Journal of Information Systems Engineering and Management
2025, 10(17s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

Opportunities and Barriers to Implementing Cyber-solutions in Higher Education Institutions

Grace Egenti[1*], Olubunmi Okesola[2], Falade Adesola[3], Oluranti Sangodoyin[4], Grace Jokthan[1], Olatunji Okesola[1,4]

[1]Africa Centre of Excellence on Technology Enhanced Learning (ACETEL), Abuja, Nigeria

[2]Library and Information Sciences, University of Ibadan, Ibadan, Nigeria

[3]College of Software Engineering, McPherson University, Seriki Sotayo, Nigeria

[4]Department of Cybersecurity, Abiola Ajimobi Technical University, Ibadan, Nigeria

**Corresponding Author: gegenti@noun.edu.ng*

ARTICLE INFO

Received: 05 Dec 2024

Revised: 24 Jan 2025

Accepted: 08 Feb 2025

ABSTRACT

In this era of advanced and emerging technologies, cyber-attacks have become the most challenging issues confronting cyber systems globally, and raising the necessity for Cybersecurity Solutions (Cyber Solutions) worldwide, especially amongst youths who are the heavy users of Internet and social media. This study is a Literature Review of Cyber Solution Implementation in Institutions of Higher Learning, highlighting the unique challenges faced by the developing countries and possible solution. Opportunities lie in emerging technologies and international collaboration, while barriers include socio-economic factors, infrastructure limitations, and policy challenges. The study emphasizes the significance of addressing cybersecurity for national security and economic stability, especially as it concerns developing states. It provides theoretical contributions, practical recommendations, and suggests for future research to explore cultural impacts and the sustainability of international collaboration efforts. The paper emphasizes the global responsibility to strengthen cybersecurity in developing nations for equitable digital participation and a secure digital landscape.

Keywords: Cyber-attacks, cybersecurity, developing countries, digital divide, emerging technologies.

INTRODUCTION

In an era dominated by rapid technological advancements and cyber-attacks, the significance of cybersecurity cannot be overstated (Burt, 2023; Kawalec, 2021; Tariq et al., 2023). As societies across the globe become increasingly interconnected through digital networks, the protection of information and the integrity of cyber systems have emerged as critical concerns (Li & Liu, 2021; Marr, 2023). Cybersecurity, a multidimensional field encompassing technologies, processes, and policies, is deployed to safeguard computer networks, computer systems (desktops and laptops), and data from unauthorized access, attacks, and damage (Madnick et al., 2023; Ulrich, 2023). Cybersecurity is essential not only for the smooth functioning of contemporary societies but also for the preservation of individual privacy (Joseph & Fred, 2023), economic stability (Juneja et al., 2024), and national security (Bits IO Inc, 2024; Reveron & Savage, 2020). The significance of cybersecurity is underscored by its position in retaining the integrity of important infrastructure, including electricity grids, financial structures, and healthcare networks (Krause et al., 2021; Ulrich, 2023; Uddin et al., 2020; Javaid et al., 2023).

Recent research emphasizes the evolving nature of cyber threats, with an increasing consciousness of advanced persistent threats (APTs) (Ogugua et al., 2024), ransomware attacks (Muniandy et al., 2024), and the exploitation of vulnerabilities in rising technology like the Internet of Things (IoT) (Dave et al., 2023). As the technology era progresses, the asymmetry in cybersecurity preparedness possess a tremendous challenge, specifically for nations striving to navigate the complexities of an increasingly interconnected global system. The overarching question guiding this observation is: How can developing countries conquer the prevailing obstacles and capitalize on opportunities to beef up their cyber security resilience? In analysing this research problem, the study will delve into the particular demanding situations faced by developing nations in implementing robust cyber security measures. These demanding situations not only deploy the best use of technological components but also add socio-monetary elements, regulatory frameworks, academic disparities, and the wider impact of the digital divide.

An obtrusive divide persists between developed and developing countries concerning access to and proficiency in cybersecurity measures. This digital divide, regularly reflective of broader socio-financial gaps, accentuates the challenges faced by developing nations in securing their digital infrastructures. Hence, this research will attempt to critically examine the history of cybersecurity in the context of growing international locations, shedding light on the possibilities that lie ahead and the modern-day obstacles that preclude progress. This study will also highlight the true assessment of cybersecurity capabilities among developed and developing countries. A nuanced understanding of those demanding situations is crucial for formulating powerful techniques that align with the precise contexts of developing countries.

A deep analysis of the cybersecurity environment in developing countries is within the scope of this study. The main goal of this study is to holistically integrate the different facets and aspects surrounding cybersecurity in developing countries. The study will assess the current state of cyber security in developing countries, identify opportunities for improving cyber security in developing countries, analyse the barriers hindering the effective implementation of cyber security measures, and propose strategies and recommendations for strengthening cyber security in developing countries.

The significance of this study lies in providing policymakers, cybersecurity professionals, and stakeholders with an understanding of those critical issues that prevent measures to enhance security against cyberspace threats from being effectively implemented in developing countries. The digital divide is opening up, and only by appreciating the responsibility that this brings to society can we promote cyber security programs that are both inclusive and sustainable. The purpose of this study, in tackling the research problem, is to offer fresh insights that can be used across all of society by those who wish to narrow the cybersecurity chasm between developed nations and developing countries. The findings will serve as a foundation for the development of tailored strategies, policies, and capacity-building initiatives that align with the socio-economic and technological landscapes of developing nations. Additionally, the study holds relevance for the global community by emphasizing the interconnected nature of cybersecurity. In an era where cyber threats transcend national boundaries, bolstering the cybersecurity resilience of developing countries is not only an ethical imperative but also a pragmatic approach to fortifying the collective security of the digital ecosystem.

RELATED LITERATURES

Historical Development of Cybersecurity in Developing Countries

In examining the historical progress of cybersecurity in developing countries, it is important not to ignore those pioneering efforts that provided a foundation upon which later attempts at protecting digital landscapes were built. The evolution of cybersecurity, however, has been much clearer in developed countries. But developing nations have demonstrated their resilience and are gradually becoming aware that building up digital muscle is absolutely essential for national survival. In fact, the early attempts in developing countries have often been similar to those of their more economically advanced counterparts. The differences are largely due to differential socio-economic conditions. Foundational steps involved the establishment of cybersecurity frameworks and awareness that protective measures were needed. Developing governments and businesses began investing in cybersecurity infrastructure only somewhat later compared to developed countries. Table 1 describes the various stages at which the developing countries were able to breakthrough in cybersecurity that strengthens the cyberspace.

Table 1: Development Stages in Cybersecurity in Developing countries

Year	Breakthroughs	Description
1970's	The dawn of Digital Threats	i. The Creeper and Reaper: The 1970s witnessed the birth of the first computer viruses and aptly named Creepere and Reaper. These were relatively harmless, but they served as a wake-up call, highlighting the vulnerability of interconnected systems. ii. ARPANET and the birth of security concerns: The creation of ARPANET, the precursor to the modern internet, introduced the concept of network security. As information started flowing across networks, the need for its protection became evident.
1980's	The Rise of Viruses and Antivirus	i. The dawn of Antivirus: The fight back began with the birth of commercial antivirus software like Anti4us and flushot plus. These early solutions marked the beginning of a continuous arms race between attackers and defenders. ii. The Morris Worm: The 1980s saw a significant escalation in cyber threats with the Morris worm that crippled a significant portion of early internet, emphasizing the need for robust security measures.
1990's	The Wild Wild Web Takes Off	i. The Internet Boom: The widespread adoption of the Internet brought a surge in cybercrime. Hackers targeted businesses and individuals alike, highlighting the need for broader security awareness. ii. The rise of Phishing: Phishing scams, where attackers trick users into revealing sensitive information, emerged as a major threat in the 1990s.This tactic continues to plague users today, demonstrating the need for constant vigilance.
2000's	Complexity Breeds Challenge	i. The Rise of spyware and Malware: The 2000s saw the rise of spyware and malware that could steal data, track user activity, and disrupt computer operations. ii. Cyber-attacks Become More Targeted: Cyber-attacks started to become more sophisticated and targeted, with hackers focusing on stealing specific data or disrupting critical infrastructure.
2010's	The Age of Advanced Threats	i. Cloud computing brought new security challenges, requiring organisations to adapt their security strategies to data protection. ii. Multi-factor authentication (MFA) became an essential layer of defense, adding an extra step to the login process.
2020's	The Ever- Evolving Threat Landscape	i. Artificial Intelligence (AI) is playing a growing role in both cybersecurity offense and defense, with automated systems constantly learning and adapting. ii. Focus on privacy regulations like General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) emphasizes the importance of data protection and users control over their information.

Recognizing the importance of cybersecurity to national security and economic stability, governments in developing countries also understood its strategic significance. Governments in these nations took the lead and began to draft cybersecurity policies, frameworks, and strategies as new forms of digital threat emerged (Reveron & Savage, 2020). For example, the development of Computer Emergency Response Teams (CERTs) and national cybersecurity strategies were early signs that governments had embraced a more proactive approach. In a first-of-its-kind move, in 2013, the Indian government unveiled its National Cyber Security Policy (Ministry of Electronics and Information Technology, Government of India), detailing an all-round approach to respond adequately to mounting security concerns on the Internet (Dilipraj, 2014). That policy was a milestone in the early attempts of a developing country to develop national-level formal cybersecurity controls.

The other important dimension of early cybersecurity development in developing countries was the arrival of public-private partnerships. Since cybersecurity is something that requires collective efforts, studies stress the significance of cooperation between government agencies and enterprises as well as non-governmental organizations in order to realize effective implementation (Oktavianus et al., 2018; Christensen & Petersen, 2017). A case in point is the Brazilian Internet Steering Committee (CGI.br), established late in the 1990s, which reflects a consultative model adopted by many developing countries. CGI.br, made up of representatives from different fields, was especially important in drawing up standards and guidelines for internet security (Hurel & Lobato 2018; Trinkunas & Wallace 2015).

1.1 Evolution of Cyber Threats

The nature of cyber threats has been an ever-changing playing field. Developing countries face a special set of problems fused by considerations relating to socio-economics, technology lagging behind developed nations, and geopolitical policies.

1.1.1 Rise of Cybercrime and Financial Threats

According to research, however, among developing countries, most of the various threats posed by cyberspace have taken on a form that is closest to (or at least not very far from) cybercrime. More important than hacks targeting governments or military websites are hackers who steal information for business purposes and money-hungry scam artists focusing their sights, especially upon banking institutions. Because the development of online banking and other financial transactions increases so rapidly, developing nations are particularly vulnerable to threats in the cyber-financial arena (Acharya & Joshi 2020; Uddin et al. 2019). Business-Ghana (2018) reported that well over half a million instances of everything from *trojans* to *worms* turned them away last year alone. Specifically, there were more than 400 malware-related events at financial institutions alone! While other sources (Khadam et al., 2023; Paquet-Clouston et al., 2018; Yaacoub et al., 2022) say that million cases of spam email and botnet cyber-attacks on digital networks have also occurred, criminal actors take advantage of the digital divide to choose their targets according to weaknesses in banking systems as well as various forms of online receipts and settlements. Another significant example is the wave of financial cybercrime in Nigeria. The Central Bank has reported that fraudulent activities involving online banking and electronic payment systems have increased sharply (Wang et al., 2020; Fatoki, 2023). This trend suggests that a tailored cybersecurity response to the peculiar threats from financial cyberthreats is needed in developing countries (Li & Liu, 2021).

1.1.2 Challenges in Critical Infrastructure Protection

As developing countries have continued to develop their critical infrastructure in step with technological progress, these threats have simultaneously increased (Markopoulou & Papakonstantinou, 2021). In reality, it seems today's cyber threats are not being properly described. Studies have identified the future direction of these dangers as including targeted attacks on critical infrastructure such as electricity and water grids, railways, and transport networks (Reed, 2023; Ospina et al., 2021). The absence of effective cybersecurity in these areas has exposed developing nations to the threat that essential services may be disrupted. So, for example, in South Africa, the energy sector has continually suffered from a lack of cybersecurity. There have been reports of efforts to break into power grid infrastructure (Putter & Bachmann, 2022); these incidents illustrate the changing nature of cyber threats and that developing countries must be serious about safeguarding critical infrastructure.

1.1.3 State-Sponsored Cyber Espionage

A geopolitical element has also been introduced into the shape of this evolving threat: many developing countries, including Bangladesh and Nepal, have themselves become targets of state- sponsored cyber espionage (Priyandita et al., 2022; Rowe, 2019; Wiggen, 2020). Studies show that developing nations have occasionally found themselves in the firing line of cyber clashes between leading powers, which has fuelled concerns about national security and data sovereignty. In one outstanding case, in 2016, we faced a major cyberattack known as the Bangladesh Bank heist, where hackers tried to steal money from the country's central bank. The episode raised questions about the susceptibility of developing countries to complex cyber-attacks and how they could improve their own capabilities in this area (Finkle, 2016; Hammer, 2018).

1.2 Current State of Cyber Security in Developing Countries

The existing state of cybersecurity in developing nations around the world is a complicated landscape with divergent challenges and changing practices. With nations scrambling to protect their digital environment, exploring current cybersecurity practices shows what paths they took and what measures were adopted (and how well), as well as the systemic gaps they could not overcome. The following are the current state of cybersecurity in developing countries as identified by various researchers:

a) Government Initiatives and Policies

The necessity of enhancing cybersecurity capabilities has been gradually recognized by governments in developing countries. Others have created national strategies and policies to guide cybersecurity efforts. For instance, the Cyber Swachhta Kendra, set up by India's Ministry of Electronics and Information Technology, offers cybersecurity services for citizens and organizations (The Indian Express, 2017). The National Cybersecurity Policy in Nigeria also provides a comprehensive framework for addressing cyber threats (NITDA, 2020). Although they indicate an effort to establish cybersecurity, research shows that implementation and enforcement are uneven across countries (Karake et al., 2019). Translating policy intentions into concrete cybersecurity outcomes remains a difficult task. This is largely due to resources but also to the need for on-going capacity-building (Calderaro & Craig, 2020).

b) Public-Private Collaboration

There has been formation of initiatives in developing countries dedicated to promoting information sharing, best practices, and collaborative responses to cyber threats. In countries such as Brazil and South Africa, the establishment of industry-specific Information Sharing and Analysis Centers (ISACs) has helped organizations share information about sectorial threats (Pala & Zhuang, 2019; Brand et al., 2022), but the focus of inter-agency cooperation is in fact likely to be prevented by obstacles such as information hoarding, a lack of trust, and a reluctance to share incidents publicly (Koepke, 2017). Overcoming these difficulties is an important step toward creating a more resilient and cooperative cybersecurity environment.

c) Capacity-Building and Cybersecurity Education

Today, the current cyber security scene in developing countries includes capacity-building projects and cybersecurity education programs. The lack of skilled cybersecurity personnel is understood now, and governments and organizations are investing in training programs to raise the capabilities of their workforce. The African Union's African Cybersecurity Resource Center (ACRC), for instance, provides training, research, and collaboration opportunities across the continent (African Union Commission, 2021). Also, institutions of learning in countries like Malaysia have begun to establish dedicated cybersecurity programs as demand for qualified staff increases (Dioubate & Wan Daud, 2022; Catota et al., 2019). However, even with these efforts, scalability and access to cybersecurity education remain a huge challenge. According to Foley et al., 2017, cybersecurity needs to be integrated into an overarching approach that includes it in a wide variety of educational courses. De Salins, (2023) stressed the need to reskill and upskill the existing workforce. The most successful cybersecurity skills development programs combine formal education, such as university programs, with lifelong learning opportunities. For example, in Nigeria, the CyberSafe Foundation launched the CyberGirls Fellowship, a seven-month cybersecurity training program for women aged 18 to 28. The initiative, which spans 22 African countries, aims to provide participants from underserved areas with critical cybersecurity skills. The program began small but is rapidly expanding, with 1,000 students expected by 2024. Donations and partnerships with the private sector help to fund the fellowship (De Salins, 2023).

RESEARCH METHODOLOGY

This research adopted a methodical literature review to analyse the research on the cyber security implementation in developing countries. The research considers papers in scholarly articles, conference papers, and reports on opportunities and barriers to implementing cyber security published between 2013 and 2024. The researchers also consider emerging technologies for applying security solutions, and historical development notes. Studies dealing with opportunities and obstacles, developing technology, or historical evolution are given priority in this study. Exclusion criteria are literature outside the time frame, studies of developed countries only, and sources not containing any empirical or theoretical value.

1.3 Vulnerabilities and Threats

While developing countries make strides in enhancing cybersecurity practices, they remain susceptible to a diverse range of vulnerabilities and threats. The current threat landscape underscores the need for continuous vigilance and adaptive strategies to mitigate emerging risks. The following are the various vulnerabilities and threats as identified by researchers

a) Financial Cyber Threats

Financial institutions in developing countries are prime targets for cybercriminals due to the increasing digitization of financial services. The vulnerabilities associated with online banking, digital payment systems, and inadequate cybersecurity measures make these institutions susceptible to various threats. Studies reveal a surge in financial cyber threats, including phishing attacks, Ransomware, and online fraud, in developing nations and a report by INTERPOL (2023) provides an in-depth analysis and insight into the most recent cyber threat landscape confronting African member countries. As technology advances, so do criminals' methods for exploiting vulnerabilities in networks and systems. As African countries become more reliant on digital services, there has been an increase in cyber-attacks targeting critical infrastructure, financial institutions, and other organizations. The lack of robust cybersecurity infrastructure and financial literacy exacerbates the impact of these threats, posing challenges to economic stability and consumer trust.

b) Critical Infrastructure Vulnerabilities

Boosted dissemination of ICTs means developing countries remain worried about what to do with their critical infrastructure. Sensitive areas such as energy, transportation, and healthcare are especially vulnerable. A simple burst of steam or a plug pulled on an engine could easily bring the most advanced nation to its knees; services can be interrupted in the blink of an eye through some sort of hacking attack. However, the world's most recent computerized catastrophe has been a cyber-attack on one of Nigeria's biggest oil pipelines (Jaiyeola, 2022), which shows how vulnerable many infrastructures still are. Since investment in cybersecurity is not keeping pace with the rapid proliferation of information technology and all types of systems, the enemy has been able to successfully attack supposedly critical information nodes.

c) Emerging Technologies and IoT Risks

In developing countries, the use of emerging technologies, such as the Internet, the Internet of Things (IoT), and so on, brings opportunities and threats. These technologies bring transformative benefits but also open up new attack surfaces and vulnerabilities. Studies stress the need to develop effective preventive cybersecurity strategies in the face of the dangers presented by IoT devices (Yaqoob et al., 2017). Insufficient regulation and understanding add to the risk of abuse of the vulnerabilities in such technologies, compromising the integrity of data and the privacy of users.

d) State-Sponsored Cyber Threats

Amid this, developing countries are caught up in geopolitical cyber conflicts. They are being subjected to state-sponsored cyber threats. But, as cyber warfare changes shape, so do the incidents where developing nations find themselves unwitting battlegrounds in a conflict between two major powers. For instance, a state-sponsored cyber-weapon like Stuxnet attacked crucial components of Iran's nuclear facilities but also hit computer systems around the world, including many in developing countries (Lindsay, 2013). Incidents can also cause collateral damage that attests to the interdependent threat of cybercrimes and calls for international cooperation.

1.4 Opportunities for Cybersecurity in Developing Countries

With advancement in emerging technology, there are boundless opportunities for developing countries to improve their cybersecurity. These technologies present new problems but also innovative solutions and strategic advantages. These technologies are:

a) Blockchain Technology

Developing countries may be able to improve their cybersecurity through the use of blockchain technology, which is decentralized and hard to tamper with. According to studies, the use of blockchain may resolve problems such as data integrity, secure trading, and the prevention of tampering with information (Mougayar, 2016). Integrating blockchain into heavy-use sectors such as finance and healthcare would help to establish a digital architecture that is more robust (Haleem et al., 2021; Weerawarna et. al., 2023), such as the case of land record systems in Ghana, where the application of blockchain has proved effective at reducing fraud and improving data quality (Allen et al., 2021; Ameyaw & de Vries, 2020; Khalid et al., 2024). What this application shows us is that even developing countries can use evolving technologies to safeguard their critical systems.

b) Artificial Intelligence (AI) and Machine Learning (ML)

Cybersecurity tools that combine AI and ML are service-adaptive, offering a proactive defence against ever-changing threats. However, these technologies can be used by developing countries to automate the process of threat detection, perform large-scale data searches for anomalies, and reduce incident response time. AI has potential applications in the field of cyberspace security, according to research; for instance, machine learning algorithms can identify viruses in network data (Shone et al., 2018; Verma & Sharma, 2021). These technologies enable developing nations with limited resources to better detect and contain cyber threats.

To strengthen countries cybersecurity capacities, international cooperation and assistance are necessary steps. Capability enhancement under the auspices of such international organizations as the United Nations (UN) and the International Telecommunication Union (ITU) in capacity - building programs has enabled the resilience of developing countries in cybersecurity. The training, knowledge-sharing, and best practices developed under these programs are nationally tailored (ITU, 2019). The ITU's Global Cybersecurity Index (GCI), which provides benchmarking, helps countries measure their degree of cyber readiness and encourages them to develop a culture of continuous improvement. These efforts help transfer knowledge and resources to developing nations, enhancing their capacity and ability in cybersecurity.

Furthermore, regional and international platforms for cybersecurity cooperation create a space in which information can be exchanged, threat intelligence shared jointly, and incidents responded to collectively. The Commonwealth Cyber Declaration and the African Union Convention on Cyber Security and Personal Data Protection are examples of joint efforts by nations to counter cyber security threats in a collective fashion (Commonwealth, 2018). Azmi et al. (2018) stressed in their study that it is important to create an atmosphere that promotes openness and the sharing of information between nations if cyber threats are going to be combated appropriately. Under these cooperative frameworks, developing countries use shared abilities and resources to enhance their cybersecurity resilience.

Lastly, aided by financial assistance from developed nations and international organizations, cybersecurity infrastructure investment is on the rise. It has been shown from studies that developing countries need both financial assistance and technical capabilities if they are to establish reliable cybersecurity frameworks (Oyeniyi et al., 2024). One of the most important contributions by non-governmental actors to improving capabilities has been financial backing from the World Bank for various cybersecurity projects in developing countries, such as establishing National Computer Emergency Response Teams (CIRT) (World Bank, 2023). As a kind of support to help overcome resource constraints and promote sustainable cybersecurity development, this is very important.

1.5 Barriers to Cybersecurity Implementation

Socio-economic factors play a major role in the successful implementation of effective cybersecurity measures by developing countries (Vasiu, 2020). These include differences in income, education, and digital proficiency, which pose problems finding a good fit among personnel capable of building resilient cybersecurity structures.

Secondly, unequal access to technology and the internet aggravates cybersecurity worries in developing nations, making up what is known as a digital divide. According to the study by Khan et al. (2023), insufficiently available digital resources and education are huge obstacles to developing a cybersecurity-conscious population. This lack of access itself engenders a greater degree of vulnerability, since many people in the population remain unaware of the best practices for cyber security or utilize unsafe products and services. To bridge the digital divide, a comprehensive strategy is necessary, involving attention not only to building communications networks but also educational efforts and directed social awareness programs. Grasping this gap is thus of vital importance to creating a more public-friendly cybersecurity culture in developing countries.

Furthermore, economic constraints and resource limitations is a critical barrier to cybersecurity. From its high cost to the economic constraints involved, investing in adequate cybersecurity infrastructure and training programs is a difficult task, as financial constraints hamper implementation. In studies related to the cybersecurity of developing countries, it is pointed out that financial resources are lacking for developing countries to enhance their usage of advanced information security systems or conduct regular security audits (Catota et al., 2018). Without the financial means to implement thorough cybersecurity requirements, developing countries small and medium-sized enterprises (SMEs) act like a buffet for all manner of cybercriminals (Kabanda et al., 2018). Cybersecurity initiatives will need targeted investment, public-private partnership arrangements, and creative funding models to integrate with the reality of the situation.

In developing countries, the lack of a strong cybersecurity infrastructure is one obvious obstacle to securing digital assets. A study by Malatji et al. (2021) points to the inefficiencies and gaps created by not having a dedicated cybersecurity framework or resources available, which leads to critical sectors being vulnerable. For example, it has been emphasized that the lack of complete cybersecurity policies and guidelines in other developing countries' healthcare sectors is one reason such organizations are more susceptible to cyber threats (He et al., 2020), and the infrastructure construction representing proper resource allocation calls for strategic planning, investment, and collaboration with international partners using expertise and personnel. At the same time, shortage of well-qualified cybersecurity professionals also poses a critical obstacle to securing digital assets.

The increasingly rapid shifts in forms of attack make it imperative that the workforce be updated with current knowledge. Yet such global shortages of skilled cybersecurity personnel make it difficult for most developing countries to attract and retain skilled talent (John et al., 2020). Such efforts to solve the skills gap include establishing cybersecurity education programs and certifications, as well as working together with industry experts. Nevertheless, it requires continued effort to resolve the shortage and establish a skilled labour force. The global shortage of skilled cybersecurity professionals has reached an all-time high in 2023, with approximately 4 million vacancies; the cybersecurity skills gap is rapidly expanding, particularly in developing countries, and according to LinkedIn data from 2022, the number of job postings for cybersecurity roles increased by 76% in Brazil and 55% in Indonesia, compared to a 35% increase globally (De Salins, 2023).

Cybersecurity implementation is also hampered by policy gaps, inconsistent regulations, and inadequate legal frameworks. As cybercrime increases, it also reflects the out-dated or defective nature of many governments in developing countries, as their laws are often old-fashioned and not up-to-date with new threats, so that law enforcement agencies can only lie around and do nothing. In Africa, Ajayi's (2016) study on cybercrime legislation in selected African countries revealed differences in definitions of cyber offenses. This creates problems with respect to cross-border cooperation and extradition. Such strengthening is a complex undertaking that involves a comprehensive review of legal frameworks, incorporating them with international standards, and constant revisions in light of the threats' continual evolution. Therefore, cybersecurity implementation must be a collective effort by government agencies, private enterprises, and other concerned parties. According to the study by Chaudhary et al. (2018), a lack of mechanisms for coordinating and sharing information prevents a rapid reaction to cyber threats. In some developing countries, various ministries and bureaux are in charge of different facets of cybersecurity, making it difficult to take a unified response. To overcome policy and regulatory obstacles, national cybersecurity strategies are needed that encourage collaboration, information sharing, and joint incident response.

Lastly, cybersecurity awareness and practice are closely related to culture and education. Amankwa (2021) notes that there is a need for culturally adapted cybersecurity education and insists upon the teaching of cybersecurity across all levels of educational curricula from an early age. The ways people regard technology and cybersecurity themselves affect secure practice adoption. Research shows that cultural considerations, whether it is a stick finger or preference for oral communication over digital channels, can result in the partial effectiveness of cybersecurity awareness campaigns (Jeong et al., 2021; Willie, 2023). Cultivating a cybersecurity culture is key, it means tailoring education to take account of cultural characteristics and differences. Cybersecurity education in developing nations' educational institutions often lacks special cybersecurity curricula and materials (Catota et al., 2019). This lack of talent is a major inhibition for training a workforce skilled at meeting emerging types of cyber threats.

DISCUSSION AND FINDINGS

Looking across the literature on cybersecurity in developing countries allows for multifaceted insights that are crucial to understanding the current state of things. Historical development, early government initiatives to ensure security, the evolution of cyber threats targeting the financial industry, and critical infrastructure are among the major findings. In fact, the practices of current cybersecurity already indicate that governments are increasingly recognizing its importance. These include promoting public-private collaboration and capacity-building. In particular, vulnerabilities remain in the financial sector and critical infrastructure. There are opportunities with emerging technologies and international cooperation.

The rise of financial cyber threats is one; public-private partnerships and the strategic importance of cybersecurity are others. There are differences in the degree of maturity of cybersecurity policy practices among developing countries, and different sorts of socio-economic factors also come into play. Cybersecurity policies can be more or less successful in their application as well. Patterns include such examples as new technologies, international cooperation, and strategies being organized around them; cybersecurity initiatives based on educational levels, gender, or cultural background, dividing people into different categories.

1.6 Implications of Findings

This section of the findings directly tackles the research problem of cybersecurity in developing countries, providing a full picture of opportunities and obstacles. However, the way governments are responding is largely based on their early initiatives. The changing threat landscape, therefore, requires additional adaptive responses. This clearly suggests that what is needed is comprehensive approaches, taking account of economic, infrastructural, and cultural factors.

These results are important in that they point to the special problems faced by developing countries. Three factors - the digital divide, economic constraints, and the changing character of cyber threats to a significant extent determine today's cyber security landscape. The developing world's immediate interests lie in the opportunities for emergent technologies and international cooperation, which can lead in the direction of more cybersecurity resilience; that is, reinforcing national security also means bolstering economic stability.

1.7 Theoretical and Practical Contributions

This research has helped to fill the gaps in previous studies by integrating fragmented perspectives on cybersecurity in less developed nations. It brings historical contexts to bear, setting the crucial links between past crises and their relation to current problems into an integrative perspective that covers every aspect of a perplexing reality.

From the perspective of policymakers, tackling socio-economic factors through legally conceived and child-centred targeted educational efforts, public-private cooperation, and an innovative funding model is critical. Using cutting-edge technology and taking an international approach can boost organizations' cybersecurity capabilities, while scholars can also see how culture relates to the way human beings experience cybersecurity education and develop tests for concrete situations in developing nations with regard to emerging technologies. These practical recommendations are aimed at guiding stakeholders toward more relevant and effective cybersecurity strategies in the specific contexts in which they live.

LIMITATIONS

Although the literature review approach is comprehensive, the selected literature may be biased. The omission of non-English sources creates a language bias, and the heavy reliance on existing literature may not pick up every aspect of cyber security in developing countries. Furthermore, the review's scope may not reflect the rapidly changing nature of the cybersecurity environment.

CONCLUSION AND FUTURE RESEARCH

This paper examines the development history of cybersecurity in developing countries, its present situation, opportunities, and obstacles. It notes the critical work to be done in the field of cybersecurity to deal with the digital gap between advanced and developing countries, the risk facing critical infrastructures, and the rise of cyberattacks against the financial industry. The paper also stresses the importance of government efforts, public-private joint efforts, and capacity- building programs in order to overcome these challenges. Emerging technologies such as blockchain and artificial intelligence are creating opportunities for improving the level of cybersecurity. Yet a variety of obstacles, such as social-economic factors, a lack of infrastructure, policy considerations, and cultural differences, all make this a daunting task. The paper provides government officials, organizations, and researchers with practical advice, highlighting such points as the importance of investment in education, the need to make full use of emerging technologies, and the value of international cooperation.

Leaving researchers with many questions: So future research could consider the effects of cultural and educational background, over the long term, on people's practices in the area of cybersecurity. How, over time, do they change and turn into something else? Investigating in more depth the efficacy of new technologies in individual sectors, allowing for cultural idiosyncrasies, will all lead to practical results. Furthermore, evaluating where international cooperation efforts have run up against an end-wall and the natures of various areas inside the region and how they have affected the development of the cybersecurity environment is essential to understand future obstacles and opportunities.

REFERENCES

[1] Acharya, S., & Joshi, S. (2020). Impact of cyber-attacks on banking institutions in india: A study of safety mechanisms and preventive measures. Palarch's Journal of Archaeology of Egypt/Egyptology, 17(6), 4656–4670.

[2] African Union Commission. (2021). African Union Convention on Cyber Security and Personal Data Protection | African Union. Au.int. Retrieved from: https://au.int/en/treaties/african-union-convention-cyber- security-and-personal-data-protection (Accessed June 10, 2024).

[3] Ajayi, E. F. G. (2016). Challenges to enforcement of cyber-crimes laws and policy. Journal of Internet and Information Systems, 6(1), 1–12. https://doi.org/10.5897/jiis2015.0089.

[4] Allen, D. W. E., Berg, C., Davidson, S., & Potts, J. (2021). Property Rights, Knowledge Commons, and Blockchain Governance. Cambridge University Press EBooks, 159–175. https://doi.org/10.1017/9781108692915.008.

[5] Amankwa, E. (2021). Relevance of Cybersecurity Education at Pedagogy Levels in Schools. Journal of Information Security, 12(4), 233–249. https://doi.org/10.4236/jis.2021.124013.

[6] Ameyaw, P. D., & de Vries, W. T. (2020). Transparency of Land Administration and the Role of Blockchain Technology, a Four-Dimensional Framework Analysis from the Ghanaian Land Perspective. Land, 9(12), 491. https://doi.org/10.3390/land9120491.

[7] Azmi, R., Tibben, W., & Win, K. T. (2018). Review of cybersecurity frameworks: context and shared concepts. Journal of Cyber Policy, 3(2), 258–283. https://doi.org/10.1080/23738871.2018.1520271.

[8] Bits IO Inc. (2024). The Impact Of Cybersecurity Threats And Cybercrime On Businesses. *Bits IO Inc*, *4*(2), 1361–1382. https://www.bitsioinc.com/cybercrime-impact-on-businesses/

[9] Brand, D., Singh, J. A., McKay, A. G. N., Cengiz, N., & Moodley, K. (2022). Data sharing governance in sub-Saharan Africa during public health emergencies: Gaps and guidance. South African Journal of Science, 118(11/12), 1–6. https://doi.org/10.17159/sajs.2022/13892.

[10] Burt, A. (2023). The Digital World Is Changing Rapidly. Your Cybersecurity Needs to Keep Up. Harvard Business Review. Retrieved from: https://hbr.org/2023/05/the-digital-world-is-changing-rapidly-your-cybersecurity-needs-to-keep-up (Accessed June 10, 2024).

[11] Business-Ghana. (2018). Bank of Ghana launches Cyber Security Directive for Financial Institutions. Business Ghana. Retrieved from: https://www.businessghana.com/site/news/business/175019/Bank-of-Ghana-launches-Cyber-Security-Directive-for-Financial-Institutions (Accessed June 10, 2024).

[12] Calderaro, A., & Craig, A. J. S. (2020). Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. Third World Quarterly, 41(6), 917–938. https://doi.org/10.1080/01436597.2020.1729729.

[13] Catota, F. E., Morgan, M. G., & Sicker, D. C. (2018). Cybersecurity incident response capabilities in the Ecuadorian financial sector. Journal of Cybersecurity, 4(1). https://doi.org/10.1093/cybsec/tyy002.

[14] Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: the Ecuadorian environment. Journal of Cybersecurity, 5(1). https://doi.org/10.1093/cybsec/tyz001.

[15] Chaudhary, T., Jordan, J., Salomone, M., & Baxter, P. (2018). Patchwork of confusion: the cybersecurity coordination problem. Journal of Cybersecurity, 4(1). https://doi.org/10.1093/cybsec/tyy005.

[16] Christensen, K. K., & Petersen, K. L. (2017). Public–private partnerships on cyber security: A practice of loyalty. International Affairs, 93(6), 1435–1452. https://doi.org/10.1093/ia/iix189.

[17] Commonwealth. (2018). Commonwealth Cyber Declaration, 2018. Retrieved from: https://thecommonwealth.org/commonwealth-cyber-declaration-2018 (Accessed June 10, 2024).

[18] Dave, D., Sawhney, G., Aggarwal, P., Silswal, N., & Khut, D. (2023). The New Frontier of Cybersecurity: Emerging Threats and Innovations. Retrieved from: https://arxiv.org/ftp/arxiv/papers/2311/2311.02630.pdf (Accessed July 15, 2024).

[19] De Salins Anat Lewin, G., & De Salins Anat Lewin, G. (2023, November 27). *"Hacking" the cybersecurity skills gap in developing countries*. World Bank Blogs. https://blogs.worldbank.org/digital- development/hacking-cybersecurity-skills-gap-developing-countries (Accessed July 10, 2024).

[20] Dilipraj, E. (2014). India's cyber security 2013: A review. Retrieved from: http://capsindia.org.managewebsiteportal.com/files/documents/CAPS_IB_01FEB-2014.pdf (Accessed July 12, 2024).

[21] Dioubate, B. M., & Wan Daud, W. N. (2022). A Review of Cybersecurity Risk Management Framework in Malaysia Higher Education Institutions. International Journal of Academic Research in Business and Social Sciences, 12(5). https://doi.org/10.6007/ijarbss/v12-i5/12924.

[22] Fatoki, J. O. (2023). The influence of cyber security on financial fraud in the Nigerian banking industry. International Journal of Science and Research Archive, 9(2), 503–515. https://doi.org/10.30574/ijsra.2023.9.2.0609.

[23] Finkle, J. (2016, April 25). Exclusive - Bangladesh Bank hackers compromised SWIFT software; warning issued. Retrieved from: https://www.reuters.com/article/us-usa-nyfed-bangladesh-malware-exclusiv-idUSKCN0XM0DR/ (Accessed June 10, 2024).

[24] Foley, M., Dewey, L., Williamson, S., Blackman, D., Creagh, A., Davidson, L., Zhu, M., & Slay, J. (2017). Women in cyber security literature review. Retrieved from: https://apo.org.au/node/105276 (Accessed July 12, 2024).

[25] Haleem, A., Javaid, M., Singh, R. P., Suman, R., & Rab, S. (2021). Blockchain Technology Applications in Healthcare: An Overview. International Journal of Intelligent Networks, 2(2), 130–139. https://doi.org/10.1016/j.ijin.2021.09.005.

[26] Hammer, J. (2018, May 3). The Billion-Dollar Bank Job. The New York Times. Retrieved from: https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html (Accessed August 23, 2024).

[27] He, Y., Aliyu, A., Evans, M., & Luo, C. (2020). Healthcare Cyber Security Challenges and Solutions Under the Climate of COVID19: A Scoping Review (Preprint). Journal of Medical Internet Research, 23(4). https://doi.org/10.2196/21747.

[28] Hurel, L., & Lobato, L. (2018). A Strategy for Cybersecurity Governance in Brazil. Retrieved from: https://igarape.org.br/wp-content/uploads/2019/01/A-Strategy-for-Cybersecurity-Governance-in-Brazil.pdf (Accessed August 23, 2024).

[29] INTERPOL. (2023). African Cyberthreat Assessment Report 2023 African Cyberthreat Assessment Report Cyberthreat Trends. March.

[30] ITU. (2019). Global Cybersecurity Index. International Telecommunication Union. Retrieved from: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (Accessed August 23, 2024).

[31] Jaiyeola, T. (2022, November 24). Hackers attack 39% Nigeria's oil sector computers – Report. Punch Newspapers. Retrieved from: https://punchng.com/hackers-attack-39-nigerias-oil-sector-computers-report/ (Accessed December 23, 2024).

[32] Javaid, D. M., Haleem, Prof. A., Singh, D. R. P., & Suman, D. R. (2023). Towards in sighting Cybersecurity for Healthcare domains: A comprehensive review of recent practices and trends. Cyber Security and Applications, 1, 100016. https://doi.org/10.1016/j.csa.2023.100016.

[33] Jeong, J. J., Oliver, G., Kang, E., Creese, S., & Thomas, P. (2021). The current state of research on people, culture and cybersecurity. Personal and Ubiquitous Computing. https://doi.org/10.1007/s00779-021-01591-8.

[34] John, S. N., Noma-Osaghae, E., Oajide, F., & Okokpujie, K. (2020). Cybersecurity Education: The Skills Gap, Hurdle! Innovations in Cybersecurity Education, 361–376. https://doi.org/10.1007/978-3-030-50244-7_18.

[35] Joseph, S., & Fred, W. (2023). Cybersecurity in the Digital Age: Protecting Information and Systems. *OSF Preprints*, 47. https://osf.io/preprints/osf/9bxcz

[36] Juneja, A., Goswami, S. S., & Mondal, S. (2024). Cyber Security and Digital Economy: Opportunities, Growth and Challenges. *Journal of Technology Innovations and Energy*, *3*(2), 1–22. https://doi.org/10.56556/jtie.v3i2.907

[37] Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. Journal of Organizational Computing and Electronic Commerce, 28(3), 269–282. https://doi.org/10.1080/10919392.2018.1484598.

[38] Karake, Z., Shalhoub, R., & Ayas, H. (2019). Enforcing Cybersecurity in Developing and Emerging Economies. Edward Elgar Publishing. https://doi.org/10.4337/9781785361333.

[39] Kawalec, A. (2021). Council Post: Tech Has Advanced Rapidly - And Cybersecurity Needs to Catch Up. Forbes.

Retrieved from: https://www.forbes.com/sites/forbestechcouncil/2021/06/21/tech-has-advanced- rapidly-and-cybersecurity-needs-to-catch-up/?sh=4cdef143acba (Accessed August 23, 2024).

[40] Khalid, M. I., Iqbal, J., Alturki, A., Hussain, S., Alabrah, A., & Ullah, S. S. (2022). Blockchain-Based Land Registration System: A Conceptual Framework. Applied Bionics and Biomechanics, 2022, 1–21. https://doi.org/10.1155/2022/3859629.

[41] Khan, N. F., Ikram, N., & Saleem, S. (2023). Effects of socioeconomic and digital inequalities on cybersecurity in a developing country. Security Journal. https://doi.org/10.1057/s41284-023-00375-4.

[42] Koepke, P. (2017). Cybersecurity Information Sharing Incentives and Barriers. Retrieved from: https://cams.mit.edu/wp-content/uploads/2017-13.pdf (Accessed August 23, 2024).

[43] Krause, T., Ernst, R., Klaer, B., Hacker, I., & Henze, M. (2021). Cybersecurity in Power Grids: Challenges and Opportunities. Sensors, 21(18), 6225. https://doi.org/10.3390/s21186225.

[44] Khadam, N., Anjum, N., Alam, A., Ali Mirza, Q., Assam, M., Ismail, E. A. A., & Abonazel, M. R. (2023). How to punish cyber criminals: A study to investigate the target and consequence based punishments for malware attacks in UK, USA, China, Ethiopia & Pakistan. *Heliyon*, *9*(12), e22823. https://doi.org/10.1016/j.heliyon.2023.e22823

[45] Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments. Energy Reports, 7(7), 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126.

[46] Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. Security Studies, 22(3), 365–404. https://doi.org/10.1080/09636412.2013.816122

[47] Madnick, B., Huang, K., & Madnick, S. E. (2023). The evolution of global cybersecurity norms in the digital age: A longitudinal study of the cybersecurity norm development process. Information Security Journal: A Global Perspective, 1–22. https://doi.org/10.1080/19393555.2023.2201482.

[48] Malatji, M., Marnewick, A. L., & Von Solms, S. (2021). Cybersecurity capabilities for critical infrastructure resilience. Information & Computer Security, 30(2). https://doi.org/10.1108/ics-06-2021-0091.

[49] Markopoulou, D., & Papakonstantinou, V. (2021). The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular. Computer Law & Security Review, 41, 105502. https://doi.org/10.1016/j.clsr.2020.105502.

[50] Marr, B. (2023). The 10 Biggest Cyber Security Trends In 2024 Everyone Must be Ready for Now. Forbes. Retrieved from: https://www.forbes.com/sites/bernardmarr/2023/10/11/the-10-biggest-cyber-security-trends- in-2024-everyone-must-be-ready-for-now/?sh=70a1694a5f13 (Accessed August 23, 2024).

[51] Ministry of Electronics and Information Technology, Government of India. (2013). National Cyber Security Policy 2013. Retrieved from: https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf (Accessed August 23, 2024).

[52] Mougayar, W. (2016). The Business blockchain: promise, practice, and application of the next internet technology. John Wiley & Sons.

[53] Muniandy, M., Ismail, N. A., Yahya Al-Nahari, A. Y., & Yao, D. N. L. (2024). Evolution and Impact of Ransomware: Patterns, Prevention, and Recommendations for Organizational Resilience. *International Journal of Academic Research in Business and Social Sciences*, *14*(1), 585–599. https://doi.org/10.6007/ijarbss/v14-i1/19803

[54] NITDA. (2020). National cybersecurity policy 2020. National Information Technology Development Agency. Retrieved from: https://nitda.gov.ng/ (Accessed August 23, 2024).

[55] Ogugua Chimezie Obi, Onyinyechi Vivian Akagha, Samuel Onimisi Dawodu, ` A. C. A., Shedrack Onwusinkwue, & ` I. A. I. A. (2024). Comprehensive Review on Cybersecurity: Modern Threats and Advanced Defense Strategies. *Computer Science & IT Research Journal*, *5*(2), 293–310. https://doi.org/10.51594/csitrj.v5i2.758

[56] Oktavianus, A., Mahani, I., & Meifrinaldi, M. (2018). A Global Review of Public Private Partnerships Trends and Challenges for Social Infrastructure. MATEC Web of Conferences, 147, 06001. https://doi.org/10.1051/matecconf/201814706001.

[57] Ospina, J., Liu, X., Konstantinou, C., & Dvorkin, Y. (2021). On the Feasibility of Load-Changing Attacks in Power Systems During the COVID-19 Pandemic. IEEE Access, 9, 2545–2563. https://doi.org/10.1109/access.2020.3047374.

[58] Oyeniyi, L. D., Ugochukwu, C. E., Mhlongo, N. Z., Bank, B., Kingdom, U., Researcher, I., Power, C., & Africa, S. (2024). *Developing cybersecurity frameworks for financial institutions : a comprehensive review and best practices*. *5*(4), 903–925. https://doi.org/10.51594/csitrj.v5i4.1049

[59] Paquet-Clouston, M., Décary-Hétu, D., & Bilodeau, O. (2018). Cybercrime is whose responsibility? A case study of an online behaviour system in crime. *Global Crime*, *19*(1), 1–21. https://doi.org/10.1080/17440572.2017.1411807

[60] Pala, A., & Zhuang, J. (2019). Information Sharing in Cybersecurity: A Review. Decision Analysis, 16(3), 172–196. https://doi.org/10.1287/deca.2018.0387.

[61] Priyandita, G., Hogeveen, B., & Stevens, B. (2022). Policy Brief State-sponsored economic cyber-espionage for commercial purposes Tackling an invisible but persistent risk to prosperity. Retrieved from: https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2022-12/State-sponsored%20economic%20cyber-espionage_0.pdf (Accessed August 23, 2024).

[62] Putter, D., & Bachmann, S.-D. (Dov). (2022). South Africa needs stronger security in place to stop the sabotage of its power supply. Retrieved from: https://theconversation.com/south-africa-needs-stronger-security-in-place-to-stop-the-sabotage-of-its-power-supply-187889 (Accessed August 23, 2024).

[63] Reed, J. (2023, June 26). High-impact attacks on critical infrastructure climb 140 Retrieved from: https://securityintelligence.com/news/high-impact-attacks-on-critical-infrastructure-climb-140/ (Accessed August 23, 2024).

[64] Reveron, D. S., & Savage, J. E. (2020). Cybersecurity Convergence: Digital Human and National Security. Orbis, 64(4), 555–570. https://doi.org/10.1016/j.orbis.2020.08.005.

[65] Rowe, B. (2019). Transnational State-sponsored Cyber Economic Espionage: A Transnational State-sponsored Cyber Economic Espionage: A Legal Quagmire Legal Quagmire. Retrieved from: https://digitalcommons.tamusa.edu/cgi/viewcontent.cgi?article=1010&context=crim_faculty (Accessed August 23, 2024).

[66] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A Deep Learning Approach to Network Intrusion Detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41–50. https://doi.org/10.1109/tetci.2017.2772792.

[67] Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review. Sensors, 23(8). https://doi.org/10.3390/s23084117.

[68] The Indian Express. (2017, February 21). India launches "Cyber Swachhta Kendra" to protect citizens. Retrieved from: https://indianexpress.com/article/india/india-launches-cyber-swachhta-kendra-to-protect-citizens-4536440/ (Accessed August 23, 2024).

[69] Trinkunas, H., & Wallace, I. (2015). Converging on the Future of Global Internet Governance the United States and Brazil. Retrieved from: https://www.brookings.edu/wp-content/uploads/2016/06/USBrazil-Global-Internet-Governance-web-final.pdf (Accessed August 23, 2024).

[70] Uddin, Md. H., Ali, Md. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. Risk Management, 22, 239–309. https://doi.org/10.1057/s41283-020-00063-2.

[71] Ulrich, J. (2023). Cybersecurity In Finance: Protecting Client Data and Mitigating Risks. Retrieved from: https://www.forbes.com/sites/forbesfinancecouncil/2023/09/11/cybersecurity-in-finance-protecting-client-data-and-mitigating-risks/?sh=5356db413c51 (Accessed August 23, 2024).

[72] Vasiu, I. (2020). *Cybersecurity as an Essential Sustainable Economic Development Factor Cybersecurity as an Essential Sustainable Economic Development Factor*. *September 2018*. https://doi.org/10.14207/ejsd.2018.v7n4p171

[73] Verma, A. K., & Sharma, S. K. (2021). Malware Detection Approaches using Machine Learning Techniques-Strategic Survey. IEEE Xplore, 1958–1962. https://doi.org/10.1109/ICAC3N53548.2021.9725369.

[74] Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. International Journal of Law, Crime and Justice, 62, 100415. https://doi.org/10.1016/j.ijlcj.2020.100415.

[75] Weerawarna, R., Miah, S. J., & Shao, X. (2023). Emerging advances of blockchain technology in finance: a content analysis. Personal and Ubiquitous Computing. https://doi.org/10.1007/s00779-023-01712-5.

[76] Wiggen, J. (2020). The impact of COVID-19 on cybercrime and state-sponsored cyber activities. In JSTOR. https://www.jstor.org/stable/resrep25300.

[77] Willie, M. M. (2023). The Role of Organizational Culture in Cybersecurity: Building a Security-First Culture. Social Science Research Network. https://doi.org/10.2139/ssrn.4564291.

[78] World Bank. (2023). Supporting Countries in Building Cybersecurity and Resilience of Critical Infrastructure. World Bank. Retrieved from: https://www.worldbank.org/en/programs/kodi/brief/supporting- countries-in-building-cybersecurity-and-resilience-of-critical-infrastructure (Accessed June 03, 2024).

[79] Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations. *International Journal of Information Security*, *21*(1), 115–158. https://doi.org/10.1007/s10207-021-00545-8

[80] Yaqoob, I., Ahmed, E., Hashem, I. A. T., Ahmed, A. I. A., Gani, A., Imran, M., & Guizani, M. (2017). Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges. IEEE Wireless Communications, 24(3), 10–16. https://doi.org/10.1109/mwc.2017.1600421.