by Kenyan SMEs and to devise an implementation strategy that serves as a guide for treating cyber-risk (CR) as a business risk. The study findings indicate that effective management of cyber-risk within SMEs hinges on investments in cybersecurity, robust cybersecurity governance, training and awareness initiatives, well-defined cybersecurity policies, proactive cybersecurity vulnerability management programs, real-time network monitoring, and incident management protocols.

Drawing from the literature review, the following hypothesis was formulated:

H1: Cybersecurity strategy has a positive impact on Information system Effectiveness.

Cyber Risk Assessment and Information System Effectiveness.

The importance of assessing cyber risks for maintaining information systems is evident in previous studies, [xi] The study introduced a novel framework that identifies practical organizational drivers and priorities aimed at enhancing cyber resilience from a regulatory standpoint. The results indicated that numerous organizations still face challenges in implementing cybersecurity risk assessment and management programs.

The study [xlii] conducted a review of existing cyber risk assessment methodologies and their applicability to NIST guidelines for Internet of Medical Things (IoMT) systems, focusing on Operationally Critical Threats, Asset and Vulnerability Assessment, Threat Assessment, and Remediation Analysis.

The study described in [xliii] aimed to establish a framework for cybersecurity risk assessment within an organization. This framework enables systematic evaluation of a firm's strategic alignment with its cybersecurity posture. The objective is to aid senior management in optimizing security investments while effectively managing cyber risks within their organization. This research addresses the critical need to enhance the capabilities of

organizational leaders, including Chief Information Officers (CIOs) and others, in addressing the escalating challenge of cybersecurity threats through a comprehensive methodology for cross-organizational cybersecurity risk management.

Therefore, the second hypothesis for the study was proposed as follows:

H2: Cyber Risk Assessment has a positive impact on Information System Effectiveness.

Cyber Risk Analysis and Information System Effectiveness.

According to [xliv] [iii] [ix], highlight the critical role of Cyber Risk Analysis in assessing the effectiveness of information systems across various sectors, including healthcare, financial institutions, and educational settings. These studies explore how analyzing cyber risks influences the enhancement of information system effectiveness within these specific domains, the third hypothesis for the study was proposed as follows:

H3: Cyber Risk analysis has a positive impact on information system effectiveness.

Response to Cyber Risk and Information System Effectiveness.

A study referenced by [xli] addressed responses to cyber risks, highlighting cyber security incident management as a significant area of concern. The study underscored that many companies are inadequately prepared due to limited resources, leading to heightened vulnerability to cyber security incidents. It recommends that companies develop actionable strategies to effectively manage discovered cybersecurity occurrences.

Another study, conducted by [xlv], aimed to investigate managerial responses to data security breaches and whether such breaches prompt increased earnings management activities. The findings indicate that firms are more likely to engage in earnings management, particularly when breaches involve financial data and disclosure of the breach is delayed.

these previous studies indicate a positive relationship between response to cyber risk and information system effectiveness. Therefore, the fourth hypothesis for the study was proposed as:

H4: response to cyber risk has a positive impact on information system effectiveness.

Recovery Cyber Risk and Information System Effectiveness.

The relationship between recovery from cyber risk incidents and information system effectiveness is crucial for maintaining the resilience and functionality of organizations' IT environments. The literature review on this topic explores various studies that investigate how effective recovery strategies contribute to the overall effectiveness of information systems. This was confirmed by a study conducted by [xlvi] the focus was on strategies for recovering equipment and restoring operations following a cyber incident. Communication with industry partners at the NIST Center for Teaching and Learning (CTL) outlined an approach to responding to and recovering from attacks in the manufacturing sector. This approach leverages cybersecurity capabilities such as event reporting, log review, event analysis, and incident handling and response, with the implementation of recovery plans during or after cybersecurity incidents.

Another study [xix] aimed to develop an intelligent electronic security platform designed to

protect companies at every stage of the attack process (prevention, detection, containment, and recovery). This platform aims to enhance the security of small and medium-sized enterprises (SMEs) and reduce economic and social impacts resulting from attacks. It helps SMEs prevent attacks, detect threats to their systems, take preemptive measures to mitigate attack effects, and respond effectively to restore systems to normal operation.

Additionally, study [xli] highlighted the ongoing need for small and medium-sized companies to develop internal and external communication protocols to enhance cybersecurity resilience. The study emphasized that cybersecurity training and awareness remain critical areas for improvement to effectively manage cyber risks and analyze collected data.

Accordingly, the fifth hypothesis for the study was proposed as follows:

H5: recovery cyber risk has a positive impact on information system effectiveness.

Activity Control and Information System Effectiveness.

In a study conducted by [xlvii], the effectiveness of real-time monitoring in detecting anomalous behaviors was investigated. The findings highlighted the importance of continuous monitoring in strengthening the security of information systems and enabling timely responses to potential security incidents. The role of auditing in enhancing information system effectiveness has been a topic of academic investigation.

Furthermore, research by [xlviii] examined the influence of regular audits on system resilience. Their study underscores how systematic auditing helps identify vulnerabilities and maintain resilient information systems, particularly in the context of evolving cyber threats.

Therefore, the Sixth hypothesis for the study was proposed as follows:

H6: activity control has a positive impact on information system effectiveness.

Research Framework:

Based on the above, and depending on the literature review related to the relationship between cybersecurity strategy components and information system effectiveness (see Figure 1) the researchers' development of a proposed framework illustrates the relationship between cybersecurity strategy components and information system effectiveness.

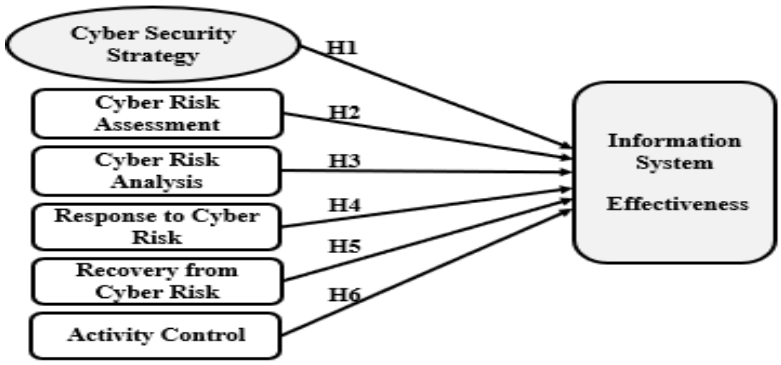

Figure 1 Proposed Research Framework

This proposed framework represents the proposed vision to include the cybersecurity strategy dimensions in organizations to enhance the effectiveness of information systems.

The Research Approach:

The research approach refers to the accurate investigative process aimed at discovering or collecting facts about an issue in a specific method. To achieve what the current research pursued, the descriptive analytical approach was used, which focuses on an accurate and detailed description of a specific phenomenon or topic to evaluate a specific situation or monitor a phenomenon and understand its content. Previous research and literature review that dealt with the variables of the current research were reviewed.

3. Recommendation:

In the realm of increasing growth of threats and risks especially toward information systems in organizations, the pivotal role of cybersecurity cannot be overstated. It begins with a foundational emphasis on cultivating a positive cybersecurity culture, this culture is not just about adherence to protocols; it's about embedding cybersecurity into the compliance to information system requirements of an organization across various dimensions, thereby achieving satisfaction for its stakeholders and enhancing its performance aiming to create and establish secure and resilient environment work.

Hence, we will present some recommendations that organizations must follow to ensure that their information systems are effective and successfully adapt to internal and external environmental changes: firstly, organizations should take and use robust cybersecurity measures by developing and formulating strategies for cybersecurity including investing in developed security technologies by using new tools, mechanisms, and methods for managing and protecting their information systems and information from cyber threats, and risks to keep confidentiality, integrity, and availability of information within their systems, and to ensure their continuity, survival, and growth.

then, organizations should adopt approaches to managing and protecting their information systems and information in them from risks and threats that threaten their systems and assets by implementing response and recovery plans that outline measures, practices, policies, and techniques that must be followed in order to mitigate cyber risks to protect their systems and ensuring the effectiveness of information systems.

these strategies for cybersecurity should be aligned with the overall organization's strategy to ensure alignment with their organizational goals and objectives through establishing clear communication channels between cybersecurity teams and other departments to facilitate proactive risk management.

Attention to the formulation of effective cybersecurity strategies plays a critical role in reinforcing an organization's resilience against cyber threats.

as well as organizations should also enhance collaboration and knowledge sharing between cybersecurity specialists, and relevant stakeholders to stay informed about emerging threats and best practices, through participation in conferences, workshops, and forums.

Furthermore, the development and implementation of comprehensive training programs for employees, particularly those within information technology units, are paramount. These programs should focus on fostering a deep understanding of cybersecurity practices, promoting responsibility for usage behaviors, and heightening awareness of potential threats. By empowering employees with this knowledge, organizations can fortify their first line of defense against cyber threats.

Lastly, the landscape of cybersecurity is ever-evolving, with new threats emerging at an unprecedented pace. This reality underscores the necessity for continuous innovation and research within the field of cybersecurity. Staying ahead of potential hacks and threats requires a proactive approach to cybersecurity, that anticipates future challenges and devises innovative solutions to address them.

In sum, the journey towards enhanced information systems is multifaceted, involving the cultivation of a cybersecurity-aware culture, interdisciplinary research, employee training, strategic cybersecurity planning, and ongoing innovation. Together, these components form a comprehensive framework for organizations aiming to navigate the complexities of the digital age securely and successfully.

4. Conclusion:

In conclusion, this study underscores the inevitability for organizations to prioritize the development of comprehensive cybersecurity strategies. As organizations increasingly rely on information systems to achieve their operations, goals, and general strategies, the protection of these systems against risks, threats, and attacks is essential, crucial, and indispensable.

based on the above that are mentioned in recommendations, organizations can address and confront the challenges, and obstacles and enhance the effectiveness of their information systems, ultimately safeguarding their assets, enhancing stakeholder's trust, and continuity of their survival and growth. By considering cybersecurity as strategic inevitable and unavoidable. Thus, through adopting proactive plans, organizations can mobility the cybersecurity landscape with confidence and successfully.

Acknowledgment:

We thank Mohammad Falahat[2] for his contribution to this work. Special thanks to the Asia Pacific University of Technology and Innovation (APU).

Funding Statement:

"No financing / There is no fund received for this article".

Data Availability:

“No new data were created or analyzed in this study”.

References

1. [i]. Parsons E K, Panaousis E, Loukas G, and Sakellari G, A survey on cyber risk management for the Internet of things, Applied Sciences, 2023; 13(15): 9032, https://doi.org/10.3390/app13159032.
2. [ii]. Melaku H M, Context-Based and Adaptive Cybersecurity Risk Management Framework, Risks, 2023; 11(6): 101, https://doi.org/10.3390/risks11060101.
3. [iii]. Lee I, Cybersecurity: Risk management framework and investment cost analysis, Business Horizons, 2021; 64(5): 659- 671, https://doi.org/10.1016/j.bushor.2021.02.022.
4. [iv]. Goel R, Haddow J, Kumar A, Managing cybersecurity risk in government: an implementation model, IBM Center for the Business of Government, Washington, (2018), http://www. business of government. org/.
5. [v]. Rodrigues A R D, Ferreira F A, Teixeira F, and Zopounidis C, "Artificial intelligence, digital transformation and cybersecurity in the banking sector, A multi-stakeholder cognition-driven framework," Research in International Business And Finance, 2022; 60: 101616.
6. [vi]. Rodrigues A R D, Ferreira F A, Teixeira F, and Zopounidis C, "Artificial intelligence, digital transformation and cybersecurity in the banking sector, A multi-stakeholder cognition-driven framework," Research in International Business And Finance, 2022; 60: 101616.
7. [vii]. Limba T, Plėta T, Agafonov K, and Damkus M, Cyber security management model for critical infrastructure, Entrepreneurship and sustainability issues, Vilnius: Entrepreneurship and Sustainability Center, 2017; 4(4): 559-573, http://doi.org/10.9770/jesi.2017.4.4(12).
8. [viii]. Tondel I A, Seehunen F,. Gjaere E A, and. Moe M E G, "Differentiating Cyber Risk of Insurance Customers: The Insurance Company Perspective," In International Conference on Availability, Reliability and Security, Springer, 2016; 175-190.
9. [ix]. Gordon L A, Loeb M. P, and Zhou L, Integrating cost-benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model, Journal of Cybersecurity, 2020; 6(1): tyaa005. Doi: 10.1093/cybsec/tyaa005.
10. [x]. National Institute of Standards and Technology (NIST), Framework for improving critical infrastructure security, Washington: DC, NIST, 2014; https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf.
11. [xi]. Jarjoui S, and Murimi R, A framework for enterprise cybersecurity risk management, In Advances in cybersecurity management, Cham: Springer International Publishing, 2021; 139-161, https://www.researchgate.net/.
12. [xii]. Liu C, Tan C K, Fang Y S, and Lok T S, The security risk assessment methodology, Procedia Engineering, 2012; 43: 600-609, Doi: 10.1016/j.proeng.2012.08.106.
13. [xiii]. Stoneburner G, Goguen A, and Feringa A, Risk management guide for information technology systems, NIST special publication, 2002; 800(30): 800-30, https://sites.pitt.edu/~dtipper/2825/NIST_Risk.pdf.
14. [xiv]. National Institute for Standard and Technology (NIST), Guide for applying the risk management framework to federal information systems, U.S. Department of Commerce, 2022; http://dx.doi.org/10.6028/NIST.SP.800-37r1
15. [xv]. Eggers S, and Le Blanc K, Survey of cyber risk analysis techniques for use in the nuclear industry, Progress in Nuclear Energy, 2021; 140: 103908, https://doi.org/10.1016/j.pnucene.2021.103908.
16. [xvi]. Shaikh F A, and Siponen M, Organizational Learning from Cybersecurity

Performance: Effects on Cybersecurity Investment Decisions, Information Systems Frontiers, 2023; 1-12, https://doi.org/10.1007/s10796-023-10404-7.

17. [xvii]. Ganin A A, Quach P, Panwar M, Collier Z A, Keisler J M, Marchese D, and Linkov I, Multicriteria decision framework for cybersecurity risk assessment and management, Risk Analysis, 2020; 40(1): 183-199, https://doi.org/10.1111/risa.12891.
18. [xviii]. Zamfiroiu A, and Sharma R C, Cybersecurity Management for Incident Response, Romanian Cyber Security Journal, ISSN, 2022; 2668-6430. http://doi.org/10.54851/v4i1y202208
19. [xix]. López M A, Lombardo J, López M, Alba M, Velasco S, Braojos M, and Fuentes-García M, Intelligent Detection and Recovery from Cyberattacks for Small and Medium-Sized Enterprises, International Journal of Interactive Multimedia and Artificial Intelligence, 2020; 6(3): 1-8. DOI: 10.9781/ijimai.2020.08.003.
20. [xx]. Kashyap A K, and Wetherilt A, Some principles for regulating cyber risk, In AEA Papers and Proceedings, 2019; (109): 482-487, DOI: 10.1257/pandp.20191058.
21. [xxi]. Al-Manea A, Requirements for Achieving Cybersecurity in Saudi Universities in Light of Vision 2030, Scientific Journal, 2022; 38 (1): 156-19, http://www.aun.edu.eg/faculty_education/arabic.
22. [xxii]. Hasan S, Ali M, Kurnia S, and Thurasamy R, Evaluating the cyber security readiness of organizations and its influence on performance, Journal of Information Security and Applications, 2021; 58: 102726, https://doi.org/10.1016/j.jisa.2020.102726.
23. [xxiii]. Al-Samhan M, Requirements for Achieving Cybersecurity for Administrative Information Systems at King Saud University, College of Education Journal, 2020; 111(1): 2-29, https://search.emarefa.net/detail/BIM-1101516.
24. [xxiv]. Reilly D, Contemporary Issues in Information Systems - A Global Perspective, In Zemmouchi-Ghomari L, Basic Concepts of Information Systems, United Kingdom, 2022; 7-25, DOI: 10.5772/intechopen.97644.
25. [xxv]. Antunes M, Maximiano M, Gomes R, and Pinto D, Information security and cybersecurity management: A case study with SMEs in Portugal, Journal of Cybersecurity and Privacy, 2021; 1(2), 219-238, https://doi.org/10.3390/jcp1020012.
26. [xxvi]. DeLone W H, and McLean E R, The DeLone and McLean model of information systems success: a ten-year update, Journal of management information systems, 2003; 19(4): 9-30, https://doi.org/10.1080/07421222.2003.11045748.
27. [xxvii]. Al-Mamary Y H, Shamsuddin A, and Aziati N, The relationship between system quality, information quality, and organizational performance, International Journal of Knowledge and Research in Management & E-Commerce, 2014; 4(3), 7-10, https://www.researchgate.net/profile/Yaser-Hasan-Salem-Al-Mamary-d-yasr-hsn-.
28. [xxviii]. Widiastuti R, Haryono B S, and Said A, Influence of system quality, information quality, service quality on user acceptance and satisfaction and Its impact on net benefits (study of information system user's lecturer performance load (BKD) in Malang State University), HOLISTICA–Journal of Business and Public Administration, 2019; 10(3): 111-132, DOI:10. 2478/hjbpa-2019-0032.
29. [xxix]. Jiang G, Liu F, Liu W, Liu S, Chen Y, and Xu D, Effects of information quality on information adoption on social media review platforms: Moderating role of perceived risk, Data Science and Management, 2021; 1(1): 13-22, https://doi.org/10.1016/j.dsm.2021.02.004.
30. [xxx]. Alshikhi O A, and Abdullah B M, Information quality: definitions, measurement, dimensions, and relationship with decision making, European Journal of Business and Innovation Research, 2018; 6(5): 36-42, https://www.academia.edu/download/76933348/Information-Quality-Definitions-Measurement-Dimensions-and-Relationship-with-Decision-Making-6.pdf.

31. [xxxi]. Al-Badawi A, and Al-Qahtani I, Using the SERVQUAL Model of Perceptions and Expectations in Measuring the Quality of Educational Services in Public Schools in Urban Abha City, Faculty of Education Journal, Al-Azhar University, 2019; 2 (184): 11-49, https://doi.org/10.21608/jsrep.2019.78731.
32. [xxxii]. Vatolkina N, Gorbashko E, Kamynina N, and Fedotkina O, E-service quality from attributes to outcomes: The similarity and difference between digital and hybrid services, Journal of Open Innovation: Technology, Market, and Complexity, 2020; 6(4): 143, https://doi.org/10.3390/joitmc6040143.
33. [xxxiii]. Rita P, Oliveira T, and Farisa A, The impact of e-service quality and customer satisfaction on customer behavior in online shopping, Heliyon, 2019; 5(10): 1-14, https://doi.org/10.1016/j.heliyon.2019.e02690.
34. [xxxiv]. Barney J, "Firm resources and sustained competitive advantage", Journal of Management, 1991, 17 (1): 99-120, doi: 10.1177/014920639101700108.
35. [xxxv]. Wernerfelt B, "A resource-based view of the firm", Strategic Management Journal, 1984, 5(2): 171-180, doi: 10.1002/smj.4250050207.
36. [xxxvi]. Hovav A, Gnizy I, and Han J, The effects of cyber regulations and security policies on organizational outcomes: a knowledge management perspective, European Journal of Information Systems, 2023, 32(2): 154-172, https://doi.org/10.1080/0960085X.2021.1908184
37. [xxxvii]. Obitade P O, Big data analytics: a link between knowledge management capabilities and superior cyber protection, Journal of Big Data, 2019, 6(1): 71, https://doi.org/10.1186/s40537-019-0229-9.
38. [xxxviii]. Samara N K, Cybersecurity Requirements for Management Information Systems, Journal of Information Security, 2023; 14(3): 212-226, https://doi.org/10.4236/jis.2023.143013.
39. [xxxix]. Masrek M N, Soesantari T, Khan A, and Dermawan A K, EXAMINING THE RELATIONSHIP BETWEEN INFORMATION SECURITY EFFECTIVENESS AND INFORMATION SECURITY THREATS, International Journal of Business & Society, 2020; 21(3): 1203-1214, https://www.ijbs.unimas.my/images/repository/pdf/Vol21-no3-paper15.pdf.
40. [xl]. Rawass J, Cybersecurity strategies to protect information systems in small financial institutions (Publication No.13904293), [Doctoral dissertation, Walden University], ProQuest Dissertations and Theses Global, 2019; https://www.proquest.com/dissertations-theses/cybersecurity-strategies-protect-information/docview/2272840761/se-2?accountid=27719.
41. [xli]. Rishad A, Managing Cybersecurity as A business Risk in Information Technology-Based SMES (Publication No.4009), [Master dissertation, University of Nairobi], ProQuest Dissertations and Theses Global, 2019; .http://erepository.uonbi.ac.ke/handle/11295/107172
42. [xlii]. Kandasamy K, Srinivas S, Achuthan K, and Rangan V P, IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process, EURASIP Journal on Information Security, 2020; (8): 1-18, https://doi.org/10.1186/s13635-020-00111-0.
43. [xliii]. Goel R, Kumar A, and Haddow J, PRISM: a strategic decision framework for cybersecurity risk assessment, Information & Computer Security, 2020; 28(4): 591-625, https://doi.org/10.1108/ICS-11-2018-0131.
44. [xliv]. Lee M, Jang-Jaccard J, and Kwak J, Novel Architecture of Security Orchestration, Automation and Response in Internet of Blended Environment, Computers, Materials & Continua, 2022; 73(1): 200-223, DOI: 10.32604/cmc.2022.028495.
45. [xlv]. Xu S, A study on knowledge management capabilities towards new product innovation type and development performance of Chinese businesses, Acta Oeconomica, 2015; 65(s2):

145-157, https://doi.org/10.1556/032.65.2015.s2.11.

46. [xlvi]. Powell M, Pease M, Stouffer K, Tang C, Zimmerman T, Hoyt J, ... and Zheng K, Responding to and Recovering from a Cyberattack: Cybersecurity for the Manufacturing Sector, Project Description, National Institute of Standards and Technology (NIST) & U.S. Department of Commerce, 2022; https://csrc.nist.gov/pubs/pd/2022/02/28/responding-to-and-recovering-from-a-cyberattack-ma/ipd.
47. [xlvii]. Brown P, Ly T, Pham H, and Sivabalan P, Automation and management control in dynamic environments: Managing organisational flexibility and energy efficiency in service sectors, The British Accounting Review, 2020; 52(2): 100840, https://doi.org/10.1016/j.bar.2019.100840.
48. [xlviii]. García-Martínez I, Fernández-Batanero J M, Cobos Sanchiz D, and Luque de La Rosa A, Using mobile devices for improving learning outcomes and teachers' professionalization, Sustainability, 2019, 11(24): 6917, https://doi.org/10.3390/su11246917.