e-ISSN: 2320-4230, p-ISSN: 2961-6085

Journal of Drug Discovery and Therapeutics

Available Online at www.jddt.in

CODEN: - JDDTBP (Source: - American Chemical Society)

Volume 13, Issue 4; 2025, 66-85

Managing responsibility for cybersecurity risks in new technologies

Sourabh Singh, Sanjeev Kumar Sharma

Department of CSE, Sunrise University, Alwar, Rajasthan

Received: 11-04-2025 / Revised: 10-05-2025 / Accepted: 23-06-2025

Corresponding author: Sourabh Singh

Conflict of interest: No conflict of interest.

Abstract:

In modern times, it is essential for companies to effectively manage cyber security threats linked to emerging technology. This article offers a comprehensive overview of cybersecurity across several technologies. It illustrates the difficulties that organizations have while addressing these risks. The field of cybersecurity has challenges that must be addressed. Technical challenges include the protection of communication networks and the defence of data and systems against intruders. Moreover, it is important to ensure the trustworthiness and credibility of emerging technologies. Organizational challenges include the preparation and training of personnel, with the development of effective strategies to address the unique cybersecurity issues associated with evolving technologies. Regulatory challenges arise from changing compliance mandates in a global environment marked by diverse cybersecurity laws across countries. To effectively manage cyber security risks, it is crucial to follow established risk management standards, including the systematic identification and evaluation of threats. However, there are shortcomings in research and practices that need improvement. The highlighted inadequacies include the lack of frameworks for conducting cost-benefit analyses, a limited understanding of the impact of mistakes in cybersecurity incidents, and the need for comprehensive strategies to tackle the constantly evolving landscape of cybersecurity threats. Addressing these deficiencies requires study and the development of viable solutions to improve cybersecurity in emerging technologies.

Keywords: Cyber security Risks, Risk Management Strategies, Technical Challenges

Introduction

In the contemporary digital environment, emerging technologies such as Artificial Intelligence (AI), autonomous vehicles, the Internet of Things (IoT), Machine Learning (ML), blockchain, and Cloud Computing are transforming diverse sectors, including healthcare, finance, manufacturing, and education. Although technology presents opportunity for innovation and efficiency, organizations must also adeptly handle emerging cyber security concerns. Incorporating new technologies into current infrastructures not only broadens the attack surface but also presents distinct vulnerabilities that conventional cyber security solutions may inadequately mitigate. The decentralized structure of blockchain technology, whilst providing improved security in some aspects, also presents issues to data integrity and system compatibility.

Likewise, the Internet of Things (IoT), with its multitude of interconnected gadgets, poses issues of data privacy, unauthorized access, and the possible exploitation of sensitive information. Furthermore, the human factor continues to be a crucial ingredient in the cyber security equation. Notwithstanding significant technological breakthroughs, security breaches continue to transpire often. This often occurs due to human errors, which may be ascribed to insufficient awareness or training. Furthermore, organizations have difficulties stemming from compliance concerns when legislation fails to keep pace with technological progress. The intricacy of cyber security is exacerbated by technological use, requiring a holistic strategy that encompasses technical, organizational, human, and legal dimensions.

In this context, it is essential to formulate a comprehensive strategy to adeptly address the cyber security concerns associated with the advent of new technologies. Organizations should not only depend on risk management techniques. It must also provide a comprehensive framework that addresses the distinct problems posed by these technologies. This article will examine the management of cyber security risks in developing technologies.

Research Objectives

This study aims to evaluate the approaches used to manage cyber security threats in developing technology. The research aims to examine the present condition of cyber security in emerging technologies, together with the associated challenges and consequences for organizations and stakeholders.

- To ascertain the technological, organizational, and regulatory obstacles encountered in the management of cyber security risks associated with developing technologies.
- To analyze the current risk management techniques and frameworks used to mitigate cyber security risks associated with new technologies

Literature Review

The proficient management of cyber security risks is crucial for organizations across several sectors, particularly in relation to developing technology. The evolving technological environment has offered organizations benefits and opportunities. This encompasses innovations such as artificial intelligence, machine learning, the Internet of Things, blockchain technology, and cloud computing. These innovations possess the capacity to enhance efficiency, production, and creativity. The use of modern technology also presents intricate cyber security threats that need proper management. A literature assessment was performed to evaluate the existing body of work on addressing cyber security risks in emerging technologies. The findings indicated that new technologies might improve cyber security and resilience for organizations; nevertheless, issues may arise during their implementation. (Li et al., 2022).

Current State of Cyber security in Emerging Technologies

The reliance of organizations on emerging technology underscores the significance of cyber security for innovation and efficiency. Emerging technologies such as IoT, AI, and cloud computing have introduced novel cyber security threats. Organizations must comprehend these threats and execute plans to safeguard their systems, data, and operations.

Lee (2020) presents a four-layer structure for the management of cyber hazards in the Internet of Things (IoT). Suggests use

programming to distribute financial resources among various cyber security initiatives inside this framework. The article highlights a deficiency in current cyber security frameworks, particularly with the allocation of resources for cyber security projects. Although frameworks such as the National Institute of Standards and Technology (NIST) Cyber security Framework provide valuable insights for risk assessment and mitigation, they do not give direction for doing cost-benefit evaluations or for establishing informed implementation priorities. This ambiguity often compels organizations to depend on intuition instead of concrete evidence when distributing resources for cyber security initiatives.

In 2021, Fouad analyzes the security and privacy concerns associated with blockchain technology. The authors examine the weaknesses and threats that threaten the security of blockchain systems and recommend solutions to bolster the security and privacy of blockchain-based applications. Ding et al. (2021) examine the security concerns and solutions associated with edge computing. The authors examine the distinct security vulnerabilities linked to edge computing and provide many security procedures and protocols to safeguard edge devices and data.

Emerging technologies, such as Fintech, IoT, and Smart Grid, provide ambiguity and difficulties in problem delineation and regulatory jurisdiction. The characteristics of these technologies expand the variety and extent of assets susceptible to cyber-attacks, resulting in a greater number of regulating entities asserting authority over cyber security matters. The ambiguity around issue characterization and regulatory jurisdiction has prompted lawmakers to seek support from federal officials to mitigate their uncertainties (Taeihagh et al., 2021). To address cyber security concerns presented by evolving technologies, Security Information and Event Management (SIEM) systems provide a viable solution. SIEM systems can detect, standardize, and create correlations among security issues. This makes them very important for the protection of ecosystems such as the Smart Grid (Radoglou-Grammatikis et al., 2021).

Moreover, Raimundo and Rosário (2022) have investigated cyber security in the context of the Industrial Internet of Things (IIoT). They highlight subjects like as machine learning and cloud computing, which are often used to address security challenges in IIoT. In the same year, Hireche et al. (2022) did research focusing on the security concerns and solutions associated with the Internet of Medical Things (IoMT). They analyze diverse security concerns and provide strategies to protect sensitive medical information inside IoMT systems.

These literature evaluations provide significant insights into the present condition of cyber security in developing technologies. They emphasize the problems and vulnerabilities inherent in these technologies and provide solutions and tactics to alleviate cyber security threats. By comprehending these concerns and enacting suitable security procedures, organizations may safeguard their systems and data from cyber assaults.

Challenges in Managing Risks in Emerging Technologies

In the rapidly evolving technological landscape, organizations are increasingly focused on mitigating cyber security risks associated with new technologies. The issues include technological, organizational, and regulatory aspects with substantial interrelations. Technological innovations, like IoT, AI, and cloud computing, are undeniably transformational. Nonetheless, they introduce new risks that need attention.

Recent instances have shown the need for organizations to proactively secure devices and protect data to mitigate dangers linked to developing technology. Ongoing surveillance and prompt threat intelligence are essential because of the evolving nature of these technologies.

Organizations must urgently address the shortage of competent cyber security experts capable of adapting to the evolving situation. In addition to recruitment, organizations must cultivate an omnipresent culture of cyber security. This entails the implementation of comprehensive training programs, awareness campaigns, and fostering a communal feeling of responsibility for cyber resilience.

Regulatory concerns provide a distinct difficulty. As technology progresses swiftly, regulatory frameworks fail to adapt, resulting in gaps that generate uncertainty. Recent dialogues around data protection and privacy rules underscore the intricacies that organizations must traverse. Achieving equilibrium between compliance and adaptability to new regulatory developments is a nuanced challenge that organizations must endeavor to manage.

The interrelations among these three concerns complicate the technological environment and exacerbate the difficulties encountered by organizations and regulators. Securing devices, upholding privacy standards, and managing extensive ecosystems while adhering to evolving legislation are essential. Regulatory difficulties are interconnected with both technological and organizational dimensions. As technology advances outside legal frameworks, discrepancies arise, resulting in uncertainty. Reconciling compliance and agility in the face of new rules is a multifaceted problem including both technological and organizational aspects.

Technical Challenges

Addressing cyber security concerns in developing technologies poses several technological problems for organizations. These issues stem from the intricate and dynamic characteristics of developing technology and the growing complexity of cyber-attacks. The following sources provide insights into the technological difficulties related to controlling cyber security threats in new technologies.

The emergence of Fintech in the banking industry underscores the need for stringent cyber security measures and anti-fraud systems. The technological issues in securing financial technology include the protection of sensitive financial data, the assurance of secure transactions, and the defense against cyber-attacks aimed at financial institutions (Ng & Kwok, 2017).

Emerging technologies, such as the Internet of Things, Smart Grid, and Fintech, have transformed several sectors, including electricity grids. Nonetheless, the incorporation of these technologies into power grids introduces cyber security issues and risks. As power grids constitute critical infrastructure, it is essential to implement security measures to safeguard against cyber-attacks and maintain the grid's stability and resilience. Cyber security for power grids encounters difficulties in safeguarding communication networks, control systems, and the grid's resistance to cyber-attacks (Sakhnini et al., 2021). As electrical grid systems get more sophisticated and linked due to the emergence of IoT and Smart Grid technologies, the associated risks and vulnerabilities also increase (Yan et al., 2012). Therefore, it is essential to establish and execute security methods and protocols that may avert unauthorized access, data breaches, or device manipulation (Radoglou-Grammatikis et al., 2021). Researchers

emphasize the need of tackling cyber security concerns in power grids, as these initiatives are crucial for safeguarding sensitive data and ensuring grid stability. Institutions such as NIST, the Energy Expert Cyber Security Platform (EESCP), and the European Commission's Smart Grids Task Force have recognized the significance of cyber security in the advancement of grid technology (Sakhnini et al., 2021). A variety of methods and strategies have been proposed to improve the security and resilience of power grid networks. The identification and modeling of nodes inside these grids have become essential to enhance system resilience and mitigate hazards (Li et al., 2022). Strategies such as access control rules, granular dynamic access control techniques, and security assessment technologies have been investigated to safeguard power grid systems from access and cyber threats (Li et al., 2023; Qiu et al., 2022). Furthermore, research has been conducted on cloud-based charging management and effective communication frameworks to guarantee energy management and stability inside power grids (Rimal et al., 2022). In conclusion, the incorporation of developing technology into power grids presents potential but also entails cyber security threats.

Confronting problems, instituting security protocols, and embracing comprehensive cyber security strategies are essential for protecting power grid systems from cyber-attacks to guarantee dependable operation.

The emergence of technologies like the IoT has posed significant hurdles in the effective management of cyber security threats. The incorporation of IoT devices across diverse sectors, such as healthcare, industrial management, and smart homes, presents novel vulnerabilities and complications (Sharma & Sharma, 2022). To alleviate these concerns, cyber security certification programs are increasingly being adopted, propelled by business, governmental bodies, and research organizations (Khurshid et al., 2022). Nonetheless, obstacles exist in applying these certification methodologies to the varied IoT world (Matheu et al., 2020). In the domain of cyber security, there are technological challenges that need consideration. These problems include the protection of communication networks, the safeguarding of control systems, and the assurance of device resilience against cyber-attacks (Sharma & Sharma, 2022). Risk assessment and testing procedures are crucial to the development of a cyber security certification framework (Matheu et al., 2020). Historically, cyber security threats related to IoT have impeded its adoption. Nonetheless, initiatives are under progress to mitigate these risks by formulating standards and frameworks for cyber security (Khader et al., 2021). Nonetheless, difficulties remain in effectively recognizing and categorizing threats, ensuring privacy and security inside systems, and controlling the interaction between devices and the physical environment (Tawalbeh et al., 2020). Successfully overcoming these problems requires a strategy that synthesizes research results, technology tools, policy initiatives, and governance frameworks. The management of cyber security threats associated with developing technologies, particularly the Internet of Things, presents issues. These problems include complexities, assessing risks, safeguarding privacy, and instituting certification processes. Addressing these challenges requires a plan, collaboration among stakeholders, and the development of robust cyber security frameworks tailored to the specific needs of developing technologies.

Mitigating the dangers linked to cyber security is notably complex, particularly in

relation to developing technologies like as cloud computing. Cloud computing has fundamentally revolutionized the methods by which organizations store, process, and retrieve data. Nevertheless, it also introduces risks and complexity (Salek et al., 2022). Securing communication networks, protecting data and applications, and maintaining the privacy and integrity of cloud-based services are key problems in cyber security for cloud computing. The evolving characteristics of cloud systems, shared responsibility frameworks, and the possibility of access or data breaches present considerable threats (Kaja et al., 2022). To address these difficulties successfully, several strategies and best practices have been proposed in the realm of cyber security. This encompasses the use of encryption methods, the establishment of stringent access control measures, the deployment of intrusion detection systems, and the execution of security audits (Morol, 2022). Furthermore, it is essential to have explicit incident response procedures and consistently oversee cloud infrastructures to identify and alleviate cyber risks. Moreover, the management of cyber security threats in cloud computing is further complicated by legislative considerations (Aljumah & Ahanger, 2020). Compliance with data protection and privacy standards, such as the General Data Protection Regulation (GDPR), complicates security processes (Paul et al., 2020). Ensuring compliance with these rules, which pertain to jurisdictional matters and contractual obligations, necessitates meticulous coordination between cloud service providers and their clients (Kumar & Kumar, 2021). Furthermore, the fast advancement of technology such as quantum computing presents problems to the security of cloud computing. Quantum computing has the capability to compromise encryption algorithms, necessitating the creation of encryption techniques that are resilient to quantum assaults. Mitigating the effects of quantum computing on cloud security requires proactive study and cooperation among academia, business, and regulators. In conclusion, overseeing cyber security threats in developing technologies, especially with cloud computing, poses considerable hurdles. Technical difficulties, legal and regulatory compliance, and the dynamic threat environment need organizations to implement comprehensive Cyber security methodologies. Organizations may successfully manage cyber security risks in cloud computing by deploying stringent security measures, being informed about new threats, and promoting cooperation among stakeholders.

Mitigating the cyber security vulnerabilities linked to developing technologies in artificial intelligence and machine learning poses considerable problems. The incorporation of AI and ML technology introduces complications and risks that must be mitigated to guarantee cyber security measures. Securing AI models and algorithms to protect training and inference data, together with assuring the dependability and integrity of AI systems, are critical problems (Matheu et al., 2020). Considering the characteristics of AI and ML with the possibility for assaults and data poisoning, it is essential to adopt sophisticated security measures to alleviate significant risks (Goldblum et al., 2020). Furthermore, addressing the deficiency of interpretability and explainability in AI and ML models presents challenges in detecting biases, vulnerabilities, or malevolent actions that may emerge (Harshith et al., 2023). To successfully mitigate risk in cyber security, it is essential to prioritize openness and accountability in AI and ML systems. Moreover, aligning with the advancement of AI and ML technologies requires frameworks and policies that effectively

handle cyber security issues (Geluvaraj et al., 2018). The evolving characteristics of AI and ML need ongoing surveillance, updates, and patches to mitigate new vulnerabilities and threats. Collaboration among academics, industry specialists, and politicians is crucial for establishing comprehensive cyber security standards and recommendations for artificial intelligence and machine learning. In conclusion, overseeing cyber security threats in new technologies, especially with AI and ML, poses distinct problems. Technical difficulties, interpretability, and the changing threat environment need organizations to implement comprehensive cyber security strategy.

Emerging technologies, like Blockchain, provide new issues in the management of cyber security threats. The rapid use of Blockchain technology is accompanied by security issues and concerns (Zamani et al., 2018). Technical issues in Blockchain cyber security include safeguarding communication networks, securing data and transactions, and maintaining the integrity and stability of Blockchain systems (Maidamwar & Chavhan, 2020). The decentralized and transparent characteristics of Blockchain provide distinct risks that need sophisticated security protocols (Kushwaha et al., 2022). The absence of a unified framework for the development and implementation of security management techniques in Blockchain presents issues in addressing cyber security concerns (Canelon et al., 2019). The lack of a procedure for recording and reporting occurrences impedes the capacity to learn from previous errors and enhance security policies. The rapid advancement of Blockchain technology surpasses the progress of thorough cyber security frameworks and legislation. Cooperation among academics, industry specialists, and regulators is essential to tackle these difficulties and establish comprehensive cyber security standards for Blockchain (Parizi et al., 2020). Within the realm of Blockchain technology, many applications and sectors have distinct cyber security issues. In the banking industry, the adoption of Blockchain requires legislative backing, interoperability, and standardization across platforms (Abeysekera & Kumarawadu, 2022). The use of AI and Blockchain in the power production and distribution industry presents novel issues in maintaining cyber security and anticipating emerging risks (Oubelaid, 2023). In conclusion, handling cyber security threats associated with new technologies, like Blockchain, poses distinct problems. Technical difficulties, the absence of a unified framework, and the changing threat environment necessitate that organizations implement comprehensive cyber security policies. Organizations may alleviate cyber security concerns in Blockchain technology by using sophisticated security measures, fostering cooperation, and tackling domain-specific difficulties.

The difficulties associated with controlling cyber security threats in upcoming technology for autonomous cars are a significant issue. The integration of driving technology introduces difficulties and risks that need attention to provide robust cyber security.

Technical challenges in vehicle cyber security include securing communication networks, protecting data and systems, and ensuring the dependability and integrity of driving systems (Campbell et al., 2010). Due to the characteristics of cars and the possibility of cyber-attacks and data breaches, significant risks need enhanced security measures (Raiyn, 2018). Moreover, it is essential to collaboratively design the safety and security features of cars to address cyber security threats efficiently (Kavallieratos et al., 2020). Creating models

and frameworks for risk assessment is essential for detecting and reducing vulnerabilities and threats. Collaboration among academics, industry professionals, and politicians is essential for defining cyber security standards and recommendations for autonomous cars (Cui et al., 2019). Autonomous cars have distinct cyber security concerns across diverse applications and sectors. The design of autonomous vehicle voice agents (AVVAs) influences the intention to adopt and the overall experience of autonomous cars (Lee et al., 2019). Moreover, the communication and networking technologies for autonomous cars need dependable and secure communication systems (Zolich et al., 2018). In summary, overseeing cyber security threats in developing technologies, especially with autonomous cars, poses distinct issues. The intricate technical challenges, co-engineering of safety and security, and the changing threat environment necessitate that organizations implement thorough cyber security policies. Organizations may successfully minimize cyber security threats in autonomous vehicle technology by using sophisticated security measures, fostering cooperation, and tackling domain-specific difficulties. Table 1 presents a summary of the technological obstacles encountered in the management of cyber security risks associated with several developing technologies.

Table 1 Technical Difficulties in Overseeing Cyber security Threats 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, controlling cyber security risks in developing technologies necessitates tackling several technological obstacles. These problems include the safeguarding of financial technology, power grids, Internet of Things devices, cloud services, artificial intelligence and machine learning technologies, blockchain, and autonomous cars. Organizations must be informed on the newest cyber security policies and technology to properly address these technological issues and safeguard against changing cyber-attacks.

Organisational Challenges

Organizations must confront the issues of managing cyber security threats associated with developing technology. These

difficulties include the culture of talent management and awareness. A specific administrative problem in controlling cyber security threats is personnel management. The transition to virtual workplace ecosystems, expedited by the COVID-19 pandemic, has brought complexity in addressing cyber security threats (Burrell, 2020). Organizations must understand the complexities associated with managing cyber security staff. Verify that they have the necessary skills to address new dangers (Treacy et al., 2023). This entails the recruitment and retention of cyber security experts to effectively manage and mitigate risks linked to developing technologies (Zwilling, 2022).

A notable problem is cultivating a cyber security culture inside the organization. Historically, safeguarding information assets has relied significantly on the implementation of hardware and software controls. Nonetheless, dependence on controls is inadequate in addressing contemporary information risk landscapes. The cyber security culture inside an organization includes personnel, methodologies, procedures, symbols, technology, training, knowledge, commitment, and actionable measures used to maintain cyber security (De Silva, 2023). Establishing a cyber security culture involves enhancing employee knowledge via training programs and cultivating a feeling of responsibility and dedication to upholding security protocols throughout the organization.

Furthermore, maintaining knowledge of cyber security threats is essential. The escalation of cyber threats has prompted managers and policymakers to reassess cyber security protocols at organizational, sectoral, and national levels (Tsohou et al., 2023). Organizations must comprehend the cyber hazards they may encounter and the repercussions that data breaches might impose on their operations (Naik, 2022). This comprehension allows organizations to formulate plans and initiatives to mitigate cyber security threats.

In summary, addressing cyber security risks associated with developing technology poses problems for organizations. These difficulties include people management, cultivating a cyber security culture, and enhancing organizational understanding of cyber security threats. Addressing these difficulties necessitates the recruitment and retention of cyber security specialists, the cultivation of a cyber security culture inside the organization, and ensuring that all members recognize and understand the possible hazards related to cyber security.

Regulatory Challenges

Securing developing technology necessitates that organizations navigate regulatory challenges. These problems include the changing frameworks, compliance requirements, and the significance of international cooperation. A significant problem in mitigating cyber security threats is the structure of regulatory regimes. As new technologies advance, regulatory organizations have the issue of maintaining alignment with this evolving environment. As a result, there may be deficiencies in legislation and an absence of recommendations for addressing cyber security concerns linked to these technologies (Hadzovic et al., 2023). To guarantee compliance and avoid risks, organizations must remain informed about legislative changes and adapt their cyber security plans appropriately.

Compliance obligations provide difficulties in the management of cyber security threats. Organizations across sectors such as banking, healthcare, and IoT must adhere to compliance norms and laws. These requirements often require the

implementation of cyber security measures, the execution of risk assessments, and the preservation of data privacy. Meeting compliance regulations may be intricate and resource-demanding, as organizations must dedicate resources and expertise to assure conformance (Jalali & Kaiser, 2018).

Moreover, global collaboration is essential in addressing cyber security threats linked to developing technology. Cyber security dangers transcend geographical borders. Efficient risk management necessitates cooperation and information exchange across nations and regulatory authorities (Dacorogna & Kratz, 2023). Nonetheless, attaining collaboration in the domain of Cyber security presents challenges because to variations in methodologies, legal frameworks, and geopolitical influences. Organizations operating worldwide must manage these complications.

The Malaysian Communications and Multimedia Commission (MCMC) is tasked for regulating cyber security in Malaysia. One issue encountered by organizations such as MCMC is adapting to the dynamic nature of regulatory regimes. As new technologies progress, organizations must remain informed about these developments (Perumal et al., 2018). This may sometimes lead to regulatory loopholes and insufficient guidance for addressing cyber security concerns linked to these technologies. Organizations operating in Malaysia must adapt to these evolving frameworks. Ensure adherence to legislation to proficiently handle cyber security threats (Abdalla & Arshad, 2020). In Malaysia, organizations must comply with rules and regulations established by MCMC, including the Malaysian Personal Data Protection Act (PDPA) and the Malaysian Communications and Multimedia Act. (CMA) (Alibeigi & Munir, 2020).

Organizations must take cyber security safeguards by conducting risk assessments to safeguard data privacy and confidentiality. Meeting these compliance standards may be resource-intensive, requiring organizations to invest resources and expertise for compliance. In Malaysia, organizations must engage closely with MCMC to comprehend and adhere to duties for the efficient management of cyber security risks. Numerous research publications examine the problems and effects of cyber security policies in Malaysia. Shaukat et al. (2020) examine the challenges encountered in using machine learning methodologies within cyber security, emphasizing the need for frameworks to evolve in response to changing technology and mitigate associated risks.

In summary, managing cyber security risks in developing technologies necessitates addressing difficulties such as changing frameworks, compliance mandates, and their effects on cyber security practices. It is essential for organizations in Malaysia to be informed about changes, adhere to MCMC legislation, and prioritize cyber security measures for successful risk management.

Existing Risk Management

Effective risk management is essential for every organization, since it involves identifying, assessing, and mitigating any risks that might impede the achievement of objectives. Through the use of risk management methods, organizations may proactively detect and mitigate possible threats across many operational domains, including financial, operational, and reputational risks. By systematically implementing management policies, processes, and practices, organizations may proficiently mitigate risk and secure their sustainability.

Best Practices in Existing Risk Management Strategies for Cyber security

Effectively tackling the difficulties of cyber security in the area of technology requires a strategic strategy. Researchers have found nine strategies for efficiently managing and mitigating current hazards. A crucial component of this methodology is recognizing and assessing risks, often using recognized frameworks such as the NIST Cyber security Framework or ISO standards. These frameworks provide a systematic approach for evaluating cyber security risks and prioritizing risk mitigation (Rea-Guaman et al., 2020).

A vital component is the adoption of Multi-Factor Authentication (MFA), which bolsters security by requiring several forms of verification. This is particularly important for access accounts when access is possible. MFA has progressed from single-factor authentication (SFA) to two-factor authentication (2FA). It currently incorporates sensors and providers that provide user authentication (Ometov et al., 2018). The growing use of MFA is driven by the need for reliable authentication across many services. Prevalent IoT cyber security solutions, such as multi-factor authentication (MFA), are essential for safeguarding information confidentiality, identifying and mitigating online threats and vulnerabilities, and administering credentials. The use of MFA and other cyber security solutions is crucial for safeguarding against cybercrime and guaranteeing secure interactions with new technologies (Kanu et al., 2022).

The third strategy involves the upgrading and management of software patches, which is essential when integrated with MFA. Automated updating and patching may substantially reduce the likelihood of cyberattacks (Ansari et al., 2022). Software upgrades mitigate cyber security threats by rectifying flaws and fortifying system security. Algarni et al. (2021) emphasize the need of software updates to rectify known vulnerabilities and safeguard against assaults. They underscore the need for organizations to prioritize and execute software updates according to the severity of vulnerabilities and their possible effect on the system, using a risk-based methodology. Patch management is a critical component of cyber security risk management. Dissanayake et al. (2020) performed a literature study on software security patch management, highlighting difficulties, methodologies, tools, and practices. They underscore the need of a thorough patch management protocol that include vulnerability screening, evaluation, prioritization, and prompt implementation of fixes. The assessment emphasizes the need for efficient tools and methodologies to tackle the issues related to patch management. Yaacoub et al. (2021) examine the cyber security implications of robotic surgery, highlighting the need of regular software upgrades to mitigate vulnerabilities and bolster system security. It is advised to adhere to cyber security best practices, invest in routine software upgrades, and enhance transparency to guarantee the comprehensive safety and security of robotic surgical systems.

The fourth way involves providing training and awareness programs to workers, since human errors remain a contributing role in cyber security breaches. Thus, continuous education and simulated assessments, such as phishing attack simulations, may significantly improve an organization's cyber security posture.

The fifth strategy entails the use of data encryption, a method for protecting sensitive information, especially during transmission or storage. Data encryption serves as a safeguard against unauthorized access to

critical information. Eichelberg and Kleber (2020) emphasize the need of using encryption methods in Picture Archiving and Communication Systems (PACS) and medical imaging. They underscore the use of encryption techniques to guarantee the security and integrity of data during transmission and storage. They emphasize the significance of data encryption inside cyber security protocols. Encryption serves to protect data from unauthorized access, even if it is intercepted or compromised. It is advisable to use encryption protocols for sensitive data at rest, in transit, and in use. Implementing data encryption necessitates the use of powerful encryption algorithms and safe key management protocols. Organizations must embrace industry-standard encryption protocols and guarantee the correct installation and setup of encryption technologies.

The sixth aspect that may greatly aid in addressing a cyber security event is the existence of a comprehensive and routinely updated incident response strategy. It may save a little disturbance from escalating into a significant tragedy. The plan must be frequently tested, and personnel should be acquainted with the procedures to be implemented during a real crisis. Efficient incident response is essential for mitigating the effects of a cyber security event. Burrell (2020) emphasizes the function of incident response teams in managing events, doing intrusion assessments, overseeing crisis management, and conducting forensic data analyses. These teams are essential in rapidly containing and reducing the situation. The use of incident Management frameworks are crucial for directing organizations in the resolution of cyber security incidents. Walker-Roberts et al. (2019) underscore the significance of comprehending security concerns in the context of cyber-physical systems. They underscore the significance of incident management systems in addressing the risks associated with cyber security events. The participation of elements is essential in resolving cyber security events. Walker-Roberts and colleagues Walker-Roberts et al. (2019) emphasize the significant internal security violations caused by human mistake. This underscores the need for a reassessment of cyber security principles and the significance of training and awareness programs to mitigate human variables in incident response.

Ongoing surveillance and periodic assessments are crucial to the appraisal of cyber security protocols inside an organization. They provide insights on the efficacy of these measures. Assist in identifying areas for improvement. Regular audits are essential for evaluating the effectiveness of cyber security measures and identifying vulnerabilities or deficiencies inside the system. Islam et al. (2018) underscore the significance of audit functions in performing security and cyber security audits. The report emphasizes the need for audit teams to possess the requisite knowledge and competence to comprehensively assess cyber security risks and controls. Continuous monitoring is the real-time surveillance of systems, networks, and data to swiftly identify and address cyber security problems. Malatji et al. (2019) underscore the significance of ongoing surveillance within a socio-technical systems cyber security paradigm. The report emphasizes the need for organizations to consistently evaluate their cyber security strategies to guarantee the alignment of social, technological, and environmental aspects.

The eighth facet of cyber security often neglected is vendor risk management. Organizations must assess the cyber security protocols of third-party vendors and mandate contractual obligations that ensure

compliance with established cyber security standards. Many firms rely on suppliers to provide various services, which may include providing them access to information. It is important to evaluate and mitigate the cyber security risks linked to these third parties to safeguard data.

Ultimately, it is important for organizations to comply with regulatory standards, not alone due to legal obligations but also because it offers a foundation for implementing effective cyber security measures. Ensuring adherence to these objectives involves ongoing monitoring and improvement. Organizations should establish systems to monitor their compliance status, including performing audits and evaluations. This facilitates the identification of deviations or non-compliance, allowing organizations to take immediate action. Furthermore, being informed on alterations in laws, regulations, and industry standards is essential for ensuring compliance. By integrating these nine practices into their cyber security risk management strategies, organizations may adeptly traverse the domain of developing technologies while maintaining a superior degree of security assurance.

Case Study in Existing Risk Management Strategies for Cyber security

The effective implementation of risk management methods in developing technologies is most comprehended via empirical case studies. These case studies give insights into successful techniques and critical lessons for organizations aiming to improve their cyber security posture.

Ng and Kwok (2017) performed a case study on the rise of Fintech and cyber security in Hong Kong as an international financial hub. The research focused on the regulatory framework and the development and execution of supplementary regulatory policies by the Hong Kong Monetary Authority (HKMA), the financial regulator of Hong Kong. The authors discovered that the HKMA used a risk-based strategy to manage the potential and hazards related to Fintech. They emphasized the need of establishing a cyber security profession that includes proficiency in auditing, management controls, risk management, and information technology. This is essential for tackling emerging cyber risks in a financial center (Ng & Kwok, 2017).

The case study by Raimundo and Rosário (2022) examines the cyber security problems in the Industrial Internet of Things (IIoT). The research examines critical papers to assess the potential and risks related to IIoT cyber security. The authors have discovered a substantial gap in the existing effectiveness of IoT cyber risk solutions after a literature study. This obviously suggests that there is potential for improving the capacity to mitigate the cyber security threats linked to IIoT. The case study underscores the need for research and development to enhance the efficacy of cyber security measures in the context of IIoT. By solving this deficiency, organizations may enhance the protection of their industrial systems and infrastructure against cyber-attacks in the evolving technological world.

Gaps in Current Research and Practice

Emerging technologies are progressing swiftly and have instigated substantial transformations across several sectors. Nevertheless, they also provide novel cyber security dangers and concerns. Despite significant advancements in comprehending the ramifications of cyber security in developing technologies, some critical problems persist, necessitating more academic inquiry. This study seeks to identify and analyze the deficiencies in existing research and practices on the

management of cyber security risks associated with developing technologies.

Comprehensive frameworks are essential for conducting cost-benefit analyses to mitigate cyber security risks associated with developing technologies. Nevertheless, there is a paucity of particular references addressing this subject. Consequently, I will provide a comprehensive review of cost-benefit analysis frameworks and their limitations. Cost-benefit analysis is the evaluation of the costs and advantages linked to a certain choice or investment. It assists organizations in evaluating the economic viability and prospective returns of cyber security projects. Although much literature exists on cost-benefit analysis across other disciplines, cyber security remains an evolving domain. A shortcoming of current cost-benefit analysis frameworks is the absence of approaches especially designed for cyber security. Numerous research concentrates on finding and measuring the costs and benefits linked to cyber security solutions. Frameworks are required that consider the distinct qualities and problems presented by new technologies. Future research should focus on developing frameworks and procedures for doing cost-benefit evaluations within the realm of cyber security to address these constraints. This entails developing criteria to assess the costs and benefits of cyber security measures while including dynamic and changing aspects into the study. Furthermore, initiatives must be undertaken to augment data collection and dissemination to refine the precision of cost-benefit calculations. While references specifically addressing the deficiencies in cost-benefit analysis frameworks for cyber security in developing technologies may be lacking, the available references give insights into cost-benefit analysis approaches across other areas.

Despite advancements in cyber security technology, we must not disregard the aspect that remains a constant and sometimes undervalued element in the cyber security equation. Human mistake remains a substantial contributor to security breaches in security systems. These faults may include minor mistakes, such as password use, to more intricate problems, including susceptibility to phishing attempts. Consequently, it is essential to comprehend the factors that lead to cyber security vulnerabilities. The ramifications of human error on cyber security beyond mere blunders. Infiltrates extensive organizational and cultural frameworks. An organization's cyber security culture influences employee behavior. In organizations where cyber security is deprioritized, personnel are more susceptible to behaviors such as using networks or disseminating critical information without appropriate authorization. Moreover, the issue of mistake extends beyond workers to include third-party suppliers, contractors, and other external stakeholders who engage with an organization's information systems. The lack of training programs for these organizations might exacerbate the hazards linked to human error.

Organizations must use a multifaceted strategy to alleviate the risks associated with human error. This strategy encompasses both solutions and extensive training programs aimed at improving workers' cyber security awareness. Organizations have to tailor these programs to address the risks associated with their operations. It is important to update them to ensure alignment with the evolving cyber security scenario. Executing simulated cyber-attack exercises, such as phishing simulations, may significantly enhance workers' ability to recognize and appropriately react to attacks.

In conclusion, while technology will persist

in significantly boosting cyber security, addressing the human factor is equally vital. A detailed comprehension of human error's involvement in cyber security events, grounded on empirical research, may substantially enhance the formulation of more effective risk mitigation techniques.

Conclusion

Managing cyber security threats in new technologies is a continually evolving problem for organizations. The present condition of cyber security in these technologies underscores the significance of risk management solutions. Organizations have challenges when addressing these risks, including institutional and regulatory impediments. Technical challenges mainly concern the security of communication networks, safeguarding data and systems while assuring the reliability and integrity of evolving technologies. Addressing cyber security concerns presented by developing technology may be fairly difficult for organizations. A key component is educating and equipping the personnel with appropriate techniques to address these difficulties. Furthermore, regulatory problems arise from compliance obligations within a worldwide framework characterized by varied cyber security legislation. To proficiently manage cyber security risks in developing technologies, organizations may use traditional risk management approaches, including systematic risk identification and evaluation.

Nonetheless, there are deficiencies in current studies and methods that need consideration. The deficiencies include the absence of frameworks for executing cost-benefit evaluations, understanding the impact of human error on cyber security events, and the need for comprehensive plans to address the ever-expanding environment of cyber security threats. Addressing these gaps necessitates research focused on creating standardized frameworks for cost-benefit evaluations, enhancing comprehension of human dynamics in cyber security events, and formulating effective tactics for workforce training and preparedness. Moreover, it is crucial to recognize the evolving nature of compliance and examine the challenges associated with interoperability in developing technologies. These factors need research endeavors. By concentrating on closing gaps and executing comprehensive risk management strategies, organizations may enhance their cyber security protocols to effectively mitigate risks in the dynamic landscape of developing technologies.

References

1. Abdalla, M., & Arshad, Y. B. (2020). Information Security: Cyber security Standards Adoption Among Malaysian Public Listed Companies. International Journal of Engineering Research and Technology, 9(8). https://doi.org/10.17577/IJERTV9IS080133
2. 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
3. Algarni, A., Thayananthan, V., & Malaiya, Y. K. (2021). Quantitative Assessment of Cyber security Risks for Mitigating Data Breaches in Business Systems. Applied Sciences, 11(8), 3678. https://doi.org/10.3390/app11083678
4. 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

5. 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
6. Ansari, M. M., Sharma, P. K., & Dash, B. (2022). Prevention of Phishing Attacks Using AI-Based Cyber security Awareness Training. International Journal of Smart Sensor and Adhoc Network., 3(3), 61-72. https://doi.org/10.47893/IJSSAN.2022.1221
7. Burrell, D. N. (2020). Understanding the Talent Management Intricacies of Remote Cyber security Teams in COVID-19 Induced Telework Organisational Ecosystems. Land Forces Academy Review, 25(3), 232 - 244. https://doi.org/10.2478/raft-2020-0028
8. 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
9. Canelon, J., Huerta, E., Incera, J., & Ryan, T. (2019). A Cyber security Control Framework for Blockchain Ecosystems. The International Journal of Digital Accounting Research, 19, 103-144. https://doi.org/10.4192/1577-8517-v19_5
10. 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
11. 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
12. De Silva, B. (2023). Exploring the Relationship Between Cyber security 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
13. 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
14. 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
15. Eichelberg, M., & Kleber, K. (2020). Cyber security 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. Journalof Cyber Policy, 6(2), 137-154. https://doi.org/10.1080/23738871.2021.1973526

16. Geluvaraj, B., Satwik, P. M., & Kumar, T. A. A. (2018). The Future of Cyber security: 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
17. 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
18. 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
19. 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
20. Hireche, R., Mansouri, H., & Pathan, A.-S. K. (2022). Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis. Journal of Cyber security and Privacy, 2(3), 640-661. https://doi.org/10.3390/jcp2030033
21. Islam, M. S., Farah, N., & Stafford, T. W. (2018). Factors Associated With Security/Cyber security Audit by Internal Audit Function. Managerial Auditing Journal, 33(4), 377-409. https://doi.org/10.1108/maj-07-2017-1595
22. Jalali, M. S., & Kaiser, J. (2018). Cyber security in Hospitals: A Systematic, Organisational Perspective. Journal of Medical Internet Research, 20(5), e10059. https://doi.org/10.2196/10059
23. 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
24. Kanu, V. P. S., Naiem, Y. A., & Prasad, S. S. (2022). A Research of Cyber security 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
25. Kavallieratos, G., Katsikas, S. K., & Gkioulos, V. (2020). Cyber security and Safety Co-Engineering of Cyberphysical Systems: A Comprehensive Survey. Future Internet, 12(4), 65. https://doi.org/10.3390/fi12040065
26. Khader, M., Karam, M. R., & Fares, H. (2021). Cyber security Awareness Framework for Academia. Inf., 12(10), 417. https://doi.org/10.3390/info12100417
27. Khurshid, A., Alsaaidi, R., Aslam, M., & Raza, S. (2022). EU Cyber security Act and IoT Certification: Landscape, Perspective and a Proposed Template Scheme. IEEE Access, 10, 129932-129948. https://doi.org/10.1109/ACCESS.2022.3225973
28. Kumar, N., & Kumar, S. (2021). Conceptual Service Level Agreement

Mechanism to Minimise the SLA Violation with SLA Negotiation Process in Cloud Computing Environment.

29. 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
30. Lee, I. (2020). Internet of Things (IoT) Cyber security: Literature Review and IoT Cyber Risk Management. Future Internet, 12(9), 157. https://doi.org/10.3390/fi12090157
31. 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
32. 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
33. 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
34. 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/ijeast2020.v04i12.039
35. Malatji, M., Solms, S. V., & Marnewick, A. (2019). Socio-Technical Systems Cyber security Framework. Information and Computer Security, 27(2), 233-272. https://doi.org/10.1108/ics-03-2018-0031
36. Matheu, S. N., Hernández-Ramos, J. L., Skarmeta, A. F., & Baldini, G. (2020). A Survey of Cyber security Certification for the Internet of Things. ACM Computing Surveys (CSUR), 53(6), 1 https://doi.org/10.1145/3410160
37. 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
38. 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
39. Ng, A. W., & Kwok, B. K. B. (2017). Emergence of Fintech and Cyber security in a Global Financial Centre. Journal of Financial Regulation and Compliance, 25(4), 422-434. https://doi.org/10.1108/jfrc-01-2017-0013
40. 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
41. 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

42. Parizi, R. M., Dehghantanha, A., Azmoodeh, A., & Choo, K. K. R. (2020). Blockchain in Cyber security Realm: An Overview. Blockchain Cyber security, Trust and Privacy, 79, 1-5. https://doi.org/10.1007/978-3-030-38181-3_1
43. 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
44. 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
45. 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
46. 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
47. Raimundo, R. J., & Rosário, A. T. (2022). Cyber security in the Internet of Things in Industrial Management. Applied Sciences, 12(3), 1598. https://doi.org/10.3390/app12031598
48. 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
49. Rea-Guaman, A. M., Mejía, J., San Feliu, T., & Calvo-Manzano, J. A. (2020). AVARCIBER: A framework for assessing cyber security risks. Cluster Computing, 23, 1827-1843. https://doi.org/10.1007/s10586-019-03034-9
50. 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
51. 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
52. Salek, M. S., Khan, S. M., Rahman, M. M., Deng, H.-W., Islam, M., Khan, Z., Chowdhury, M., & Shue, M. (2022). A Review on Cyber security 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
53. 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

54. 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 Cyber security. Energies, 13(10), 2509. https://doi.org/10.3390/en13102509
55. 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
56. 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
57. Treacy, S., Sabu, A., Bond, T., O'Sullivan, J., Sullivan, J., & Sylvester, P. (2023). Organizational Cyber security 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
58. 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
59. 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
60. 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
61. 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
62. 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
63. 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
64. 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