Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/

(REVIEW ARTICLE)

Check for updates

Cybersecurity in Namibia: Challenges, strategies and prospects

Iyaloo Ndapandula Waiganjo [1,*], Jude Osakwe [2] and Ambrose Azeta [2]

[1] *Faculty of Information and communications technology (ICT), International University of Management (IUM), Windhoek, Namibia.*
[2] *Faculty of Informatics, Namibia University of Science and Technology (NUST), Windhoek, Namibia*

Global Journal of Engineering and Technology Advances, 2025, 22(03), 001-008

Publication history: Received on 19 January 2025; revised on 24 February 2025; accepted on 27 February 2025

Article DOI: https://doi.org/10.30574/gjeta.2025.22.3.0048

Abstract

Africa's technological evolution has surged in recent years and is marked by impressive strides in connectivity and innovation. However, amid this progress, cybersecurity challenges persist, particularly in nations such as Namibia. This study examines Africa's cybersecurity landscape, with a focus on Namibia, to understand the current challenges and proactive efforts aimed at enhancing cybersecurity. The study draws insights from recent reports and studies to analyze Namibia's cybersecurity landscape. It explores advancements in digital infrastructure and connectivity alongside the challenges identified through global cybersecurity indices and cyber incident reports. Key focus areas include the examination of existing legislative frameworks, awareness initiatives, and vulnerabilities in critical infrastructure, as well as Namibia's efforts to address these challenges through capacity-building and international collaborations. Despite notable advancements in digital infrastructure and connectivity, Namibia faces significant cybersecurity challenges. These include the absence of comprehensive legislation, cybersecurity awareness gaps, and vulnerabilities in critical infrastructure. However, Namibia has demonstrated a proactive approach through the development of cybersecurity legislation, strategic capacity-building initiatives, and collaborations with international partners. The National Cybersecurity Strategy and Awareness Creation Plan 2022-2027 outlines strategic pillars to strengthen the country's cybersecurity framework, safeguard digital assets, and foster a resilient and secure digital environment.

Keywords: Namibia; Cybersecurity; Cyber threats; Legislation

1. Introduction

Africa's rapid technological advancement in recent years has underscored the continent's potential for innovation and growth. However, alongside this progress comes the pressing need to address cybersecurity challenges that threaten to undermine these advancements. This paper explores the cybersecurity landscape in Africa, with a specific focus on Namibia, highlighting key challenges, progress, and strategies. It begins by discussing the surge in connectivity and technological innovation across Africa, setting the stage for the discussion on cybersecurity. The paper then delves into specific challenges faced by Namibia, drawing on global cybersecurity indices, reports of cyber incidents, and legislative gaps. Subsequently, it examines Namibia's proactive initiatives to strengthen cybersecurity, including legislative developments, capacity-building efforts, and collaborative endeavors. The paper concludes by emphasizing the importance of concerted efforts and collaborative approaches in building a resilient cybersecurity ecosystem to safeguard Namibia's digital infrastructure and ensure its citizens' safety in the digital age.

2. Methodology

This study employs a qualitative literature review approach to analyze Namibia's cybersecurity landscape, focusing on challenges, progress, and strategies. The methodology involves a systematic examination of secondary data, including

* Corresponding author: Iyaloo Ndapandula Waiganjo

global cybersecurity indices, academic literature, government documents, and industry reports. Additionally, news articles and media reports are utilized to provide context on recent cyber incidents and trends. The study adopts a thematic analysis framework to identify recurring themes, such as legislative gaps, cybersecurity awareness, critical infrastructure vulnerabilities, and international collaborations. A case study approach is used to provide an in-depth analysis of Namibia's cybersecurity ecosystem, examining its digital infrastructure advancements, legislative developments, and incident response mechanisms.

3. Navigating Cyber Challenges in Africa

In recent years, Africa has witnessed remarkable progress in connectivity and technological innovation, showcasing the region's vast potential. The surge in economic growth has significantly heightened the demand for the Internet and digital services, painting a picture of a continent on the brink of a digital revolution (Sarfo, 2023). However, amidst these promising advancements, Africa's cybersecurity landscape grapples with distinctive challenges that demand attention and strategic response. Liquid C2 (2023) sheds light on a pressing concern in South Africa, where hacking is the predominant threat faced by companies, with 76% in 2022. Kenya and Zambia are not immune and are experiencing a surge in their apprehensions regarding this risk. Meanwhile, email and social engineering attacks persist as major ongoing threats across continents (Liquid C2, 2023). Kshetri (2019), stated that it becomes evident that cybercriminals are homing in on financial organisations, making them the primary target.

Between 2022 and 2023, 18% of the successful cyber-attacks were directed at these institutions. Simultaneously, telecommunication companies find themselves in crosshairs, with 13% of the attacks targeting them. This heightened threat can be attributed to their expanding customer base, making them attractive targets for data theft and extortion (Kshetri, 2019). The evolving business landscape has propelled companies to increase their reliance on digital currency, electronic data, and computer networks. This paradigm shift, as highlighted by Tariq (2018), has elevated stakes, as all-encompassing repositories of personal and financial information have become prime targets for cybercriminals. A comprehensive review by Pieterse (2021) spanning a decade underscores the gravity of the situation. Data exposure emerged as the predominant threat, constituting 39.19% of the incidents, followed closely by compromised websites (21.62%). System intrusion incidents experienced a significant surge of 14.86%, reflecting the adaptability and sophistication of cyber threats. Furthermore, cybercrime (13.51%) and denial of service attacks (10.81%) round out the landscape of threats facing organizations across the continent. As Africa embraces digital transformation, the imperative to fortify cybersecurity measures has become more pronounced. This exploration of prevailing challenges serves as a clarion call for collaborative efforts, innovative solutions, and heightened awareness to safeguard the digital future of the continent.

4. Cybersecurity Landscape in Namibia

Namibia is at the cusp of technological evolution, which is evident through its remarkable strides in digital infrastructure and connectivity. The nation boasts an impressive surge in mobile technology, with over 2.7 million subscribers embracing the convenience of mobile services. Moreover, Namibia has witnessed a commendable 52% internet penetration rate, translating to a significant user base of 1.28 million individuals actively engaging with online platforms (Waiganjo & Valungameka, 2023; NCS & Awareness Arise Plan 2022-2027). Among these users, approximately 710,000 are active on various social media platforms, showcasing the country's growing digital presence. Furthermore, the emergence of online commerce is palpable, with an estimated 76,000 individuals engaging in online shopping activities, marking a burgeoning trend in e-commerce adoption (NSC & Awareness Arise Plan 2022-2027). The country's connectivity infrastructure is a testament to its commitment to bridging the digital divide. With 3G broadband accessibility extending to 75% of the population and 4G services reaching 48% of Namibians, the nation has made significant strides in providing access to high-speed internet, even in remote areas. This effort is further accentuated by the establishment of 26 multipurpose community centers in underserved and remote regions, fostering connectivity and access to digital resources where it was once limited. However, amidst these advancements, the Global Cybersecurity Index (GCI) has unveiled a sobering reality. The GCI, which assesses countries based on key cybersecurity pillars, highlights the gap in Namibia's commitment to cybersecurity readiness. This evaluation encompasses five critical dimensions: cooperation, capacity development, organizational measures, technical measures, and legal measures. Namibia's GCI scores paint a picture of deficiency: Legal Measures stand at 2.84, technical measures and organizational Measures at 0.00 each, Capacity Development at 2.34, and cooperation at 6.30. These scores culminate in an overall GCI score of 11.47 out of 20, reflecting a notable shortfall in cybersecurity preparedness. Despite the commendable progress in digital access and infrastructure, the nation faces an urgent need to fortify its cybersecurity framework to safeguard technological advancements and the integrity of its digital ecosystem.

5. Cybersecurity Challenges in Namibia

Namibia is facing significant cybersecurity challenges. In 2017 and 2018, the Global Cybersecurity Index ranked Namibia as low, positioning it at 151 out of 165 globally and 35 out of 42 in Africa for low commitment to cybersecurity measures and awareness. Uudhila (2016) highlighted the absence of policy guidance on cyber risk management, contributing to network security challenges owing to interconnected systems. Also, there is a growing concern (44%) among organisations about cyberattacks, Deloitte's 2020 Corporate Governance Survey revealed that only 46% of Namibian organizations have a cybersecurity plan in place. This lack of prioritization or integration into existing plans leaves the majority (54%) without a specific cybersecurity strategy. Namibia witnessed a surge in cyberattacks, as evidenced by Xinhua (2022). The instances of malware targeting Namibian banks resulted in the country ranking third globally in such attacks. According to Kamutueza (Rengura, 2022), government offices have also fallen victim to cyber threats. IT outages, ransomware, data breaches, crypto mining, and mobile cyber-attacks have affected various sectors, such as education, government, and communications, posing severe threats to individuals' safety and privacy (Shipena et al., 2021). The ramifications of cyber incidents are dire, impacting data integrity, economic stability, infrastructure, individuals, and organizational reputation. Notably, a company incurs N$15 million in operational costs owing to a cyberattack. In December 2024, Namibia faced a ransomware attack on a state-owned telecommunications company, resulting in the leak of sensitive data belonging to 500,000 customers (Rukanga, 2024). The breach reportedly included information on top government officials, highlighting significant vulnerabilities in the country's cybersecurity defenses.

Waiganjo and Valungameka (2023) assessed cybersecurity awareness levels in Windhoek, the capital city of Namibia. Their research showed that Namibians had a remarkably favorable opinion on cyber awareness. This research demonstrated Namibians' awareness of cyber threats, crimes, and practical defenses. Nonetheless, Namibia continues to face significant obstacles because it lacks comprehensive cybersecurity legislation. Namibia demonstrates proactive efforts despite this legislative gap, as evidenced by the numerous initiatives and committed organizations working to strengthen cybersecurity measures in the nation.

6. Namibian Legislation and Regulation

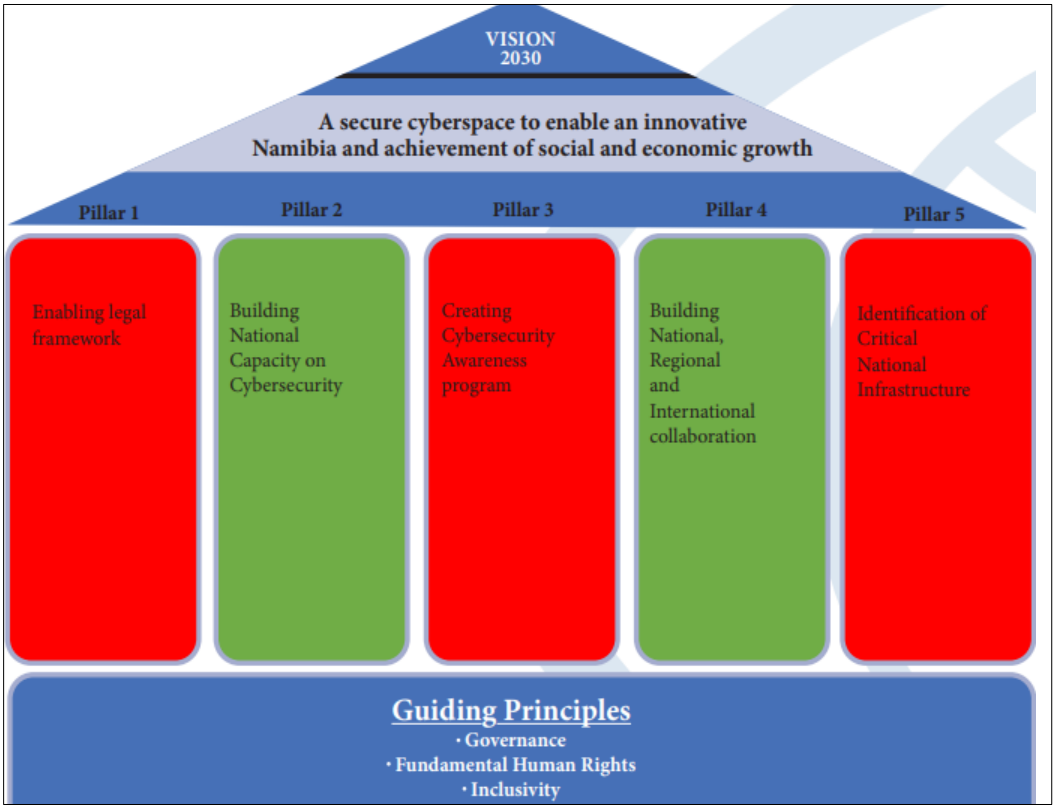

Figure 1 Cybersecurity Strategic Pillars (NCS & Awareness Arise Plan 2022-2027, 2023)

Namibia has embarked on the implementation of cybersecurity legislation and regulations. The Ministry of Information and Communication Technology (MICT) introduced the “Electronic Transactions and Cybercrime Bill" in 2013, which underwent public consultations but was withdrawn in 2017. In 2019, the bill was divided into the "Electronic Transactions Bill" (enacted in 2019) and the "Computer Security and Cybercrime Bill," the status of which remains pending due to amendments after the death of a key advocate in 2021. The NCS and Awareness Arise Plan 2022-2027, (2023) reported that, In May 2019, the World Bank, the United Kingdom Foreign Commonwealth Office, and the institutions jointly conducted an in-country mission to conduct a needs assessment, review the Cybercrime Bill and other pertinent legislation, and evaluate Namibia's cybersecurity maturity level. The mission also involved reviewing the cybersecurity landscape to identify gaps and potential vulnerabilities. Vulnerabilities were discovered during the preparation of the Cybercrime Bill. The Budapest Convention, which is regarded as the premier convention on cybercrime legislation worldwide, was not complied with by the Cybercrime Bill. The absence of a national cybersecurity strategy has led to this problem (NCS and Awareness Arise Plan 2022-2027, 2023). In February 2020, with external assistance, Namibia worked on the components of its cybersecurity strategy, aiming to align with international conventions like the Budapest Convention. The National Cybersecurity Strategy and Awareness Creation Plan 2022-2027, launched in March 2023, focuses on critical information infrastructure protection, education, information sharing, and user safety.

The strategic plan outlined for enhancing cybersecurity in Namibia encompasses five fundamental pillars, each focusing on the critical aspects imperative for fortifying the country's digital defenses and resilience against cyber threats.

6.1. Enabling Legal Framework

A comprehensive legal framework for cybersecurity is imperative to empower governments in adopting a proactive stance against various cyber threats (Mishra et al., 2022). Therefore, this pillar is dedicated to the meticulous development and revision of legislation and policies with the objective of fortifying cybersecurity measures by the year 2024. The emphasis is placed on establishing a robust legal infrastructure capable of effectively addressing evolving cyber threats, safeguarding digital assets, and furnishing law enforcement with a structured approach to combatting cybercrimes.

Presently, Namibia lacks any specific laws dealing with cybercriminals or national policies addressing cybersecurity. Hence, the primary focus of the first pillar is the establishment of such legislation, which is currently in progress. Once enacted at the national level, these laws and policies in Namibia will not only address cybercriminal activities but also provide guidance on cyber use for individuals and organisations within their jurisdiction (Lubua & Pretorius, 2019).

A comprehensive legal framework for cybersecurity is imperative to empower governments to adopt a proactive stance against cyber threats (Mishra et al. 2022). Therefore, this pillar is dedicated to the meticulous development and revision of legislation and policies with the objective of fortifying cybersecurity measures by 2024. Emphasis is placed on establishing a robust legal infrastructure capable of effectively addressing evolving cyber threats, safeguarding digital assets, and furnishing law enforcement with a structured approach to combat cybercrimes. Currently, Namibia lacks specific laws dealing with cybercriminals or national policies addressing cybersecurity. The primary focus of the first pillar is the establishment of such legislation, which is currently in progress. Once enacted at the national level, these laws and policies in Namibia will not only address cybercriminal activities but also provide guidance on cyber use for individuals and organizations within their jurisdiction (Lubua & Pretorius, 2019).

6.2. Building National Capacity on Cybersecurity

Creese et al. (2021) highlighted that numerous international organizations and governments have prioritized efforts to educate and train citizens on emerging cybersecurity threats and preventive measures, aiming to enhance national capacity in cybersecurity. More reason why Namibia put on the emphasis on establishing a dedicated National Cybersecurity Incident Response Team (NCIRT) and fostering a skilled pool of cybersecurity professionals. The NCIRT serves as a proactive unit, swiftly responding to cyber incidents, coordinating responses across sectors, and formulating cybersecurity policies and procedures. Concurrently, investing in the development of expertise within the cybersecurity realm ensures sustainable defense against evolving cyber threats.

6.3. Creating Cybersecurity Awareness

This pillar is committed to educating various stakeholders, including government officials, private sector entities, and Internet users. The goal is to raise awareness of the risks associated with cyber activities, promote safe online practices, and enlighten individuals about the potential repercussions of cyber threats. By cultivating a culture of cybersecurity consciousness, it aims to empower individuals and organizations to protect themselves against cyber-attacks.

6.4. National, Regional, and International Collaboration

Recognizing the interconnected nature of cyber threats, this pillar focuses on fostering collaboration at various levels locally, regionally, and internationally. The objective is to synchronize cybersecurity efforts, share threat intelligence, and devise collective strategies to mitigate cyber risk. Namibia aims to strengthen its cybersecurity posture through shared expertise and resources by forging alliances with other nations, regional bodies, and international organizations Namibia aims to strengthen its cybersecurity posture through shared expertise and resources.

6.5. Identification of Critical National Infrastructure

This pillar underscores the significance of identifying and safeguarding critical national infrastructure (CNIs) that are vital for societal and economic functions. This involves compiling an updated list of critical infrastructure assets and conducting comprehensive risk assessments. These assessments aid in prioritizing investments to fortify the security of these crucial assets and ensure their resilience against potential cyber threats.

The proliferation of online activities has made it possible for hackers, cybercriminals, and terrorists to target important social and governmental infrastructures, as well as valuable assets. This seriously threatens the safety and stability of cyberspace. Because critical infrastructure is the main target of these attacks, they are vulnerable to frequent and disruptive cyberthreats (Mishra et al., 2022). The importance of protecting this infrastructure stems from the fact that cybercriminals exploit the increased intricacy and interconnectedness of these networks to compromise national security, economic stability, and public health and safety. Roshanaei (2021) suggests that all countries need to recognize and develop plans to deal with different kinds of risks to their vital infrastructure, ensuring resilience in the face of potential challenges.

The collective impact of these efforts, including capacity-building initiatives, public awareness campaigns, and collaborative endeavors with international partners, has played a pivotal role in augmenting Namibia's cybersecurity landscape. These coordinated initiatives signify a multifaceted approach to fortifying defenses against cyber threats, while fostering a resilient and secure digital environment for the nation's growth and prosperity. While challenges persist, Namibia is in the right direction for growth and fortification in the cybersecurity domain. With concerted efforts, a proactive approach, and collective commitment from stakeholders across sectors, the nation is poised to build a resilient cybersecurity ecosystem that safeguards its digital infrastructure, protects its citizens, and fosters a secure and thriving digital future.

7. Recommendations for Strengthening Cybersecurity in Namibia

Cybersecurity remains a critical concern for Namibia as the country continues to advance in digital infrastructure and connectivity. Despite ongoing efforts to improve cybersecurity, challenges such as the lack of comprehensive legislation, low awareness, and vulnerabilities in critical infrastructure persist. To address these issues effectively, targeted recommendations must be directed toward the Namibian government, private organizations, and individuals.

7.1. Recommendations for the Namibian Government

The Namibian government must prioritize the establishment of a comprehensive legal framework to combat cyber threats effectively. The absence of specific cybersecurity laws has left gaps in regulation and enforcement, making it imperative to finalize and implement the Computer Security and Cybercrime Bill. Additionally, aligning Namibia’s cybersecurity policies with international frameworks such as the Budapest Convention on Cybercrime will enhance global cooperation in cyber incident response and prosecution (Ifeanyi-Ajufo, 2024; Mosimolodi, 2022). The establishment of a National Cybersecurity Incident Response Team (NCIRT) is critical. This dedicated unit should be equipped with the necessary resources and skilled personnel to respond swiftly to cyber incidents, coordinate cross-sector responses, and develop effective cybersecurity policies. Third, the government must prioritize the protection of Critical National Infrastructure (CNI), such as energy, telecommunications, health, and financial systems. These systems are indispensable to the nation’s stability and economic security, making them prime targets for cyberattacks. Effective cybersecurity resilience for CNI is non-negotiable, as the nation and its citizens heavily rely on the uninterrupted functioning of these critical infrastructures for daily operations, public safety, and economic stability (Roshanaei, 2023). A breach or disruption in these systems could have catastrophic consequences, underscoring the urgent need for robust protective measures, including regular risk assessments, advanced threat detection systems, and coordinated response strategies. By safeguarding CNI, Namibia can ensure the continuity of essential services and fortify its national security against evolving cyber threats.

Namibia needs to continue promoting cybersecurity awareness and education through nationwide campaigns and integrating cybersecurity into school curricula will foster a culture of digital safety. Finally, fostering regional and international collaboration, particularly with bodies like the Southern African Development Community (SADC) and the International Telecommunication Union (ITU), will enable Namibia to share threat intelligence, access technical expertise, and strengthen its cybersecurity posture.

7.2. Recommendations for Private Organizations

Private sector organizations must prioritize cybersecurity governance by adopting and adhering to internationally recognized frameworks, such as ISO/IEC 27001 and the NIST Cybersecurity Framework. Qudus (2025) emphasizes that when organizations integrate and adapt these frameworks, they can ensure a unified and effective response to cyber threats. Additionally, regular cyber risk assessments and vulnerability testing should be conducted to proactively identify and mitigate potential security breaches before they occur (Qudus, 2025). Organizations should implement robust cybersecurity policies that include multi-factor authentication (MFA), encryption protocols, and regular software updates to safeguard sensitive data. Waiganjo et al. (2024) emphasized that building a strong cybersecurity culture within organizations is critical to addressing these challenges, ensuring the effective implementation of cybersecurity policies, and enhancing organizational resilience against cyber threats. Additionally, investing in cybersecurity awareness training for employees is crucial, as human error remains a significant factor in cyber incidents. Employees should be trained to recognize phishing attempts, social engineering tactics, and other forms of cyber threats.

Collaboration with government and industry partners is essential for enhancing Namibia's cybersecurity resilience. Establishing public-private partnerships (PPPs) for information sharing and coordinated incident response can help mitigate large-scale cyber threats. Furthermore, businesses should establish cyber incident response teams (CIRTs) to ensure a structured approach to handling cybersecurity breaches and minimizing operational disruptions (Farok & Zolile. 2024).

7.3. Recommendations for Individuals

Cybersecurity awareness among individuals remains a fundamental component in mitigating cyber threats. (Waiganjo and Valungameka, 2023) pointed out that Namibians should adopt strong password management practices by using complex passwords and password managers to reduce the risk of credential-based attacks. While Nawa et al. (2021) explained that enabling multi-factor authentication (MFA) on online accounts can provide an added layer of security against unauthorized access.

Social engineering and phishing attacks are among the most common cyber threats targeting individuals. Therefore, public awareness campaigns should emphasize how to identify fraudulent emails, suspicious links, and fake websites (Waiganjo et al., 2024). Individuals must also be encouraged to regularly update their devices and software to patch security vulnerabilities.

With the rise in online financial transactions and e-commerce activities, individuals should exercise caution when making online payments by ensuring websites use secure encryption (HTTPS) and avoiding public Wi-Fi when conducting financial transactions (Nawa et al., 2021). Additionally, data privacy best practices, such as limiting personal information shared on social media, should be promoted to reduce exposure to identity theft and cyber fraud.

8. Conclusion

Namibia's initiative-taking efforts to strengthen its cybersecurity framework, as outlined in the National Cybersecurity Strategy and Awareness Creation Plan 2022-2027, demonstrate a commitment to safeguarding its digital future. However, addressing the persistent challenges requires a concerted and collaborative approach. By implementing the recommendations outlined above, the Namibian government, private organizations, and individuals can collectively build a resilient cybersecurity ecosystem. This will not only protect critical infrastructure and digital assets but also ensure the safety and prosperity of Namibia's citizens in an increasingly interconnected world. With sustained efforts, Namibia is poised to overcome its cybersecurity challenges and emerge as a leader in digital security within the region. Namibia hopes to create a robust cybersecurity ecosystem, protect its digital infrastructure, safeguard its people, and promote a safe and prosperous digital future with the help of partners in many industries.

Compliance with ethical standards

Disclosure of conflict of interest

The Authors proclaim no conflict of interest.

References

[1] Creese, S., Dutton, W. H., Esteve-González, P., & Shiller, R. (2021). Cybersecurity capacity-building: cross-national benefits and international divides. Journal of Cyber Policy, 6(2), 214–235. https://doi.org/10.1080/23738871.2021.1979617

[2] Deloitte. (2020, February). A Namibian perspective on the governance of cybersecurity. Retrieved from https://www2.deloitte.com/za/en/namibia/pages/risk/articles/namibian-perspective-on-cyber-security-2020.html.

[3] Farok, N. A. Z., & Zolkipli, M. F. (2024). Incident response planning and procedures. Borneo International Journal eISSN 2636-9826, 7(2), 69-76.

[4] Ifeanyi-Ajufo, N. (2024). Commonwealth Countries' Cybercrime Laws: An Overview. Retrieved from: https://eprints.leedsbeckett.ac.uk/id/eprint/11552/.

[5] Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. Journal of Global Information Technology Management, 22(3), 160-177. https://doi.org/10.1080/1097198X.2019.1603527

[6] Liquid C2. (2023, June 29). Liquid C2 Cyber Security Report reveals that cyber-attacks increased in Kenya, South Africa, and Zambia by 76% in 2022. Retrieved from https://liquid.tech/about-us/news/liquid-c2-cyber-security-report/.

[7] Lubua, E. W., & Pretorius, P. D. (2019). Cybersecurity policy framework and procedural compliance in public organisations. Proceedings of the International Conference on Industrial Engineering and Operations Management, Pilsen, Czech Republic, July 23-26.

[8] Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: Evidence from seven nations. Computers & Security, 120, 102820. https://doi.org/10.1016/j.cose.2022.102820

[9] Mosimolodi, S. S. (2022). Investigating the cybersecurity threat landscape for Botswana (master's thesis, Botswana International University of Science and Technology (Botswana)). Retrieved from: http://repository.biust.ac.bw/handle/123456789/553.

[10] Namibia National Cybersecurity Strategy & Awareness Raising Plan 2022-2027. (2022). Retrieved from https://mwt.gov.na/documents/869282/1898587/NCS+%26+Awareness+Raising+Plan+2022-2027.pdf.

[11] Nawa, E. L. T. (2021). Developing a cybersecurity framework for the banking sector of Namibia (Doctoral dissertation, Namibia University of Science and Technology). Retrieved from https://ir.nust.na/items/d9075c0a-648f-4cd2-87b1-24f25020bb92.

[12] Pieterse, H. (2021). The cyber threat landscape in South Africa: A 10-year review. The African Journal of Information and Communication, 28, 1-21. https://doi.org/10.23962/10539/31580

[13] Rengura, R. (2022). No contradiction between the Access to Information and Data Protection Bills. Retrieved from https://nbcnews.na/node/98959.

[14] Roshanaei, M. (2021). Resilience at the core: Critical infrastructure protection challenges, priorities, and cybersecurity assessment strategies. Journal of Computer and Communications, 9(8), 80-102. https://doi.org/10.4236/jcc.2021.98006

[15] Roshanaei, M. (2023). Cybersecurity Preparedness of Critical Infrastructure—A National Review. Journal of Critical Infrastructure Policy, Volume, 4(1). doi: 10.18278/jcip.4.1.4

[16] Rukanga, B. (2024, December 17). Sensitive data leaked after Namibia ransomware hack. Retrieved from https://www.bbc.com/news/articles/ce3l509e6x7o.

[17] Sarfo, S. (2023). The state of Africa's cybersecurity: Challenges and opportunities. Retrieved from https://www.linkedin.com/pulse/state-africas-cybersecurity-challenges-opportunities-samuel-sarfo/.

[18] Shipena, D., Mude, T., & Bhunu-Shava, F. (2021). Social media implications of cybercrime on human security in Namibia. AfriFuture Research Bulletin, 1(2), 22-35. ISSN: 2710-0421 (Print) ISSN-L: 2788-8924. Retrieved from www.afrifuture.org.

[19] Tariq, N. (2018). Impact of cyberattacks on financial institutions. Journal of Internet Banking and Commerce, 23(2). Retrieved from http://www.icommercecentral.com.

[20] Uudhila, J. M. (2016). Cybersecurity risk management and threat control model (CSRM-TCM): A study carried out to enhance the protection of information in the Namibian public service (master's thesis). Retrieved from http://hdl.handle.net/11070/1688.

[21] Vassiliadis, T., & Hedström, J. (2024). The challenges and opportunities in incident response for companies. 33, p. 54. URN: urn: nbn:se: his: diva-24067

[22] Waiganjo, I., & Valungameka, E. (2023). An assessment of cybersecurity awareness level in Namibia: Case study of Windhoek. Retrieved from http://dx.doi.org/10.2139/ssrn.4654473.

[23] Waiganjo, I., Osakwe, J., & Azeta, A. (2024). Impediments to Cybersecurity Policy Implementation in Organisations: Case Study of Windhoek, Namibia. International Journal of Research and Scientific Innovation, 11, 540-546. DOI: https://doi.org/10.30574/ijsra.2025.14.1.0225

[24] Xinhua. (2022, February 24). Namibian businesses more prone to cyberthreats: Research firm. Retrieved from https://www.bignewsnetwork.com/news/272331963/namibian-businesses-more-prone-to-cyberthreats-research-firm.