www.idosr.org
©IDOSR PUBLICATIONS

Ugwu and Ugwuanyi, 2024
ISSN: 2550-7958

International Digital Organization for Scientific Research
IDOSRJCE91.810.202411
IDOSR JOURNAL OF COMMUNICATION AND ENGLISH 9(1) 8-10, 2024.
https://doi.org/10.59298/IDOSR/JCE/91.810.202411

Addressing the Escalating Threat of Cybercrime in African Nations: Strategies for Legislation, Governance, and Capacity Building

[1]Ugwu Jovita Nnenna and [2]Ugwuanyi Ifeoma Perpetua

[1]Department of Publication and Extension Kampala International University Uganda.
[2]Department of Educational Management Enugu State University of Science and Technology, Enugu Nigeria.

ABSTRACT

This overall assessment considers the intricate terrain of cyber-threats in African countries in depth, showing how varied it is, what its economic consequences are, and why the appropriate countermeasures are needed. Cybercrime is a comprehensive threat that includes different types of activities, including hacking and phishing, right up to damaging intellectual property. The ripple effect goes far beyond immediate financials losses and is caused by service failures and reputational damage. The rising trends of cybercrime in Africa necessitate the urgency to fight it because, of its prevalence, with the annual losses running into billions. The article looks at the growth of cybercrime in Africa, especially the fact that cybercriminals are revolving into cybercriminal activities. As we've witnessed an internet population of over a billion people in the continent, the vulnerabilities become more widespread as there are insufficient cyber security laws and regulations in place. Mobile phone propagation aggravates weak security infrastructure that today are scaring Africa with a total cost of up to $4 billion yearly. Businesses and governments may fail to engage in cyber security which will increase their vulnerability since the commitment to the cyber security measures will be delayed, and timely and tactical response is needed. Legislation is a critical element in tackling cyber-attacks and this is a challenge many African countries face when it comes to enacting all-encompassing laws. The rules of Budapest Convention are used to create a guiding framework, which is aimed at supporting the harmonization with the international standards for the efficient cooperation. A coordinated effort culturally, as well as internationally, becomes evident to protect Africa's digital future by lessening the economic and social implications of cyber threats.

Keywords: Cybercrime, cybercrime strategies, internet security, cyber legislation, cyber governance, cyber capacity building and cyber threats.

INTRODUCTION

Crime is a big problem that great societies face in the world, and cybercrime makes it more complicated and more serious. Cybercrime comprises of a wide scope of activities; ranging from hacking to phishing, copy right infringement, theft of intellectual property and financial fraud. The aftermath of cybercrime is much more than financial losses: it affects businesses through service interruptions and damage to reputation. This article looks into cybercrime landscape in African countries, accepting that it goes on beyond the imagination day by day and the great challenge of dealing with it.

Cyber Crime Concepts

Cybercrime can be broadly categorized into two types: offenses such as violence and offenses to property. They are usually the beginning of the attack and the culprit is always a programmer who engineers the code, making the actions like hacking, virus attacks, etc., possible and harmful. The others deal with the crimes themselves and the persons who are victims of the illicit acts as the criminals' impact is often life- long. The findings of cyber risk surveys suggest that cyber security concerns have been ranked high worldwide, confirming the views in South Africa, the UK and North America. The damages caused by cybercrime in Africa are estimated to cost billions of dollars each year, as the continent is witnessing a tremendous growth in cyber threats and attacks [1- 3].

Trends in Cyber Security in Africa

In line with the rapid growth, Africa is much confronted with the fact that cybercrime gets more and more professionalized. By the end of 2022, the total of internet users is over a billion and thus, the continent is exposed to cyber threats with nothing to protect it, such as lack of cyber security laws and regulations [2]. The increased prevalence of mobile phones in Africa worsens the case, as the weak and dated security systems account for a $4 billion per year. The businesses as well as governments remain vulnerable to cyber-attacks as they fail in cyber security commitment although penetration of the internet has grown to very high levels [4-6].

Cyber-attacks and Cybercrime's Effect on Business

Digital crimes are becoming a major threat to companies all over the world including to African ones which are getting more exposed to cybercrimes. A lack of dedication to cybersecurity measures in African countries, along with an increased application of digital technologies, make companies more vulnerable. The wide-ranging presence of economic crimes like asset misappropriation, bribery, procurement fraud, corruption, and cybercrime in African companies [7]; [8] calls for urgent implementation of robust cyber security measures by Africa's businesses. ICT Advancements and Cyber Threats in Africa most recent AI applications. Along with the increase in Information and Communication Technology (ICT) this has also been giving rise to new challenges in the process, among them different types of cybercrime. The rivalry between the US and Russia on the issue of hacking only accentuates the gradual change of cyberspace from a peaceful initiative into a crime scene and theater of war. Nevertheless, Africa is not well prepared against cyber threats which accounts for the high number of cybercrimes which had been reported in the recent years.

Legislation and Cyber security

Adopting cybercrime will involve measures taken on various fronts with the first step being the creation of relevant legislation. Several African countries are confronted with difficulties of creating coherent legislation on cyber security, with Namibian draft bill on electronic transactions and cybercrime used as an instance (Namibian draft bill on electronic transactions and cybercrime). Hungarian Convention is an indicative rule for legislation along with the condition of the law to be in line with international standards to provide an opportunity to state parties and donors to interact with each other [13,14].

Cybercrime Strategy Implementation

A strategic approach that involves a number of key elements is needed for the successful implementation of cybercrime strategy. Governance is also of importance by having comprehensive policies and strategies from governments to fight cybercrime as well as establishing the relationship between cybercrime and cyber security policies. Criminalization of various cybercrimes, one of which is the legislation to use electronic evidence as one of the legal proceedings should first be developed [15]. The reporting and intelligence on cybercrime would be required for such purpose. Having specialized and advanced crime fighting units, backed up by capacity building and awareness programs, the law enforcement agencies and the Judiciary will be empowered. In the African context, cybercrime strategies need to be adapted, in such a way that they reflect cultural values and norms and that they are optimally implemented and monitored in terms of progress [16]; [17]. The menace of cybercrime is growing in effect in Africa, organized criminals transgressing the borders and committing crime against companies, government institutions and individuals. The continent lacks the requisite resilient cyber security systems due to the fast-evolving technology, leaving it open for cyber threats. Achieving success requires application of right tactics, for example through development of all-encompassing policies, governance, and addressing capacity deficiencies, in African nations to fight cybercrime. The matter is obvious to see that there should be the coordinated efforts my country and other states, both at home and internationally, to ensure the digital future of Africa and to prevent the economics and social impacts of cyber threats.

CONCLUSION

The focus of this article is to underline the imperative of coordinated efforts as opposed to unilateral actions and initiatives of African countries to deal with the menace of cybercrime. In the face of the growing threat of cyber-attacks and with the continual economic costs running into billions of dollars, the design of cohesive cyber security measures must be given the highest importance. The legislation, governance, and capacity building efforts ought to be prioritized to set up the right cybercrime policies. The mainland of Africa is at an important phase, where decisions determining the future of the digital are to be taken while cyber threats could never be underestimated in their implications. These proposed strategies will entail legislative frameworks, government structures, and capacity-building initiatives to build African nations' resilience as the cybercrime environment continues to evolve.

REFERENCES

1. Schell, B. H. and Martin, C. (2004). Cybercrime: A reference handbook. ABC-CLIO.
2. Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F. and Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. Geneva Pap Risk Insur Issues Pract., 47(3):698-736. doi: 10.1057/s41288-022-00266-6.
3. Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. Journal of Global Information Technology Management, 22(2), 77-81.
4. Liquid Cyber Security [Online]. (2021). The evolving cyber Security threat in Africa: IT and financial decision makers respond to critical developments in South Africa, Kenya and Zimbabwe. Retrieved from: https://liquid.tech/wps/wcm/connect/corp/00d614b5-e6cf-4552-9085_c12e47b6246c...
5. Cassim, F. (2011). Addressing the growing spectre of cybercrime in Africa: evaluating measures adopted by South Africa and other regional role players. Paper presented at the First International Conference of the South Asian Society of Criminology and Victimology at Jaipur, India, 15-17 January, 123-138.
6. Davies, W. (2018). Short cuts. London Review of Books, 5 April, 40 (7): 20-21
7. Quarshie, H. O. and Martin-Odoom, A. (2012). Fighting cybercrime in Africa. Computer Science and Engineering, 2(6): 98-100.
8. Jegede, A. E., Olowookere, E. I. and Elegbeleye, A. O. (2016). Youth identity, peer influence and internet crime participation in Nigeria: A Reflection. Ife PsychologIA, 24(1): 37-47.
9. Halder, D. and Jaishankar, K. (2011). Cybercrime and the victimisation of women. Carnegie, United Kingdom: IPR/Business books.
10. Ezeji, C. L., Olutola, A. A. and Bello, P. O. (2018). Cyber-related crime in South Africa: extent and perspectives of state's roleplayers. Acta Criminologica: Southern African Journal of Criminology Special Edition: Cybercrime, 31(3), 93-110.
11. Mbanaso, U. M. (2016). Cyber warfare: African research must address emerging reality. The African Journal of Information and Communication, 18, 157-164.
12. Fabian, C. O., Val Hyginus, U. E., Chinyere, N. U. (2023). Navigating Challenges and Maximizing Benefits in the Integration of Information and Communication Technology in African Primary Schools. International Journal of Humanities, Management and Social Sciences, vol. 6, no. 2, pp. 101-108. DOI: 10.36079/lamintang.ij-humass-0602.599
13. Gordon, B. (2000). Cyberlaw @ SA. Pretoria, South Africa: Van Schaik.
14. African Union (2015). A global approach on cybersecurity and cybercrime in Africa. <https://au.int/sites/default/files/newsevents/workingdocuments/31357-wd-a_common_african_approach_on_cybersecurity_and_cybercrime_en_final_web_site_.pdf
15. Data Protection and Cybercrime Division 2013, Capacity building on cybercrime, Global Project on Cybercrime: <http://www.combattingcybercrime.org/files/virtual-library/capacity-building/capacity-building-on-cybercrime.pdf>
16. Seger, A. (2012a). The Budapest convention on cybercrime 10 years on: Lessons learnt or the web is a web: <file:///C:/Users/JoeyCSIR/OneDrive/Cybercrime%20ICCWS2019/The%20Budapest%20Convention%20on%20Cybercrime%2010%20years%20on.pdf
17. Usmani, K. A. and Appayya, J. A. (2017). Capacity building is the key to fight against cybercrime: The Mauritian perspective', Global Cyber Expertise Magazine, vol. 4. <https://www.thegfce.com/news/news/2017/11/21/capacity-building-is-the-key-to-fight-against-cybercrime-the-mauritian-perspective>.

CITE AS: Ugwu Jovita Nnenna and Ugwuanyi Ifeoma Perpetua (2024). Addressing the Escalating Threat of Cybercrime in African Nations: Strategies for Legislation, Governance, and Capacity Building. IDOSR JOURNAL OF COMMUNICATION AND ENGLISH 9(1) 8-10. https://doi.org/10.59298/IDOSR/JCE/91.810.202411