CYBER SECURITY CAPABILITY MATURITY MODEL FOR CRITICAL INFORMATION TECHNOLOGY INFRASTRUCTURE AMONG NIGERIA FINANCIAL ORGANIZATIONS

Article *in* International Journal of Current Research · June 2019

DOI: 10.24941/ijcr.35585.06.2019

CITATIONS
0

READS
109

2 authors:

Aliyu Musa Bade
Yobe State University
3 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Idi Mohammed
Yobe State University
5 PUBLICATIONS **0** CITATIONS
SEE PROFILE

ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 11, Issue, 06, pp.4796-4799, June, 2019

DOI: https://doi.org/10.24941/ijcr.35585.06.2019

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

CYBER SECURITY CAPABILITY MATURITY MODEL FOR CRITICAL INFORMATION TECHNOLOGY INFRASTRUCTURE AMONG NIGERIA FINANCIAL ORGANIZATIONS

[1,*]Aliyu Musa Bade and [2]Idi Mohammed

[1]Department of Computer Science, Yobe State University Damaturu, Nigeria
[2]Faculty of Computing, Universiti Teknologi Malaysia

ARTICLE INFO

Article History:
Received 20th March, 2019
Received in revised form
24th April, 2019
Accepted 15th May, 2019
Published online 30th June, 2019

Key Words:

Cybersecurity, Critical Information Technology infrastructures, Cyber attack, Nigeria financial organizations.

***Corresponding author:* Aliyu Musa Bade**

ABSTRACT

The effectiveness of Nigeria Cybersecurity strategy can have serious effect on the Cybersecurity stance of the country and significantly impact how well the country financial critical IT infrastructures are protected. The problem is that, different organizations use different tools to evaluate their Cybersecurity strength against any cyber attack. This Model is developed to provide a measure which the Nigeria financial organizations can apply to determine their level of vigilance on preventing and responding to a cyber attack.

***Citation: Aliyu Musa Bade and Idi Mohammed,* 2019.** "Cyber security capability maturity model for critical information technology infrastructure among Nigeria financial organizations", *International Journal of Current Research*, 11, (06), 4796-4799.

INTRODUCTION

Critical infrastructure is made up of two words: "critical" and "infrastructure". The term "critical" includes the infrastructure that provides support for health, economic, public, social well being, and for the running of key government responsibilities (Dai, Huu and Zoltán, 2017). The word "infrastructure" refers to the stock of physical facilities needed for the functioning of any society (Goel, 2002). Invariably, critical infrastructure is also called that wide collection of public facilities and equipment put in place to offer social services and support public and private sector economic activity (Moteff and Parfomak, 2004). Studies conducted by (Curtis and Mehravari, 2015) prove that the highest rate of Cyber attacks have been directed against critical infrastructures such as power, manufacturing, financial services, and power system. The critical infrastructures that simplify our way of life are increasingly vulnerable to cyber attack. Therefore, distraction to these critical infrastructures usually incur valuable human and financial cost, which is often the main target of cyber-attack and the reason such infrastructures are targeted by actors who's motivation are profit or sociopolitical causes, among other reasons (Grau and Kennedy, 2014). Although critical infrastructure has many component, an fundamental thing is the information technology (IT).

As a result of IT, it can communicate with all other aspects of the critical infrastructure system. Consequently, though IT have significant impact on all aspects of our modern society, it may harbor prospective vulnerability as a honey-pot for actors to exploit (Dai *et al.,* 2017). Thus, critical infrastructure are pivotal for the financial organizations in Nigeria because once this system is disrupted, it will seriously influence not only citizens but also threaten other essential public and private services, including the government. The Nigeria Interbank Settlement Systems Plc's (NIBSS) reported that as at August, 2018, the estimated number of bank customers that had obtained their Bank Verification Number (BVN) stood at 34.33 million, which account for only 17% of Nigerian Population, it is envisaged that more will enroll as the population and economy continue to growth. As the enrollment increases, the increases in connectivity type and volumes of data flow, the potentiality for cyber-attacks increases. In other to prepare systems to survive cyber-attacks, the Nigeria financial organizations are faced with countless controls and standards, and many of their implementations are incoercible, which further exacerbates the risk environment and provides a false sense of security. The growth of the Internet on the country, economic hardship and financial gains are just a few of the many factors contributing to Cyber risk against critical IT infrastructure in Nigeria's financial organizations.

Cyberspace, Cybercrime and Cybersecurity

Technology advancement has also led the definitions of cyberspace, Cybercrime and cyber security. It has been debated that since computer crime may involve all classes of offense, a definition must highlight the knowledge or the use of computer technology(Ibikunle and Eweniyi, 2013). This section discusses Cyberspace, Cybercrime and Cybersecurity (C3).

Cyberspace: The most important things to know about Cyberspace are that it is borderless(Ibikunle and Eweniyi, 2013). Cyberspace refers to the unlimited space called the internet (Ibikunle and Eweniyi, 2013). In the other way, it refers to the mutually dependent network of ICT components that strengthen many of our communications technologies in use today.

Cybercrime: Ibikunle (2013) define Cybercrime as the series of structure crime attacking both cyberspace and Cybersecurity. This includes anything from penetrating into online bank accounts to downloading illegal media files. Cybercrime also includes offenses other than financial, such as spreading viruses on other end-network devices or reveal confidential business information of any organization on the internet. Nigeria financial system liveliness and national security to a greater extent depend on a vast array of interdependent and critical networks, systems, services, and resources also called cyberspace (Ibikunle and Eweniyi, 2013). Cybercrime has imagine in shortly after the advent of internet in the country in 1996 . Recently, Central Bank of Nigeria, (CBN) reported that 2.4 per cent of banking revenue was lost to Cyber fraud cases (Ibikunle and Eweniyi, 2013). Nigerian financial organizations have lost a total of half billion USD to e-fraud between 2000 and 2014, mostly due to wrong and careless management of customers' data (Grau and Kennedy, 2014). The Cyber-criminals in Nigeria are commonly known as Yahoo-Boys.

Cybersecurity: Cybersecurity is mainly the major practice to ensure the safety of cyberspace from internal, external, known and unknown threats. According to (Oyelere, Sajoh, Malgwi and Oyelere, 2015), Cybersecurity was defined as information confidentiality, systems integrity and survivability, availability, online contents filtering, wiretapping, and protection against cyberspace abuse.

a) *Confidentiality* refers to safeguarding the information from disclosure to unauthorized parties.
b) *Integrity* refers to protecting and withholding of information from modification by unauthorized parties.
c) *Survivability* refers to ability to sustain operation when one or a few network components fail.
d) *Availability* means to ensure that authorized persons or group of persons are capable to access the information when needed.
e) *Content filtering* refers to screening and excluding from access or availability resources that is deemed offensive.
f) *Wiretapping* refers to surreptitious electronic monitoring of data across the communication channels
g) *Cyberspace abuse* refers to any form of unlawful activity and behavior online

From the explanation above, Cyberspace is to provide avenue communications, Cybercriminals are offenders that abuses the use of Cyberspace while Cybersecurity is mean to safeguard Cyberspace infrastructure, the next section will discuss critical infrastructure.

Attack on critical infrastructure

The report of cyber security in general public has been raised to a record high in the last couple of years, with instances such as the WannaCry ransomeware attack making headlines globally. The problems that surround cyber-attack on critical infrastructure are exceptionally difficult to deal with and broadly hard to achieve due to the covered identities of accrediting perpetrators (Thakur, Ali, Jiang and Qiu, 2016). Currently the most high profile cyber-attacks on critical infrastructure around the globe include; New York Dam Attack(2013), Ukrainian Power Outages(2015), SWIFT global bank messaging system (2015), WannaCry ransomware attack (2017) and Rampant Data Exposures (2018). Hackers have become more terrifying, while much of the critical infrastructure continues to use legacy technology when carrying out critical processes. This vulnerability open to even simplistic forms of cyber-attack.

Securing the critical infrastructure

Securing critical infrastructure facilities against malicious attacks is a key challenge faced by managers of those facilities (Depoy *et al.,* 2005). Most of the critical infrastructures of significance are used to carry some service (Finance) to an end user. An infrastructure facility include "assets", that must control properly in order for the capacity to perform its planned function (Depoy *et al.,* 2005). The facilities include cyber elements that can control machineries, such as Automated Teller Machine(ATM) and Point of sales system(POS) which are use by financial organizations. The machines will have some form of physical and cyber protection system (Depoy *et al.,* 2005).

Capability maturity model

Capability Maturity Model (CMM) is not a software development model. It is a policy for improving the software process. It was developed in 1989 by Software Engineering Institute (SEI) of Carnegie-Mellon University (Kaur, 2014). The main purpose of using CMM is to evaluate the maturity of software processes of an organization and to identify the key practices that are required to increase the maturity of these processes. Furthermore, the levels in a CMM illustrate states of organizational maturity virtual to process maturity such as (Butkovic and Caralli, 2013).

ad-hoc → managed → defined → quantitatively managed → optimized

Because of the common ways of the process maturity scaling, the basic maturity carriage of the CMM framework can be applicable to other domains, such as Cybersecurity capability maturity model.

Cyber security Capability maturity models

From the fundamental theory of security, it is defined as the state of being secure, being free from threat(Le and Hoang, 2016). For instance, the security of a nation state comprising its citizens, establishments, and economy, which is regarded as a duty of government.

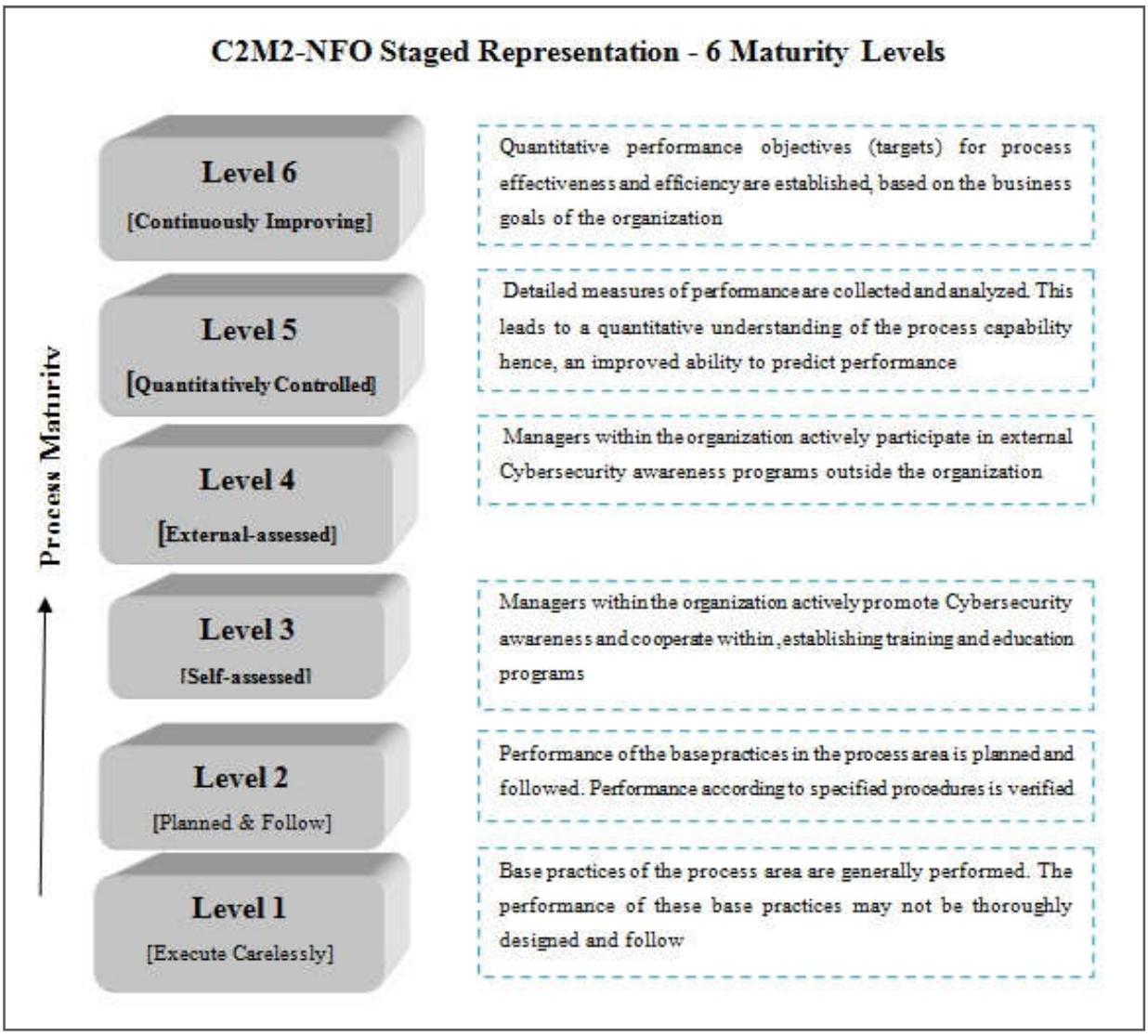

Figure 1.

However, differences in opinion cause for this usage as people consider both the cyber space and cyber security from different viewpoints. Furthermore, in order to ensure a cyber space, there have been many security models approaches, while focusing on a particular security objective such as risk, asset, identification, physical components, network, data, and application(Kozik and Chora??, 2013). There are little attempt on developing a security model that considers the security of a system holistically. In recent years, numerous security maturity models have been suggested for overall security management.

FINDINGS

Finding indicates that the Nigeria financial organizations among all, uses National Cybersecurity Strategy (NCSS) which is the nation's promptness strategy to provide unified measures with tactical actions towards assuring security and safeguarding of the country presence in cyberspace, defending critical information infrastructure, building and nurturing trusted cyber-community (Ministry of Information Communications and Technology, 2014). The drawback of NCSS is that, there is no element of strength measurement in this strategy. Secondly, to drive a C2M2 the entire objectives of bank regulation need to be identify. The most common objectives are Systemic risk reduction. In order to have Model that have element of strengthening of measures, we Propose Cybersecurity Capability Maturity Model for Nigeria Financial Organizations.

A model to address the Nigeria financial organizations cybersecurity problems

Introducing the Cybersecurity Capability Maturity Model for Nigeria Financial Organizations (C2M2-NFO) with Six Maturity Levels (MLs). The C2M2-NFO maturity levels, as shown in Figure1.

The identify of these 6 MLs were selected to ensure straightforwardness, but to indicate maturity progression. In order to progress from lower to higher level, there are some activities that would need to be consummated. According to (White and Ph, 2007) these include the development of metrics to determine the current security position of the organization, creation of information sharing mechanism

REFERENCES

Butkovic, M. J. and Caralli, R. a. 2013. Advancing Cybersecurity Capability Measurement Using the CERT-RMM Maturity Indicator Level Scale, (November), 1–37. Retrieved from http://www.sei.cmu.edu

Curtis, P. D. and Mehravari, N. 2015. Evaluating and improving cybersecurity capabilities of the energy critical infrastructure. 2015 IEEE International Symposium on Technologies for Homeland Security, HST 2015, (May. https://doi.org/10.1109/THS.2015.7225323

Dai, N., Huu, P. and Zoltán, R. 2017. The current state of information communication technology in critical infrastructure: the case of Vietnam. Hadmérnök, (Xii), 173–179. Retrieved from http://hadmernok.hu/174_17_rajnai.pdf

Depoy, J., Phelan, J., Sholander, P., Smith, B., Varnado, G. B. and Wyss, G. 2005. Risk Assessment for Physical and Cyber Attacks on Critical Infrastructures. MILCOM 2005 - 2005 IEEE Military Communications Conference, 1–9. https://doi.org/10.1109/MILCOM.2005.1605959

Goel, D. 2002. Impact of Infrastructure on Productivity:Case of Indian Registered Manufacturing. Growth (Lakeland), (106), 1–23. https://doi.org/10.2307/29793779

Grau, D. and Kennedy, C. 2014. TIM Lecture Series – The Business of Cybersecurity. Technology Innovation Management Review, 4(4), 53–57.

Ibikunle, F. and Eweniyi, O. 2013. Approach To Cyber Security Issues in Nigeria: Challenges and Solution. *International Journal of Cognitive Research in Science, Engineering and Education (IJCRSEE),* 1(1), 100–110. Retrieved from http://ijcrsee.com/index.php/ijcrsee/article/view/11/114

Kaur, J. 2014. Comparative Study of Capability Maturity Model. *International Journal of Advanced Research in Computer Science and Technology,* 2(1), 47–49.

Kozik, R. and Chora, M. 2013. Current cyber security threats and challenges in critical infrastructures protection. 2013 2nd International Conference on Informatics and Applications, ICIA 2013, 93–97. https://doi.org/10.1109/ICoIA.2013.6650236

Le, N. T. and Hoang, D. B. 2016. Can maturity models support cyber security? 2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC), 1–7. https://doi.org/10.1109/PCCC.2016.7820663

Ministry of Information Communications and Technology. 2014. National Cybersecurity Strategy. National Cybersecurity Strategy, Feel safe.

Moteff, J. and Parfomak, P. 2004. Critical Infrastructure and Key Assets: Definition and Identification. Time, 19. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA454016

Oyelere, S. S., Sajoh, D. I., Malgwi, Y. M. and Oyelere, L. S. 2015. Cybersecurity issues on web-based systems in Nigeria: M-learning case study. CYBER-Abuja 2015 - International Conference on Cyberspace Governance: The Imperative for National and Economic Security - Proceedings, 259–264. https://doi.org/10.1109/CYBER-Abuja.2015.7360510

Thakur, K., Ali, M. L., Jiang, N. and Qiu, M. 2016. Impact of Cyber-Attacks on Critical Infrastructure. Proceedings - 2nd IEEE International Conference on Big Data Security on Cloud, IEEE BigDataSecurity 2016, 2nd IEEE International Conference on High Performance and Smart Computing, IEEE HPSC 2016 and IEEE International Conference on Intelligent Data and S, 183–186. https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2016.22

White, G. B. and Ph, D. 2007. The Community Cyber Security Maturity Model the Center for Infrastructure Assurance and Security The University of Texas at San Antonio. Sciences-New York, 1–8.

****