BOOK CHAPTER | Cyber Security Approach

A Multi-Thronged Cyber Security Approach against Cybercrime in Developing Nations

Iwayemi A. & Olokun M. S.
Department of Computer Engineering
Federal Polytechnic
Ile-Oluji, Ondo State, Nigeria
E-mails: iwayemiresearch@gmail.com, samolokun@fedpolel.edu.ng

Abstract

Cyber criminality is a global challenge, and several solutions have been developed to reduce it. Meanwhile, the causes of cybercrime in developing nations are peculiar, multi-faceted and far above its motives in developed countries. Besides the common global challenges responsible for cybercrime, the prevalence of this menace in some developing countries are not dissociable from the major negative characteristics, such as mass poverty, associated to these nations. This article presents a multi-remedy system that tends to cater for the peculiar challenges of developing nations in addition to the general ones affecting cyberspace. Provision of infrastructures and amenities, employment, education, good and secure national data base system, software and hardware security, network/internet security, and social security number system alongside cybersecurity architectures form the framework necessary to cob cybercrime in developing nations. These measures are linked together using appropriately. The resulting scheme will alleviate several prevailing problems, among which cyber-attack could be seen as one of, thereby reducing cybercrime in developing nations. Inadvertently, global cybersecurity architectures will have a hundred percent penetration in the affected nations and yield maximum outcome.
Keywords: cybercrime, https, security, government, web

Introduction

What is Cybercrime?

Cybercrime is a common term similar to household crime, bank crime, industrial crime and so on. Cybercrime is said to have many different sides and can occurs in multiple set-ups and environments. (Gordon & Ford, 2006). The authors defined cybercrime as any wrong doing committed using a computer, network, hardware device, or software and presented several examples of it according to types as indicated in Table 1.

What is Multi thronging?

Multi thronging simply means a large number of things that are assembled together for the purpose of achieving a task or diverse tasks. The collection of many techniques, principles, tools, resources and mechanisms to solve a problem can be referred to as multi-thronging.

Citation : Iwayemi A. & Olokun M. S. (2022). A Multi-Thronged Cyber Security Approach against Cybercrime in Developing Nations. SMART-IEEE-ACity-ICTU-CRACC-ICTU-Foundations Series
Book Chapter on Web of Deceit - African Multistakeholders' Perspective on Online Safety and Associated Correlates Using Multi-Throng Theoretical, Review, Empirical and Design Approaches. Pp 197 -202. www.isteams.net/bookchapter2022.
DOI https://doi.org/ 10.22624/AIMS/BK2022-P33

In other words, the use of great number of resources, principles, personnel, institutions, organizations aligned together to cob cybercrime is a multithronged cybersecurity approach.

Table 1: Cybercrime by Types (Gordon & Ford, 2006)

Example	*Type*	*Software*	*Crimeware*
Phishing	I	Mail client	No
Identity Theft	I	Keylogger, Trojan	Yes
Cyberstalking	II	Email Client, Messenger Clients	No
DDoS	I	Bots	Yes
Cyberterrorism (communication)	II	Steganography, Encryption, Chat Software	No

What is Cyber security?

Cybersecurity refers to every countering or preventive measure targeted against cybercrime. Cybersecurity is also seen as a progressing task which caters for the entire field of Information and Communication Technology with respect to small, medium, and large enterprises including governmental as well as non-governmental entities. (Salamzada et al., 2015). The importance of cybersecurity cannot be overemphasized and there is the need to teach cybersecurity in schools. (Rowe et al., 2011). Common cybercrimes prevalent in developing nations include internet fraud,

Cyber Crime in Developing Nations

Internet based activities of developed nations are adopted by developing nations, however, the security requirements are yet to be catered for. (Gcaza & von Solms, 2017; Tagert, 2010). Some of these activities include cloud computing, massive open online courses, mobile computing, electronic governance, internet banking and so on. In the long run, the security gaps created by developing nations make them common platforms to affect the developed nations. (Elkhannoubi & Belaissaoui, 2017). For instance, small and medium enterprises in developing countries are constrained by certain internal factors. (Kabanda et al., 2018). Security is supposed to ensure confidentiality, availability and integrity. (Kumar, 2017).

Developing countries face the same cyber challenges as developed nations but the former lack the capacities including the awareness necessary to prevent cyber-attacks thereby making them more vulnerable. (Muller, 2015). Notwithstanding, everyone is on the network, whether developed or developing nations. (Brechbühl et al., 2010). Therefore, the vulnerabilities of developing nations should be jointly combatted. A framework comprising comprehensive solutions is necessary for bridging the cybersecurity gap between developed nations and developing or underdeveloped nations. (Salamzada et al., 2015). The authors conducted interviews with experts from which a security model was proposed for Afghanistan.

The Multi Thronged Cyber Security Model

Cybercrimes arising from several sources such as internet frauds are prevalent in developing nations, hence, the collection of remedies required in eliminating each of these sources is necessary for countering the menace. For example, lack of education, poor infrastructure, joblessness, poor orientation/ awareness are prevalent in these nations. Hence, good education; industrialization; provision of amenities/infrastructure; employment; enlightenments/awareness; data capturing; software, hardware, and internet/network security are therefore unpopular/ unidentified solutions necessary for the removal of the key sources of cybercrimes in developing nations.

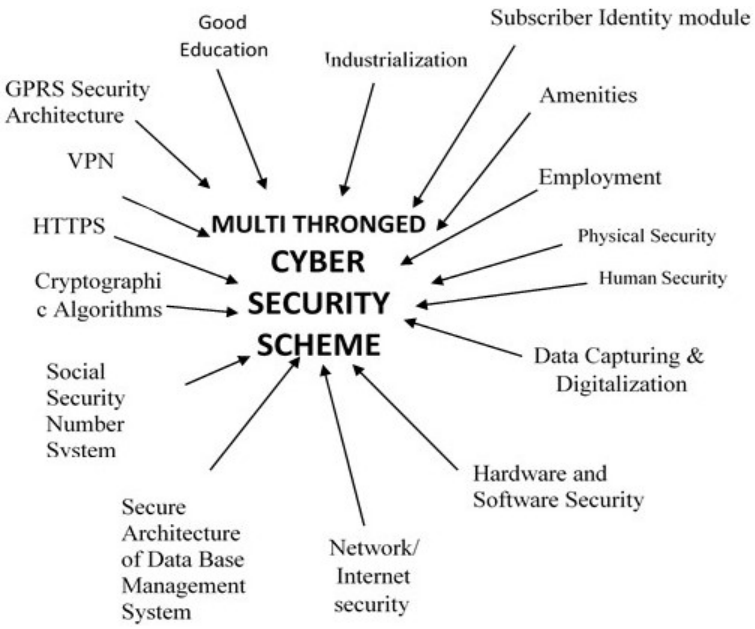

Figure 1: Multi Thronged Cyber Security Scheme Against Cybercrime in Developing Nations

In addition, the use of secure architecture of data base management system, social security number system, cryptography, VPN, GPRS Security Architecture, Intrusion Detection System, and HTTPS (against HTTP) are also cybersecurity measures recommended for full implementation in various platforms and organizations of developing nations. Figure 1 indicates the model.

Good Education

Free education, good and qualitative educational structure are necessary to alleviate the extreme poverty in some developing nations. This education will give their citizens the sense of belonging and in turn they will like to preserve the cyber resources of their nation. More so, education will make them engaged and grant them the opportunity to be gainfully employed. This means centers of cybersecurity could be created in institutions and the course could be offered by the faculties.

Industrialization

It is sardonic that many African countries depend on imported goods for survival. This is because of the low level of industrialization. Original hardware devices customized and relevant for their societies might not be available overseas. When there are adequate industries, citizens will be occupied with activities that will distract them from attacks. The percentage of people who resort to cybercrime because of no industrialization will be reduced when industries are built.

Infrastructure/ Amenities

IOT devices run on constant power supply whereas in some developing nations, power supply and other social amenities are unavailable most times. Prolonged darkness create a suitable environment for physical attack just like unavailability of constant power supply render the surveillance through CCTV unreliable.

Employment

Bad governance and poor governmental policies have kept a large population of educated and skilled people in several African nations jobless while many employed people are underpaid and suffer poor job conditions. Minimum wages in some developing nations are unable to cater for the basic needs of employees, hence, they look for alternative routes in search of basic food. Creating good employments in developing nations will therefore reduce the general crime rate and in turn decrease rate of cyber-attacks drastically.

Several intra-national crises leading to massive infrastructural destructions and cyberattacks are often premised around high unemployment rates of the working age in developing countries.

Enlightenments/ Awareness

Due to scarcity of state-of-the-art technology, poor provision of amenities, high unemployment rates, and poor educational structure; enlightenment on cybersecurity measures is not prominent. Meanwhile, enlightenment on basic security measures like the use of strong password system, difficult security questions, and so on is essential in preserving the cyberspace.

Electronic Data Capturing, Digitalization and Cloud Technology

Secure electronic data capturing is an antidote for data loss due to physical destruction of infrastructure. Digitalization is simply converting analogue data into digits that can be better secured.(Brennen & Kreiss, 2016). The data captured can be stored in the cloud for safety.

Software and Hardware Security

Software security can be ensured through the use of passwords, locks, user authentications, authorization setups, session management, captcha, and so on. Application security activities include IP filtering, post deployment security tests and others. (*Software Security*, n.d.). Hardware infrastructures are secured through the use of physical measures that are metallic, non-flammable and electronically programmed. Biometric, password or RFID based doors with high standard of barrier and resistivity will secure the cyber hardware infrastructure. Appropriate secure software and hardware barriers can be used to ensure the security of infrastructures. (Fournaris et al., 2017). To achieve hardware security, a secure channel establishment on the hardware module might be used. (Kim et al., 2014).

Network/internet security

Use of secure gateways, secure wireless systems, antiviruses, antimalware, spams, and others are some of the means of ensuring network/ internet security.

Secure Architecture of Data Base Management System

Most developing nations do not have centralized database of things, systems and people. This encourages cybercrime because hackers can easily be masked. Hence the provision of a secure database of places, systems and people will go a long way to cob cybercrime.

Social Security Number System

The SSN system is recommended as a typical means of identification and transaction without which some cyberspace features can be anonymously attacked.

Cryptography

The use of multiple encryption algorithms by originating systems in developed nations will help guard against message compromise and attack.

Secure VPN

A virtual private network (VPN) is a private network built within a public network infrastructure, such as the Internet.(Ferguson & Huston, 1998). The use of secure Virtual Private Network will keep communication private and secret among nodes

Intrusion Detection System

The use of sensors, cameras and secure embedded systems are essential in detecting intruders and controlling crimes.

HTTPS

As against conventional Hyper Text Transfer Protocol (HTTP), the secured version, HTTPS, can be adopted by all web-based applications to ensure privacy and security in transactions ranging from home banking to e-commerce and e-procurement to those involving sensitive data like career and identity information. (Callegati et al., 2009). HTTPS encrypts communication by authenticating the communicating end points and ensuring confidentiality. (Naylor et al., 2014).

Activity Diagram

Three major entities are in a nation and they are: the Government, Organizations and Individuals/Employees. Figure 2 shows the use case diagrams of the model.

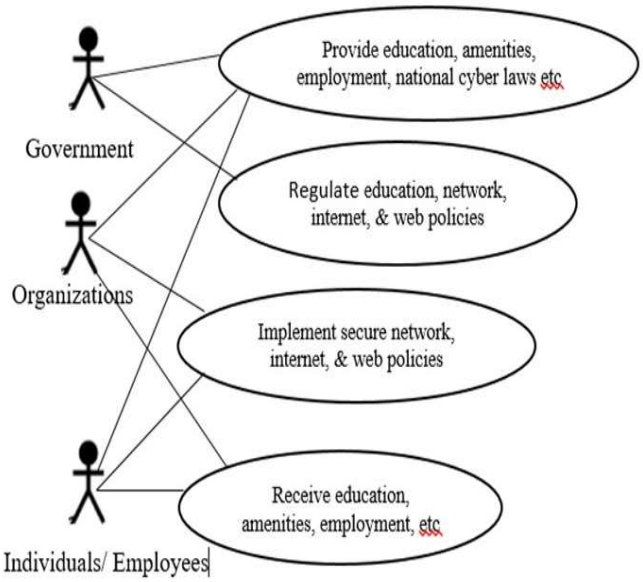

Figure 2: Use Case Diagram of the Multi-thronged Approach

Conclusion

Internet fraud, web deceit, phishing, hardware vandalism, denial of service, cyber-dating fraud, email spam, and malware are common attacks against the cyber infrastructures of developing nations. The irony is that the aforementioned are on the increase per time in these nations due to certain dominant factors in the regions. It is therefore apparent that the true solution to cybercrime must be all-encompassing, comprehensive, and multi-dimensional.

This strategic remedy includes, though not limited to, good education; industrialization; provision of amenities/infrastructure; employment; enlightenments/awareness; data capturing system; software, hardware, and internet/network in addition to the use of the security architecture of database management system, social security number system, cryptography, VPN, GPRS Security Architecture, Intrusion Detection System, and HTTPS (against HTTP). It is therefore unmistakable that when all the collections are in full implementation in developed nations, cybercrime will be reduced not only in the affected regions but also in the entire cyberspace.

References

1. Brechbühl, H., Bruce, R., Dynes, S., & Johnson, M. E. (2010). Protecting critical information infrastructure: Developing cybersecurity policy. *Information Technology for Development*, *16*(1), 83–91. https://doi.org/10.1002/itdj.20096
2. Brennen, J. S., & Kreiss, D. (2016). Digitalization. *The International Encyclopedia of Communication Theory and Philosophy*, 1–11. https://doi.org/10.1002/9781118766804.WBIECT111
3. Callegati, F., Cerroni, W., & Ramilli, M. (2009). Man-in-the-middle attack to the HTTPS protocol. *IEEE Security and Privacy*, *7*(1), 78–81. https://doi.org/10.1109/MSP.2009.12
4. Elkhannoubi, H., & Belaissaoui, M. (2017). Assess developing countries' cybersecurity capabilities through a social influence strategy. *2016 7th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications, SETIT 2016*, 19–23. https://doi.org/10.1109/SETIT.2016.7939834
5. Ferguson, P., & Huston, G. (1998). *What is a VPN?*
6. Fournaris, A. P., Lampropoulos, K., & Koufopavlou, O. (2017). Hardware Security for Critical Infrastructures - The CIPSEC Project Approach. *Proceedings of IEEE Computer Society Annual Symposium on VLSI, ISVLSI*, *2017-July*, 356–361. https://doi.org/10.1109/ISVLSI.2017.69
7. Gcaza, N., & von Solms, R. (2017). A strategy for a cybersecurity culture: A South African perspective. *Electronic Journal of Information Systems in Developing Countries*, *80*(1), 1–17. https://doi.org/10.1002/j.1681-4835.2017.tb00590.x
8. Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13–20. https://doi.org/10.1007/s11416-006-0015-z
9. 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
10. Kim, D., Jeon, Y., & Kim, J. (2014). A secure channel establishment method on a hardware security module. *International Conference on ICT Convergence*, 555–556. https://doi.org/10.1109/ICTC.2014.6983209
11. Kumar, J. (2017). Related Papers. *Over The Rim*, 191–199. https://doi.org/10.2307/j.ctt46nrzt.12
12. Muller, L. P. (2015). Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities. *Norwegian Institute of International Affairs*, *3*, 23. https://brage.bibsys.no/xmlui/bitstream/id/331398/NUPI+Report+03-15-Muller.pdf
13. Naylor, D., Finamorey, A., Leontiadisz, I., Grunenbergerz, Y., Mellia, M., Munafòy, M., Papagiannakiz, K., & Steenkiste, P. (2014). The cost of the "s" in HTTPS. *CoNEXT 2014 - Proceedings of the 2014 Conference on Emerging Networking Experiments and Technologies*, 133–139. https://doi.org/10.1145/2674005.2674991
14. Rowe, D. C., Lunt, B. M., & Ekstrom, J. J. (2011). *The Role of Cyber-Security in Information Technology Education*.
15. Salamzada, K., Shukur, Z., & Abu Bakar, M. (2015). A Framework for Cybersecurity Strategy for Developing Countries: Case Study of Afghanistan. *Asia-Pacific Journal of Information Technology and Multimedia*, *04*(01), 1–10. https://doi.org/10.17576/apjitm-2015-0401-01
16. *Software Security*. (n.d.). Retrieved January 27, 2022, from https://www.whitehatsec.com/glossary/content/software-security
17. Tagert, A. C. (2010). *Cybersecurity Challenges in Developing Nations*. Department Engineering and Public Policy, Carnegie Mellon University Pittsburgh, PA.