International Journal of Business and Technopreneurship
Volume 13, No 3, October 2023 [253-270]

Managing Cybersecurity Risks in Emerging Technologies

Mohd Noorulfakhri Yaacob[1], Syed Zulkarnain Syed Idrus[1,2] and Mariam Idris[1,3]

[1]Department of Communication, Faculty of Business & Communication, Universiti Malaysia Perlis, 01000 Kangar, Perlis, Malaysia
[2] Centre of Excellence for Social Innovation & Sustainability, Universiti Malaysia Perlis, 01000, Kangar, Perlis, Malaysia
[3]Faculty of Innovative Design & Technology, Universiti Sultan Zainal Abidin, Kampus Gong Badak, 21300 Kuala Terengganu, Terengganu, Malaysia

Received 14th September 2023, Revised 26th October 2023, Accepted 30th October 2023

ABSTRACT

Nowadays, it has become increasingly important for companies to effectively manage cybersecurity risks in emerging technologies. This article presents an overview of cybersecurity in these technologies. It sheds light on the obstacles that businesses encounter when dealing with these risks. The field of cybersecurity poses challenges that need to be overcome. Technical challenges include securing communication networks and protecting data and systems from threats. Moreover, it is crucial to ensure the dependability and trustworthiness of emerging technologies. Organisational challenges involve preparing and training employees and devising effective strategies to address the unique cybersecurity issues associated with new technologies. Regulatory challenges arise due to changing compliance requirements in a global context where different countries have diverse cybersecurity laws. To effectively manage cybersecurity risks, it is essential to follow established risk management practices, such as identifying and assessing risks systematically. However, there are gaps in research and practices that should be addressed. These gaps include the lack of frameworks for conducting cost-benefit analyses, a limited understanding of the role played by error in cybersecurity incidents, and the necessity for comprehensive strategies to deal with the constantly evolving landscape of cybersecurity threats. Bridging these gaps requires investigation along with developing effective strategies for improving cybersecurity in emerging technologies.

Keywords: Cybersecurity Risks, Risk Management Strategies, Technical Challenges

1. INTRODUCTION

In today's rapidly evolving digital landscape, emerging technologies such as Artificial Intelligence (AI), autonomous vehicles, the Internet of Things (IoT), Machine Learning (ML), blockchain, and Cloud Computing are revolutionising various sectors, from healthcare and finance to manufacturing and education. While innovation and efficiency opportunities are offered by technology, organisations must also effectively manage new cybersecurity risks. Integrating these technologies into existing infrastructures not only expands the attack surface but also introduces unique vulnerabilities that traditional cybersecurity measures may not adequately address. For instance, the decentralised nature of blockchain technology, while offering enhanced security in some respects, also poses challenges to data integrity and system interoperability.

*Corresponding Author: fakhri@unimap.edu.my

Similarly, with its myriad connected devices, the IoT presents risks related to data privacy, unauthorised access, and potential misuse of sensitive information. Moreover, the human element remains a significant variable in the cybersecurity equation. Despite the tremendous advancements in technology, security breaches still occur frequently. This often happens because of human mistakes, which can be attributed to a lack of awareness or training. Moreover, organisations face challenges due to compliance issues as laws struggle to keep up with technological advancements. The complexity of cybersecurity is further compounded by the use of technologies, which necessitates a comprehensive approach that addresses not only technical aspects but also organisational, human and legal factors.

In this context, it is important to develop a comprehensive approach to effectively handle the cybersecurity threats that come with the emergence of new technologies. Organisations should not solely rely on risk management methods. It should also develop a holistic framework that considers the unique challenges presented by these technologies. This article will explore the topic of managing cybersecurity risks in emerging technologies.

2. RESEARCH OBJECTIVES

The objectives of this research are to investigate and examine the methods used to handle cybersecurity risks in emerging technologies. Specifically, the study seeks:

- To investigate the current state of cybersecurity in emerging technologies, including the challenges and implications for organisations and stakeholders.
- To identify the technical, organisational, and regulatory challenges faced in managing cybersecurity risks in emerging technologies.
- To examine the existing risk management strategies and frameworks employed to address emerging technologies' cybersecurity risks.

3. LITERATURE REVIEW

The effective management of cybersecurity risks is extremely important for organisations across industries, especially when dealing with emerging technologies. The changing landscape of technology has presented organisations with advantages and possibilities. This includes advancements like AI, ML, IoT, blockchain and cloud computing. These advancements have the potential to improve efficiency, productivity, and innovation. However, the utilisation of emerging technologies also introduces complex cybersecurity risks that must be managed effectively. A literature review was conducted to analyse the current state of the literature on managing cybersecurity risks in emerging technologies. The results showed that emerging technologies can enhance cybersecurity and resilience for organisations, but there are also challenges that organisations may face when implementing these technologies (Li et al., 2022).

3.1 Current State of Cybersecurity in Emerging Technologies

Organisations' dependence on new technologies emphasises the importance of cybersecurity for innovation and efficiency. New technologies like IoT, AI, and cloud computing have brought new cybersecurity risks. Organisations must understand these risks and implement strategies to protect their systems, data, and operations.

In a study by Lee (2020), it introduces a four-layer framework for managing cyber risks in the IoT. Proposes using programming to allocate financial resources to multiple cybersecurity projects within this framework. The paper also emphasises a gap in existing cybersecurity frameworks, especially when allocating resources for cybersecurity initiatives. While guidelines

like the National Institute of Standards and Technology (NIST) Cybersecurity Framework offer insights into assessing and mitigating risks, they lack guidance on conducting cost-benefit analyses or making informed decisions about implementation priorities. This lack of specificity often puts organisations in a position where they have to rely on intuition rather than solid data when allocating funds to cybersecurity projects.

In 2021, Fouad (2021) examines the security and privacy issues in the context of blockchain technology. The authors discuss the vulnerabilities and attacks that can compromise the security of blockchain systems and propose mitigation strategies to enhance the security and privacy of blockchain-based applications. Furthermore, (Ding et al., 2021) explore the security challenges and solutions in the context of edge computing. The authors discuss the unique security risks associated with edge computing and present various security mechanisms and protocols to protect edge devices and data.

Emerging technologies, including Fintech, IoT, and Smart Grid, create uncertainty and challenges in problem definition and regulatory authority. The nature of these technologies increases the type and scope of assets vulnerable to cyber threats, leading to a larger number of governing units claiming jurisdiction over cybersecurity-related issues. This uncertainty regarding problem definition and regulatory authority has led legislators to seek assistance from federal bureaucrats to decrease their uncertainty (Taeihagh et al., 2021). To tackle cybersecurity challenges posed by emerging technologies, Security Information and Event Management (SIEM) systems are a promising solution. SIEM systems possess the ability to identify, standardise and establish connections between security incidents. This makes them highly valuable for safeguarding ecosystems like the Smart Grid (Radoglou-Grammatikis et al., 2021).

In addition, Raimundo and Rosário (2022) have explored cybersecurity within the framework of the Industrial Internet of Things (IIoT). They emphasise topics like machine learning and cloud computing, which are commonly used to tackle security issues in IIoT. In the same year, Hireche et al. (2022) conducted a study that centres on the security challenges and solutions related to the Internet of Medical Things (IoMT). They examine various security threats and suggest measures to safeguard sensitive medical data in IoMT systems.

Overall, these literature reviews provide valuable insights into the current state of cybersecurity in emerging technologies. They highlight the challenges and vulnerabilities in these technologies and propose solutions and strategies to mitigate cybersecurity risks. By understanding these issues and implementing appropriate security measures, organisations can protect their systems and data from cyber threats.

3.2 Challenges in Managing Risks in Emerging Technologies

In the fast-paced world of technology, organisations are increasingly concerned about addressing cybersecurity risks that come with emerging technologies. The challenges encompass technical, organisational, and regulatory dimensions with significant interconnections. Technological advancements such as IoT, AI, and cloud computing are undoubtedly transformative. However, they also bring in new vulnerabilities that must be addressed. Recent incidents have highlighted the need for organisations to proactively secure devices and safeguard data to anticipate risks associated with emerging technologies. Continuous monitoring and timely threat intelligence are crucial due to the dynamic nature of these technologies.

There is a significant need for organisations to address the scarcity of skilled cybersecurity professionals who can adapt to the changing landscape. Apart from hiring, organisations must create a pervasive culture of cybersecurity. This includes implementing elaborate training

programmes awareness campaigns, and building a sense of collective responsibility towards cyber resilience.

Regulatory challenges present a unique dilemma. As technology advances at a rapid pace, regulatory frameworks struggle to keep up, creating gaps that lead to uncertainties. Recent discussions on data protection and privacy regulations highlight the complexities that organisations must navigate. Balancing compliance with the ability to adjust to new regulatory changes is a delicate task that organisations must strive to master.

The interconnections between these three challenges add complexity to the technical landscape and magnify the challenges faced by organisations and regulators. Ensuring device security, privacy standards, and managing vast ecosystems while complying with ever-changing regulations are crucial. Regulatory challenges intertwine with both technical and organisational aspects. As technology outpaces regulatory frameworks, gaps emerge, leading to uncertainties. Balancing compliance and agility amidst new regulations is a complex challenge involving technical and organisational dimensions.

3.2.1 Technical Challenges

Managing cybersecurity risks in emerging technologies presents several technical challenges that organisations need to address. These challenges arise due to the complex and evolving nature of emerging technologies and the increasing sophistication of cyber threats. The following references provide insights into the technical challenges associated with managing cybersecurity risks in emerging technologies.

The rise of Fintech in the financial sector emphasises the need for robust cybersecurity measures and anti-fraud protocols. The technical challenges in securing financial technologies include protecting sensitive financial data, ensuring secure transactions, and safeguarding against cyber threats targeting financial institutions (Ng & Kwok, 2017).

Emerging technologies, like the IoT, Smart Grid and Fintech have brought about changes in industries, including power grids. However, integrating these technologies into power grids also brings cybersecurity challenges and vulnerabilities. Given that power grids are infrastructure, it is crucial to have security measures in place to protect against cyber threats and ensure the grid's reliability and resilience. Power grid cybersecurity faces challenges in securing communication networks, control systems, and the grid's resilience against cyber-attacks (Sakhnini et al., 2021). As power grid systems become more complex and interconnected with the rise of IoT and Smart Grid technologies, the potential risks and vulnerabilities increase well (Yan et al., 2012). Consequently, it is essential to develop and implement security mechanisms and protocols that can prevent access, data breaches or tampering with devices (Radoglou-Grammatikis et al., 2021). Researchers stress the importance of addressing cybersecurity challenges to power grids since these efforts play a role in protecting sensitive data within the grid while maintaining its stability. The importance of cybersecurity in the development of grid technologies has been acknowledged by institutions such as the NIST, the Energy Expert Cyber Security Platform (EESCP) and the European Commissions Smart Grids Task Force (Sakhnini et al., 2021). Numerous approaches and techniques have been suggested to enhance the security and robustness of power grid networks. The identification and modelling of nodes within these grids have become vital in order to strengthen system resilience and reduce risks (Li et al., 2022). Measures like access control policies grained dynamic access control methods, and security assessment technologies have been explored to protect power grid systems from access and cyber threats (Li et al., 2023; Qiu et al., 2022). Additionally, cloud-based charging management and efficient communication frameworks have also been studied to ensure energy management and stability in power grids (Rimal et al., 2022). In summary, while integrating emerging technologies into power grids brings opportunities, it also introduces cybersecurity risks.

Addressing challenges, implementing security measures and adopting comprehensive cybersecurity strategies are crucial for safeguarding power grid systems against cyber threats to ensure reliable operation.

The rise of emerging technologies, such as the IoT, has created major challenges in effectively managing cybersecurity risks. The integration of IoT devices into various domains, including healthcare, industrial management, and smart homes, introduces new vulnerabilities and complexities (Sharma & Sharma, 2022). To mitigate these risks, cybersecurity certification schemes are gaining momentum, driven by industry, governmental institutions, and research communities (Khurshid et al., 2022). However, there are challenges in making these certification schemes applicable to the diverse IoT landscape (Matheu et al., 2020). In the field of cybersecurity, there are technical obstacles that need attention. These challenges involve securing communication networks, safeguarding control systems, and ensuring the resilience of devices against cyber-attacks (Sharma & Sharma, 2022). Risk assessment and testing processes play a role in establishing a certification framework for cybersecurity (Matheu et al., 2020). In the past, cybersecurity risks associated with IoT have hindered its adoption. However, efforts are underway to address these risks through the development of standards and frameworks for cybersecurity (Khader et al., 2021). Nevertheless, challenges persist in identifying and categorising risks accurately, maintaining privacy and security in systems and managing the interaction between devices and the physical world (Tawalbeh et al., 2020). To overcome these challenges successfully requires an approach that integrates research findings, technical tools, policy measures and governance structures. To sum up, the management of cybersecurity risks in emerging technologies in relation to the IoT poses challenges. These challenges include intricacies, evaluating risks, protecting privacy and establishing certification systems. Overcoming these obstacles necessitates a strategy, cooperation among the parties involved and the creation of comprehensive cybersecurity frameworks that cater to the unique demands of emerging technologies.

Managing the risks associated with cybersecurity can be quite challenging, especially when it comes to dealing with emerging technologies like cloud computing. Cloud computing has completely transformed the way organisations store, process and access data. However, it also brings along vulnerabilities and complexities (Salek et al., 2022). Securing communication networks, safeguarding data and applications and ensuring the privacy and integrity of cloud-based services are some of the challenges involved in cybersecurity for cloud computing. The changing nature of cloud environments shared responsibility models, and the potential for access or data breaches pose significant risks (Kaja et al., 2022). To tackle these challenges effectively, various measures and best practices have been suggested in the field of cybersecurity. These include employing encryption techniques, implementing robust access control mechanisms, utilising intrusion detection systems and conducting security audits (Morol, 2022). Additionally, it is crucial to establish defined incident response plans and continuously monitor cloud environments to detect and mitigate cyber threats. Furthermore, managing cybersecurity risks in cloud computing is also complicated by regulatory factors that need (Aljumah & Ahanger, 2020). The complexity of security practices increases when it comes to complying with data protection and privacy regulations, like the General Data Protection Regulation (GDPR) (Paul et al., 2020). Making sure that these regulations are followed as dealing with jurisdictional issues and contractual agreements requires careful coordination between cloud service providers and their customers (Kumar & Kumar, 2021). Moreover, the rapid progress of technologies like quantum computing poses challenges to cloud computing security. Quantum computing has the potential to break encryption algorithms leading to the need for developing encryption methods that are resistant to quantum attacks. Addressing the impact of quantum computing on cloud security requires proactive research and collaboration between academia, industry, and policymakers. In conclusion, managing cybersecurity risks in emerging technologies, particularly in the context of cloud computing, presents significant challenges. Technical complexities, legal and regulatory compliance, and the evolving threat landscape require organisations to adopt comprehensive

cybersecurity strategies. Organisations can effectively mitigate cybersecurity risks in cloud computing by implementing robust security measures, staying updated on emerging threats and fostering collaboration between stakeholders.

Managing the risks associated with cybersecurity in emerging technologies in the realm of AI and ML presents significant challenges. The integration of AI and ML technologies brings forth complexities and vulnerabilities that must be addressed to ensure cybersecurity measures. In terms of challenges, securing AI models and algorithms safeguarding data used for training and inference as well as ensuring the reliability and integrity of AI systems are paramount concerns (Matheu et al., 2020). Given the nature of AI and ML coupled with the potential for attacks and data poisoning, it becomes crucial to implement advanced security measures to mitigate substantial risks (Goldblum et al., 2020). Moreover, dealing with the lack of interpretability and explainability in AI and ML models poses obstacles when it comes to identifying biases, vulnerabilities or malicious activities that may arise (Harshith et al., 2023). To effectively manage risk in cybersecurity, it is imperative to prioritise transparency and accountability within AI and ML systems. Furthermore, keeping pace with the evolution of AI and ML technologies necessitates frameworks and regulations that can adequately address cybersecurity concerns (Geluvaraj et al., 2018). The dynamic nature of AI and ML requires continuous monitoring, updating, and patching to address emerging vulnerabilities and threats. Collaboration between researchers, industry experts, and policymakers is essential to develop robust cybersecurity standards and guidelines for AI and ML. In conclusion, managing cybersecurity risks in emerging technologies, particularly in the context of AI and ML, presents unique challenges. Technical complexities, interpretability, and the evolving threat landscape require organisations to adopt comprehensive cybersecurity strategies.

Emerging technologies, such as Blockchain, create new challenges in managing cybersecurity risks. The adoption of Blockchain technology is taking place at a fast pace, but security risks and concerns associated with Blockchain exist (Zamani et al., 2018). Technical challenges in Blockchain cybersecurity include securing communication networks, protecting data and transactions, and ensuring the integrity and reliability of Blockchain systems (Maidamwar & Chavhan, 2020). The decentralised and transparent nature of Blockchain introduces unique vulnerabilities that require advanced security measures (Kushwaha et al., 2022). Furthermore, the lack of a common framework for developing and implementing security management practices for Blockchain poses challenges in managing cybersecurity risks (Canelon et al., 2019). The absence of a protocol for documenting and reporting incidents hinders the ability to learn from past mistakes and improve security practices. Additionally, the rapid evolution of Blockchain technology outpaces the development of comprehensive cybersecurity frameworks and regulations. Collaboration between researchers, industry experts, and policymakers is crucial to address these challenges and develop robust cybersecurity standards for Blockchain (Parizi et al., 2020). In the context of Blockchain technology, various applications and domains face specific cybersecurity challenges. For example, in the finance sector, the implementation of Blockchain requires regulatory support, interoperability, and standardisation across platforms (Abeysekera & Kumarawadu, 2022). In the power generation and distribution sector, the integration of AI and Blockchain introduces new challenges in ensuring cybersecurity and staying ahead of evolving threats (Oubelaid, 2023). In conclusion, managing cybersecurity risks in emerging technologies, particularly in the context of Blockchain, presents unique challenges. Technical complexities, the lack of a common framework, and the evolving threat landscape require organisations to adopt comprehensive cybersecurity strategies. Organisations can mitigate cybersecurity risks in Blockchain technology by implementing advanced security measures, promoting collaboration, and addressing domain-specific challenges.

The challenges involved in managing cybersecurity risks in emerging technologies on autonomous vehicles are a matter of great concern. Incorporating driving technologies brings about complexities and vulnerabilities that must be addressed to ensure strong cybersecurity.

Technical difficulties in the cybersecurity of vehicles encompass securing communication networks safeguarding data and systems and guaranteeing the reliability and integrity of driving systems (Campbell et al., 2010). Given the nature of vehicles and the potential for cyber-attacks and data breaches, there are substantial risks that call for advanced security measures (Raiyn, 2018). Additionally, it is crucial to co-engineer the safety and security aspects of vehicles to tackle cybersecurity risks effectively (Kavallieratos et al., 2020). Developing models and frameworks for risk assessment is vital in identifying and mitigating vulnerabilities and threats. Collaboration among researchers, industry experts and policymakers play a role in establishing cybersecurity standards and guidelines for autonomous vehicles (Cui et al., 2019). In the context of autonomous vehicles, various applications and domains face specific cybersecurity challenges. For example, the design of autonomous vehicle voice agents (AVVAs) plays a role in enhancing the adoption intention and experience of autonomous vehicles (Lee et al., 2019). Additionally, the communication and networking technologies for autonomous vehicles require reliable and secure communication systems (Zolich et al., 2018). In conclusion, managing cybersecurity risks in emerging technologies, particularly in the context of autonomous vehicles, presents unique challenges. Technical complexities, safety and security co-engineering, and the evolving threat landscape require organisations to adopt comprehensive cybersecurity strategies. Organisations can effectively mitigate cybersecurity risks in autonomous vehicle technologies by implementing advanced security measures, promoting collaboration, and addressing domain-specific challenges. Table 1 provides an overview of the technical challenges faced in managing cybersecurity risks across various emerging technologies.

Table 1 Technical Challenges in Managing Cybersecurity Risks in Emerging Technologies

Emerging Technology	Technical Challenges
Fintech	Protecting sensitive financial data, Ensuring secure transactions, Safeguarding against cyber threats
Power Grids (IoT, Smart Grid)	Securing communication networks, Control systems security, Grid resilience against cyber attacks
IoT	Securing communication networks, Safeguarding control systems, Device resilience against cyber attacks
Cloud Computing	Securing communication networks, Safeguarding data and applications, Privacy and integrity of cloud services
AI and ML	Securing AI models and algorithms, Safeguarding training data, Reliability and integrity of AI systems
Blockchain	Securing communication networks, Protecting data and transactions, Integrity and reliability of Blockchain systems
Autonomous Vehicles	Securing communication networks, Safeguarding data and systems, Reliability and integrity of driving systems

In conclusion, managing cybersecurity risks in emerging technologies involves addressing various technical challenges. These challenges include securing financial technologies, power grids, IoT devices, cloud services, AI and ML technologies, blockchain, and autonomous vehicles. Organisations need to stay updated with the latest cybersecurity practices and technologies to effectively mitigate these technical challenges and protect against evolving cyber threats.

3.2.2 Organisational Challenges

Managing the risks associated with cybersecurity in emerging technologies poses challenges for organisations that need to be addressed. These challenges encompass talent management culture and awareness. One particular administrative challenge when it comes to managing

cybersecurity risks is talent management. The shift towards virtual workplace ecosystems, which has been accelerated by the COVID-19 pandemic has introduced complexities in managing cybersecurity risks (Burrell, 2020). Organisations must comprehend the intricacies involved in overseeing cybersecurity teams. Ensure they possess the requisite talent to tackle emerging threats (Treacy et al., 2023). This involves recruiting and retaining cybersecurity professionals to efficiently manage and mitigate risks associated with emerging technologies (Zwilling, 2022).

Another significant challenge is establishing a culture of cybersecurity within the organisation. Historically, protecting information assets has heavily depended on utilising controls such as hardware and software systems. However, relying on controls is insufficient when combating modern information risk environments. The culture of cybersecurity within an organisation includes individuals, methods, protocols, symbols, technology, training, knowledge, dedication and practical steps taken to maintain cybersecurity (De Silva, 2023). Building a cybersecurity culture entails promoting awareness among employees through training initiatives while fostering a sense of responsibility and commitment to maintaining security measures throughout the organisation.

Moreover, ensuring awareness regarding cybersecurity risks remains crucial. The severity of cyber threats is increasing, which has led managers and policymakers to reevaluate cybersecurity measures at levels such as organisational, sectoral and national (Tsohou et al., 2023). It is crucial for organisations to understand the cyber threats they may face and the impact that data breaches can have on their operations (Naik, 2022). This understanding enables organisations to develop strategies and actions to reduce cybersecurity risks.

To summarise, managing cybersecurity risks in emerging technologies presents challenges for organisations. These challenges encompass talent management, establishing a culture of cybersecurity and fostering organisational awareness regarding cybersecurity risks. Overcoming these challenges involves recruiting and retaining cybersecurity professionals, promoting a cybersecurity culture within the organisation and ensuring that all members are aware of and comprehend the potential risks associated with cybersecurity.

3.2.3 Regulatory Challenges

Ensuring the security of emerging technologies is a task that requires organisations to overcome regulatory obstacles. These challenges encompass the evolving frameworks, compliance obligations and the importance of international collaboration. One of the challenges in addressing cybersecurity risks lies in the nature of regulatory frameworks. As emerging technologies continuously progress, regulatory bodies face the challenge of keeping pace with this changing landscape. Consequently, there may be gaps in regulations and a lack of guidelines for managing cybersecurity risks associated with these technologies (Hadzovic et al., 2023). To ensure compliance and mitigate risks organisations must stay up to date with the regulatory developments and adjust their cybersecurity strategies accordingly.

Compliance requirements also pose challenges when it comes to managing cybersecurity risks. Organisations operating across industries such as finance, healthcare and IoT are subject to compliance standards and regulations. These standards often necessitate implementing cybersecurity measures conducting risk assessments and safeguarding data privacy protection. Meeting these compliance requirements can be complex and resource-intensive as organisations need to allocate resources and expertise to ensure adherence (Jalali & Kaiser, 2018).

Furthermore, international cooperation plays a role in managing cybersecurity risks associated with emerging technologies. Cybersecurity threats are not limited to boundaries. Effectively managing risks requires collaboration and the sharing of information among countries and regulatory bodies (Dacorogna & Kratz, 2023). However, achieving cooperation in the field of

cybersecurity can be challenging due to differences in approaches, legal frameworks and geopolitical factors. Organisations that operate globally must navigate through these complexities.

In Malaysia, the Malaysian Communications and Multimedia Commission (MCMC) is responsible for overseeing cybersecurity regulations. One of the challenges faced by bodies like MCMC is keeping up with the evolving nature of regulatory frameworks. As emerging technologies continue to advance, there is a need for bodies to stay updated with these changes (Perumal et al., 2018). This can sometimes result in gaps in regulations and a lack of guidelines for managing cybersecurity risks associated with these technologies. Organisations operating in Malaysia must navigate through these changing frameworks. Ensure compliance with the regulations to effectively manage cybersecurity risks (Abdalla & Arshad, 2020). In Malaysia, organisations are required to adhere to compliance standards and regulations set by MCMC, such as the Malaysian Personal Data Protection Act (PDPA) and the Malaysian Communications and Multimedia Act (CMA) (Alibeigi & Munir, 2020).

Organisations are required to implement cyber security measures by performing risk assessments protecting data privacy and confidentiality. Meeting these compliance requirements can be resource-intensive, necessitating organisations to allocate resources and expertise for adherence. In Malaysia, it is important for organisations to closely collaborate with MCMC to understand and comply with obligations in order to effectively manage cybersecurity risks. Several research papers discuss the challenges and impact of cybersecurity regulations in Malaysia. Shaukat et al. (2020) delve into the difficulties faced when applying machine learning techniques in the realm of cybersecurity, highlighting the necessity for frameworks to adapt to emerging technologies and address their risks.

To summarise, managing cybersecurity risks in emerging technologies requires navigating through challenges such as evolving frameworks, compliance requirements and their impact on cybersecurity practices. It is crucial for organisations in Malaysia to stay updated on developments, ensure compliance with MCMC regulations and prioritise cybersecurity measures for effective risk management.

4. EXISTING RISK MANAGEMENT

Effective risk management is a component for any organisation as it encompasses the tasks of recognising, evaluating and minimising potential risks that may hinder the accomplishment of goals. By implementing risk management practices, organisations can proactively identify and address potential threats that may arise within various areas of their operations, such as financial, operational, and reputational risks. Through the systematic application of management policies, procedures, and practices, organisations can effectively manage risk and ensure their survival.

4.1 Best Practices in Existing Risk Management Strategies for Cybersecurity

In the realm of technology effectively addressing the challenges posed by cybersecurity demands an approach. In studies researchers have identified nine approaches that can be used to effectively handle and address existing risks. An essential aspect of this approach involves identifying and evaluating risks, often utilising established frameworks, like the NIST Cybersecurity Framework or ISO standards. These frameworks provide a method for assessing cybersecurity threats and prioritising risk mitigation (Rea-Guaman et al., 2020).

Another crucial element is the implementation of Multi-Factor Authentication (MFA), which enhances security by demanding forms of verification. This becomes especially significant for access accounts where the possibility of access exists. MFA has evolved from single-factor

authentication (SFA) to two-factor authentication (2FA). It now includes sensors and providers that help authenticate users (Ometov et al., 2018). The increasing utilisation of MFA is motivated by the desire for dependable authentication when using various services. Common IoT cybersecurity technologies, including MFA, play a vital role in ensuring the confidentiality of information, detecting and countering online threats and vulnerabilities, and managing credentials. The implementation of MFA and other cybersecurity technologies is essential for protecting against cybercrime and ensuring secure interactions in emerging technologies (Kanu et al., 2022).

The third approach involves updating and managing software patches, which is crucial when combined with MFA. Automated updates and patching can significantly decrease the chances of cyberattacks (Ansari et al., 2022). Upgrading software plays a role in reducing cybersecurity risks by addressing vulnerabilities and enhancing system security. Algarni et al. (2021) stress the importance of updating software to ensure that known vulnerabilities are fixed and protected against cyberattacks. They emphasise the need for organisations to prioritise and implement software upgrades based on the criticality of vulnerabilities and their potential impact on the system adopting a risk-based approach. Patch management is another aspect of cybersecurity risk management. Dissanayake et al. (2020) conducted a review of the literature on software security patch management identifying challenges, approaches, tools and practices. They emphasise the importance of having a comprehensive patch management process that includes vulnerability scanning, assessment, prioritisation, and timely deployment of patches. The review also highlights the need for effective tools and practices to address the challenges associated with patch management. Yaacoub et al. (2021) discuss the cybersecurity considerations for robotic surgery, emphasising the importance of regular software updates to address vulnerabilities and enhance the security of the system. They recommend following cybersecurity best practices, investing in regular software updates, and increasing transparency to ensure the overall safety and security of robotic surgery systems.

The fourth method is to offer training and awareness programmes to employees as human mistakes continue to be a factor in cybersecurity breaches. Consequently, ongoing education and simulated tests like phishing attack simulations can greatly enhance an organisation's cybersecurity stance.

The fifth approach involves implementing data encryption, which's a practice for safeguarding sensitive information particularly when it is being transmitted or stored. Data encryption acts as a measure against unauthorised access to sensitive data. Eichelberg and Kleber (2020) underscore the significance of employing encryption techniques in Picture Archiving and Communication Systems (PACS) and medical imaging. They emphasise the use of encryption methods to ensure the confidentiality and integrity of data during transmission and storage. They also highlight the importance of data encryption as part of cybersecurity practices. Encryption plays a role in safeguarding data from access even if it is intercepted or stolen. It is recommended to implement encryption measures for sensitive data at rest, in transit, and in use. Implementing data encryption requires the use of robust encryption algorithms and secure key management practices. Organisations should adopt industry-standard encryption protocols and ensure the proper implementation and configuration of encryption mechanisms.

The sixth factor that can significantly assist in resolving a cybersecurity incident is having a well-developed and regularly updated incident response plan in place. It can help prevent a minor disruption from turning into a major catastrophe. To ensure its effectiveness, the plan should be tested periodically, and staff should be familiarised with the procedures to be followed during an actual incident. Effective incident response is crucial in minimising the impact of a cybersecurity incident. Burrell (2020) highlights the role of incident response teams in handling incidents, conducting intrusion evaluations, crisis management, and forensic data examinations. These teams play a vital role in containing and mitigating the incident promptly. The use of incident

management frameworks is essential in guiding organisations through the process of resolving a cybersecurity incident. Walker-Roberts et al. (2019) emphasise the importance of understanding security threats in the era of cyber-physical systems. They emphasise the importance of incident management frameworks, in tackling the risks linked to cybersecurity incidents. The involvement of factors is crucial when it comes to addressing cybersecurity incidents. Walker-Roberts et al. Walker-Roberts et al. (2019) highlight the extensive internal security breaches resulting from human error. This emphasises the need for a reevaluation of cybersecurity principles and the importance of training and awareness programmes to address human factors in incident resolution.

Continuous monitoring and regular audits play a role in the evaluation of cybersecurity measures within a company. They offer insights into the effectiveness of these measures. Help identify areas that require improvement. Regular audits are vital for assessing the efficiency of cybersecurity controls and pinpointing vulnerabilities or weaknesses in the system. In their research, Islam et al. (2018) emphasise the importance of audit functions in conducting security and cybersecurity audits. The study underscores the necessity for audit teams to have the required knowledge and expertise to thoroughly evaluate cybersecurity risks and controls. Continuous monitoring involves the real-time monitoring of systems, networks, and data to detect and respond to cybersecurity incidents promptly. Malatji et al. (2019) emphasise the importance of continuous monitoring in the context of a socio-technical systems cybersecurity framework. The study highlights the need for organisations to continuously monitor their cybersecurity practices to ensure the alignment of social, technical, and environmental dimensions.

The eighth aspect of cybersecurity that is often overlooked is vendor risk management. Organisations must evaluate third-party vendor cybersecurity measures and insist on contractual terms requiring adherence to set cybersecurity standards. Numerous companies depend on vendors to provide a range of services, which may involve granting them access to information. It is essential to assess and manage the cybersecurity risks associated with these third parties to ensure the protection of data.

Lastly, it is crucial for organisations to adhere to regulatory requirements, not only because it's a legal obligation but also because it provides a framework for establishing robust cybersecurity measures. Ensuring compliance with these requirements is a process that necessitates monitoring and improvement. Organisations should implement mechanisms to monitor their compliance status, such as conducting audits and assessments. This helps identify any deviations or non-compliance enabling organisations to promptly take action. Moreover, staying abreast of changes in laws, regulations and industry standards is vital to ensure compliance. By incorporating these nine practices into their cybersecurity risk management strategies, organisations can confidently navigate the realm of emerging technologies while maintaining a higher level of security assurance.

4.2 Case Study in Existing Risk Management Strategies for Cybersecurity

The practical application of risk management strategies in emerging technologies is best understood through real-world case studies. These case studies not only provide insights into effective strategies but also offer invaluable lessons learned for organisations looking to enhance their cybersecurity posture.

Ng and Kwok (2017) conducted a case study on the emergence of Fintech and cybersecurity in Hong Kong as a global financial centre. The study focused on the regulatory environment and the formulation and implementation of complementary regulatory policies by the Hong Kong Monetary Authority (HKMA), the financial regulator of Hong Kong. The authors found that the HKMA adopted a risk-based approach to address the opportunities and risks associated with Fintech. They highlighted the significance of creating a cybersecurity profession that

encompasses expertise in auditing, management controls, risk management and information technology. This is crucial for addressing evolving cyber threats in a financial hub (Ng & Kwok, 2017).

The case study by Raimundo and Rosário (2022) focuses on the cybersecurity challenges in the IIoT. The study reviews key articles to analyse the opportunities and threats associated with IIoT cybersecurity. After conducting an analysis of the literature, the authors have identified a significant gap in the current efficacy of IoT cyber risk solutions. This clearly indicates that there is scope for enhancing the ability to address the cybersecurity risks associated with IIoT. The case study serves as a reminder of the necessity for research and development aiming to bolster the effectiveness of cybersecurity measures, within the realm of IIoT. By addressing this gap, organisations can better protect their industrial systems and infrastructure from cyber threats in the emerging technology landscape.

5. GAPS IN CURRENT RESEARCH AND PRACTICE

Emerging technologies are advancing rapidly and have brought about significant changes in various industries. However, they also come with new cybersecurity risks and challenges. Although much progress has been made in understanding the implications of cybersecurity in emerging technologies, several critical questions remain unanswered, which require further scholarly investigation. This paper aims to identify and discuss the gaps in current research and practice in managing cybersecurity risks in emerging technologies.

Robust frameworks are necessary for cost-benefit analysis to manage cybersecurity risks in emerging technologies. However, there is a scarcity of specific references that tackle this topic. Therefore, I will give a general overview of cost-benefit analysis frameworks along with their limitations. Cost-benefit analysis refers to the process of evaluating the costs and benefits associated with a particular decision or investment. It helps organisations assess the economic feasibility and potential returns of cybersecurity initiatives. While there is a wealth of literature discussing cost-benefit analysis in fields of its application, cybersecurity is still a developing area. One limitation of existing cost-benefit analysis frameworks is the lack of methodologies specifically tailored for cybersecurity. Many studies focus on identifying and quantifying the costs and benefits associated with cybersecurity measures. There is a need for frameworks that take into account the unique characteristics and challenges posed by emerging technologies. To overcome these limitations, future research should concentrate on establishing frameworks and methodologies for conducting cost-benefit analyses in the context of cybersecurity. This involves creating metrics to measure the costs and benefits of cybersecurity measures as well as incorporating dynamic and evolving factors into the analysis. Moreover, efforts should be made to enhance data collection and sharing in order to improve the accuracy of cost-benefit analyses. Although there may not be references addressing the gaps in cost-benefit analysis frameworks for cybersecurity in emerging technologies, the provided references offer insights into cost-benefit analysis methodologies across various domains.

Despite the progress made in cybersecurity technology, we must not overlook the factor which remains an ever-present and often underestimated variable in the cybersecurity equation. With security systems, it is human error that continues to be a significant cause of security breaches. These errors can range from slip-ups like using passwords to more complex issues such as falling prey to phishing attacks. Therefore, it is crucial to develop an understanding of the aspects that contribute to cybersecurity vulnerabilities. Human error's impact on cybersecurity extends beyond mistakes. Permeates broader organisational and cultural contexts. For instance, an organisation's cybersecurity culture plays a role in shaping employee behaviour. In environments where cybersecurity is not given priority employees are more prone to engaging in actions like using networks or sharing sensitive information without proper authorisation. Furthermore, the

problem of error goes beyond employees and includes third-party vendors, contractors and other external stakeholders who interact with an organisation's information systems. The absence of training programmes for these entities can further amplify the risks associated with human error.

Given these complexities organisations must adopt a faceted approach to mitigate the risks stemming from human error. This approach entails not only solutions but also comprehensive training programmes designed to enhance employees' awareness of cybersecurity. Organisations should customise these programmes to tackle the risks linked to their operations. It is crucial to update them so they stay in sync with the changing cybersecurity landscape. Conducting simulated cyber-attack exercises, like phishing simulations can be highly beneficial in training employees to identify and effectively respond to threats.

In conclusion, while technology will continue to play a critical role in enhancing cybersecurity, addressing the human element is equally important. A more nuanced understanding of the role of human error in cybersecurity incidents, informed by empirical research, can significantly contribute to the development of more effective risk mitigation strategies.

6. CONCLUSION

Managing cybersecurity risks in emerging technologies presents an ever-changing challenge for organisations. The current state of cybersecurity in these technologies highlights the importance of risk management strategies. There are hurdles that organisations face when dealing with these risks, including organisational and regulatory obstacles. Technical issues primarily focus on the security of communication networks, protecting data and systems as ensuring the dependability and trustworthiness of emerging technologies. Dealing with cybersecurity challenges posed by emerging technologies can be quite challenging for organisations. One major aspect is training and equipping the workforce with the right strategies to handle these challenges. Moreover, regulatory challenges come into play due to compliance requirements in a global context with diverse cybersecurity laws. To effectively manage risks associated with cybersecurity in emerging technologies, organisations can utilise established risk management practices such as systematic identification and assessment of risks.

However, there are gaps in existing research and practices that need attention. These gaps include the lack of frameworks for conducting cost-benefit analyses, knowledge about the role of human error in cybersecurity incidents and a need for comprehensive strategies to tackle the ever-evolving landscape of cybersecurity threats. Bridging these gaps requires investigation involving the development of standardised frameworks for cost-benefit analyses, understanding human factors involved in cybersecurity incidents better and devising effective strategies for training and preparing the workforce. Furthermore, it is essential to acknowledge the changing nature of compliance and delve into the difficulties surrounding interoperability in emerging technologies. These aspects warrant research efforts. By focusing on bridging gaps and implementing robust risk management strategies, organisations can bolster their cybersecurity measures to effectively address risks within the evolving realm of emerging technologies.

REFERENCES

Abdalla, M., & Arshad, Y. B. (2020). Information Security: Cybersecurity Standards Adoption Among Malaysian Public Listed Companies. *International Journal of Engineering Research and Technology*, *9*(8). https://doi.org/10.17577/IJERTV9IS080133

Abeysekera, M. C., & Kumarawadu, P. (2022). Analysis of Factors Influencing Blockchain Implementation in Finance Sector in Sri Lanka. *Ho Chi Minh City Open University Journal of Science - Economics and Business Administration*, *12*(2), 3-14. https://doi.org/10.46223/hcmcoujs.econ.en.12.2.2236.2022

Algarni, A., Thayananthan, V., & Malaiya, Y. K. (2021). Quantitative Assessment of Cybersecurity Risks for Mitigating Data Breaches in Business Systems. *Applied Sciences*, *11*(8), 3678. https://doi.org/10.3390/app11083678

Alibeigi, A., & Munir, A. B. B. (2020). Malaysian Personal Data Protection Act, a Mysterious Application. *University of Bologna Law Review*, *5*(2), 362-374. https://doi.org/10.6092/ISSN.2531-6133/12441

Aljumah, A. A., & Ahanger, T. A. (2020). Cyber Security Threats, Challenges and Defence Mechanisms in Cloud Computing. *IET Commun.*, *14*(7), 1185-1191. https://doi.org/10.1049/iet-com.2019.0040

Ansari, M. M., Sharma, P. K., & Dash, B. (2022). Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training. *International Journal of Smart Sensor and Adhoc Network.*, *3*(3), 61-72. https://doi.org/10.47893/IJSSAN.2022.1221

Burrell, D. N. (2020). Understanding the Talent Management Intricacies of Remote Cybersecurity Teams in COVID-19 Induced Telework Organisational Ecosystems. *Land Forces Academy Review*, *25*(3), 232 - 244. https://doi.org/10.2478/raft-2020-0028

Campbell, M., Egerstedt, M., How, J. P., & Murray, R. M. (2010). Autonomous Driving in Urban Environments: Approaches, Lessons and Challenges. *Philosophical Transactions of the Royal Society a Mathematical Physical and Engineering Sciences*, *368*(1928), 4649-4672. https://doi.org/10.1098/rsta.2010.0110

Canelon, J., Huerta, E., Incera, J., & Ryan, T. (2019). A Cybersecurity Control Framework for Blockchain Ecosystems. *The International Journal of Digital Accounting Research*, *19*, 103-144. https://doi.org/10.4192/1577-8517-v19_5

Cui, J., Sabaliauskaite, G., Liew, L. S., Zhou, F., & Zhang, B. (2019). Collaborative Analysis Framework of Safety and Security for Autonomous Vehicles. *IEEE Access*, *7*, 148672-148683. https://doi.org/10.1109/ACCESS.2019.2946632

Dacorogna, M. M., & Kratz, M. (2023). Managing Cyber Risk, a Science in the Making. *ArXiv*, *2023*(10), 1000-1021. https://doi.org/10.1080/03461238.2023.2191869

De Silva, B. (2023). Exploring the Relationship Between Cybersecurity Culture and Cyber-Crime Prevention: A Systematic Review. *International Journal of Information Security and Cybercrime*, *12*(1), 23-29. https://doi.org/10.19107/IJISC.2023.01.03

Ding, Y., Li, K., Liu, C., Tang, Z., & Li, K. (2021). Short- and Long-term Cost and Performance Optimisation for Mobile User Equipments. *Journal of Parallel and Distributed Computing*, *150*, 69-84. https://doi.org/10.1016/j.jpdc.2020.12.006

Dissanayake, N., Jayatilaka, A., Zahedi, M., & Babar, M. E. (2020). Software Security Patch Management: A Systematic Literature Review of Challenges, Approaches, Tools and Practices. *Information and Software Technology*, *144*, 106171. https://doi.org/10.1016/j.infsof.2021.106771

Eichelberg, M., & Kleber, K. (2020). Cybersecurity in PACS and Medical Imaging: An Overview. *Journal of Digital Imaging*, *33*, 1527–1542. https://doi.org/10.1007/s10278-020-00393-3

Fouad, N. S. (2021). Securing Higher Education Against Cyberthreats: From an Institutional Risk to a National Policy Challenge. *Journal of Cyber Policy*, *6*(2), 137-154. https://doi.org/10.1080/23738871.2021.1973526

Geluvaraj, B., Satwik, P. M., & Kumar, T. A. A. (2018). The Future of Cybersecurity: Major Role of Artificial Intelligence, Machine Learning, and Deep Learning in Cyberspace. *International Conference on Computer Networks and Communication Technologies*, *15*, 739-747. https://doi.org/10.1007/978-981-10-8681-6_67

Goldblum, M., Tsipras, D., Xie, C., Chen, X., Schwarzschild, A., Song, D. X., Madry, A., Li, B., & Goldstein, T. (2020). Dataset Security for Machine Learning: Data Poisoning, Backdoor Attacks, and Defenses. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *45*, 1563-1580. https://doi.org/10.48550/arXiv.2012.10544

Hadzovic, S., Mrdović, S., & Radonjić, M. (2023). A Path Towards an Internet of Things and Artificial Intelligence Regulatory Framework. *IEEE Communications Magazine*, *61*, 90-96. https://doi.org/10.1109/MCOM.002.2200373

Harshith, J., Gill, M. S., & Jothimani, M. (2023). Evaluating the Vulnerabilities in ML systems in terms of adversarial attacks. *ArXiv*, *2308.12918*, 1-14. https://doi.org/10.48550/arXiv.2308.12918

Hireche, R., Mansouri, H., & Pathan, A.-S. K. (2022). Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis. *Journal of Cybersecurity and Privacy*, *2*(3), 640-661. https://doi.org/10.3390/jcp2030033

Islam, M. S., Farah, N., & Stafford, T. W. (2018). Factors Associated With Security/Cybersecurity Audit by Internal Audit Function. *Managerial Auditing Journal*, *33*(4), 377-409. https://doi.org/10.1108/maj-07-2017-1595

Jalali, M. S., & Kaiser, J. (2018). Cybersecurity in Hospitals: A Systematic, Organisational Perspective. *Journal of Medical Internet Research*, *20*(5), e10059. https://doi.org/10.2196/10059

Kaja, D. V. S., Fatima, Y., & Mailewa, A. B. (2022). Data Integrity Attacks in Cloud Computing: A Review of Identifying and Protecting Techniques. *International Journal of Research Publication and Reviews*, *3*(2), 713-720. https://doi.org/10.55248/gengpi.2022.3.2.8

Kanu, V. P. S., Naiem, Y. A., & Prasad, S. S. (2022). A Research of Cybersecurity and Threats in Emerging Technologies. *International Journal for Research in Applied Science and Engineering Technology*, *10*(4), 2935 - 2938. https://doi.org/10.22214/ijraset.2022.41858

Kavallieratos, G., Katsikas, S. K., & Gkioulos, V. (2020). Cybersecurity and Safety Co-Engineering of Cyberphysical Systems: A Comprehensive Survey. *Future Internet*, *12*(4), 65. https://doi.org/10.3390/fi12040065

Khader, M., Karam, M. R., & Fares, H. (2021). Cybersecurity Awareness Framework for Academia. *Inf.*, *12*(10), 417. https://doi.org/10.3390/info12100417

Khurshid, A., Alsaaidi, R., Aslam, M., & Raza, S. (2022). EU Cybersecurity Act and IoT Certification: Landscape, Perspective and a Proposed Template Scheme. *IEEE Access*, *10*, 129932-129948. https://doi.org/10.1109/ACCESS.2022.3225973

Kumar, N., & Kumar, S. (2021). Conceptual Service Level Agreement Mechanism to Minimise the SLA Violation with SLA Negotiation Process in Cloud Computing Environment.

Kushwaha, S. S., Joshi, S., Singh, D., Kaur, M., & Lee, H.-N. (2022). Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract. *IEEE Access*, *10*, 6605 - 6621. https://doi.org/10.1109/ACCESS.2021.3140091

Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet*, *12*(9), 157. https://doi.org/10.3390/fi12090157

Lee, S. U., Ratan, R. A., & Park, T. (2019). The Voice Makes the Car: Enhancing Autonomous Vehicle Perceptions and Adoption Intention Through Voice Agent Gender and Style. *Multimodal Technologies and Interaction*, *3*(1), 20. https://doi.org/10.3390/mti3010020

Li, L., Li, Y., Liu, Z., Zeng, Y., Ding, G., & Zhang, Q. (2022). Identification of Vulnerable Node Groups in Wind Power Grids Based on K-Order Structure Entropy. *Journal of Physics Conference Series*, *2369*(1), 012064. https://doi.org/10.1088/1742-6596/2369/1/012064

Li, S., Chen, M., Chen, Y., Cao, L., Liu, Y., & Sun, Y. (2023). Research on Security Assessment and Control Technology for Power Mobile Terminal. *International Conference on Computer Application and Information Security (ICCAIS 2022) 12609*, 232-239. https://doi.org/10.1117/12.2671955

Maidamwar, P., & Chavhan, N. A. (2020). Blockchain Technology: A Review On Architecture, Security Issues And Challenges. *International Journal of Engineering Applied Sciences and Technology, 4*(12), 245-249.https://doi.org/10.33564/ijeast.2020.v04i12.039

Malatji, M., Solms, S. V., & Marnewick, A. (2019). Socio-Technical Systems Cybersecurity Framework. *Information and Computer Security*, *27*(2), 233-272. https://doi.org/10.1108/ics-03-2018-0031

Matheu, S. N., Hernández-Ramos, J. L., Skarmeta, A. F., & Baldini, G. (2020). A Survey of Cybersecurity Certification for the Internet of Things. *ACM Computing Surveys (CSUR)*, *53*(6), 1 - 36. https://doi.org/10.1145/3410160

Morol, M. K. (2022). Data Security and Privacy in Cloud Computing Platforms: A Comprehensive Review. *International Journal of Current Science Research and Review*, *5*(5), 1453-1463. https://doi.org/10.47191/ijcsrr/v5-i5-09

Naik, L. B. (2022). Cyber Security Challenges and Its Emerging Trends on Latest Technologies. *International Journal of Scientific Research in Engineering and Management*, *6*(6). https://doi.org/10.55041/IJSREM14488

Ng, A. W., & Kwok, B. K. B. (2017). Emergence of Fintech and Cybersecurity in a Global Financial Centre. *Journal of Financial Regulation and Compliance*, *25*(4), 422-434. https://doi.org/10.1108/jfrc-01-2017-0013

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. *Cryptography*, *2*(1), 1. https://doi.org/10.3390/cryptography2010001

Oubelaid, A. (2023). Staying Ahead of Threats: A Review of AI and Cyber Security in Power Generation and Distribution. *International Journal of Electrical and Electronics Research*, *11*(1), 143-147. https://doi.org/10.37391/ijeer.110120

Parizi, R. M., Dehghantanha, A., Azmoodeh, A., & Choo, K. K. R. (2020). Blockchain in Cybersecurity Realm: An Overview. Blockchain Cybersecurity, Trust and Privacy, *79*, 1-5. https://doi.org/10.1007/978-3-030-38181-3_1

Paul, P., Aremu, S. B., Aithal, P. S., Saavedra, R., & Sinha, R. R. S. R. R. (2020). A Study on Cloud Computing and Service Market: International Context With Reference to India. *Asian Journal of Managerial Science*, *9*(1), 52-56. https://doi.org/10.51983/ajms-2020.9.1.1629

Perumal, S., Pitchay, S. A., Samy, G. N., Shanmugam, B., Magalingam, P., & Albakri, S. H. (2018). Transformative Cyber Security Model for Malaysian Government Agencies. *International Journal of Engineering & Technology*, *7*(4.15), 87-92. https://doi.org/10.14419/IJET.V7I4.15.21377

Qiu, R., Xue, X., Chen, M., Zheng, J., Jing, S., & Li, Y. (2022). A Fine-Grained Dynamic Access Control Method for Power IoT Based on Kformer. *Infocommunications Journal*, *14*(4), 79-85. https://doi.org/10.36244/icj.2022.4.11

Radoglou-Grammatikis, P., Sarigiannidis, P., Iturbe, E., Rios, E., Martinez, S., Sarigiannidis, A., Eftathopoulos, G., Spyridis, Y., Sesis, A., Vakakis, N., Tzovaras, D., Kafetzakis, E., Giannoulakis, I., Tzifas, M., Giannakoulias, A., Angelopoulos, M., & Ramos, F. (2021). SPEAR SIEM: A Security Information and Event Management system for the Smart Grid. *Computer Networks*, *193*, 108008. https://doi.org/10.1016/j.comnet.2021.108008

Raimundo, R. J., & Rosário, A. T. (2022). Cybersecurity in the Internet of Things in Industrial Management. *Applied Sciences*, *12*(3), 1598. https://doi.org/10.3390/app12031598

Raiyn, J. (2018). Data and Cyber Security in Autonomous Vehicle Networks. *Transport and Telecommunication Journal*, *19*, 325 - 334. https://doi.org/10.2478/ttj-2018-0027

Rea-Guaman, A. M., Mejía, J., San Feliu, T., & Calvo-Manzano, J. A. (2020). AVARCIBER: A framework for assessing cybersecurity risks. *Cluster Computing*, *23*, 1827-1843. https://doi.org/10.1007/s10586-019-03034-9

Rimal, B. P., Kong, C., Poudel, B., Wang, Y., & Shahi, P. (2022). Smart Electric Vehicle Charging in the Era of Internet of Vehicles, Emerging Trends, and Open Issues. *Energies*, *15*(5), 1908. https://doi.org/10.3390/en15051908

Sakhnini, J., Dehghantanha, A., Parizi, R. M., & Srivastava, G. (2021). Security Aspects of Internet of Things Aided Smart Grids: A Bibliometric Survey. *Internet of Things*, *14*, 100111. https://doi.org/10.1016/j.iot.2019.100111

Salek, M. S., Khan, S. M., Rahman, M. M., Deng, H.-W., Islam, M., Khan, Z., Chowdhury, M., & Shue, M. (2022). A Review on Cybersecurity of Cloud Computing for Supporting Connected Vehicle Applications. *Ieee Internet of Things Journal*, *9*(11), 8250-8268. https://doi.org/10.1109/jiot.2022.3152477

Sharma, R., & Sharma, N. (2022). Attacks on Resource-Constrained IoT Devices and Security Solutions. *Int. J. Softw. Sci. Comput. Intell.*, *14*, 1-21. https://doi.org/10.4018/IJSSCI.310943

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., Chen, S., Liu, D., & Li, J.-M. (2020). Performance Comparison and Current Challenges of Using Machine Learning Techniques in Cybersecurity. *Energies*, *13*(10), 2509. https://doi.org/10.3390/en13102509

Taeihagh, A., Ramesh, M., & Howlett, M. (2021). Assessing the Regulatory Challenges of Emerging Disruptive Technologies. *Decision-Making in Public Policy & the Social Good eJournal*, *15*(4), 1009-1019. https://doi.org/10.1111/rego.12392

Tawalbeh, L. a. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and Security: Challenges and Solutions. *Applied Sciences*, *10*, 4102. https://doi.org/10.3390/app10124102

Treacy, S., Sabu, A., Bond, T., O'Sullivan, J., Sullivan, J., & Sylvester, P. (2023). Organizational Cybersecurity Post The Pandemic: An Exploration of Remote Working Risks and Mitigation Strategies. *International Conference on Cyber Warfare and Security*, *18*(1). https://doi.org/10.34190/iccws.18.1.973

Tsohou, A., Diamantopoulou, V., Gritzalis, S., & Lambrinoudakis, C. (2023). Cyber Insurance: State of the Art, Trends and Future Directions. *International Journal of Information Security*, *22*(3), 737-748. https://doi.org/10.1007/s10207-023-00660-8

Walker-Roberts, S., Hammoudeh, M., Aldabbas, O., Aydin, M. E., & Dehghantanha, A. (2019). Threats on the Horizon: Understanding Security Threats in the Era of Cyber-Physical Systems. *The Journal of Supercomputing*, *76*(1), 2643–2664 https://doi.org/10.1007/s11227-019-03028-9

Yaacoub, J.-P. A., Noura, H. N., Salman, O., & Chehab, A. (2021). Robotics Cyber Security: Vulnerabilities, Attacks, Countermeasures, and Recommendations. *International Journal of Information Security*, *21*, 115 - 158. https://doi.org/10.1007/s10207-021-00545-8

Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A Survey on Cyber Security for Smart Grid Communications. *IEEE Communications Surveys & Tutorials*, *14*(4), 998-1010. https://doi.org/10.1109/surv.2012.010912.00035

Zamani, E. D., He, Y., & Phillips, M. (2018). On the Security Risks of the Blockchain. *Journal of Computer Information Systems*, *60*(6), 495-506. https://doi.org/10.1080/08874417.2018.1538709

Zolich, A., Palma, D., Kansanen, K., Fjørtoft, K. E., Sousa, J. M. C., Johansson, K. H., Jiang, Y., Dong, H., & Johansen, T. A. (2018). Survey on Communication and Networks for Autonomous Marine Systems. *Journal of Intelligent & Robotic Systems*, *95*, 789–813. https://doi.org/10.1007/s10846-018-0833-5

Zwilling, M. (2022). Trends and Challenges Regarding Cyber Risk Mitigation by CISOs: A Systematic Literature and Experts' Opinion Review Based on Text Analytics. *Sustainability*, *14*(3), 1311. https://doi.org/10.3390/su14031311