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

IDI MOHAMMED

A dissertation submitted in fulfilment of the
requirements for the award of the degree of
Master of Computer Science

School of Computing
Faculty of Engineering
Universiti Teknologi Malaysia

MAY 2019

ACKNOWLEDGEMENT

In preparing this thesis, I was in contact with many people, researchers, academicians, and practitioners. They have contributed towards my understanding and thoughts. In particular, I wish to express my sincere appreciation to my supervisor, Dr. Siti Hajar Othman, for encouragement, guidance, critics and friendship. I am also very thankful to Dr. Anazida Binti Zainal for her guidance, advices and motivation. Without their continued support and interest, this dissertation would not have been the same as presented here.

I am also indebted to Tertiary Education Trust Fund (TetFund) of Nigeria for funding my studies. The committee of Provosts, Deans and Directors of Yobe State University, Damaturu also deserve special thanks for their nomination.

My fellow postgraduate student should also be recognised for their support. My sincere appreciation also extends to all my colleagues and others who have provided assistance at various occasions. Their views and tips are useful indeed. Unfortunately, it is not possible to list all of them in this limited space. I am grateful to all my family member.

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 information technology infrastructures are protected. In order to measure the strength and weaknesses of Cybersecurity, organizations can implement the developed Cybersecurity Capability Maturity Model (C2M2). Many developers have developed a range of Cybersecurity oriented models for strengthening practices to protect critical infrastructure. These models, however, similar to any other security oriented models are subject to uncertainty and a comprehensive critical infrastructure protection strategy is to be able to reduce exposure to risk and address uncertainty. Cybersecurity Capability Maturity Model (C2M2) for Nigeria financial organizations as a security oriented model to determine the level of Cybersecurity strength in Nigeria financial organizations is developed. The developed model provided five maturity levels: i) Nothing Exists, ii) Basic, iii) Progressed, iv) Advanced, and v) Innovative. The goal of this research is to build up a model that will validate the level of Cybersecurity strength in Nigeria financial organizations. Seven organizations which includes Guarantee Trust Bank , United Bank for Africa, Union Bank of Nigeria, First Bank of Nigeria, Stanbic-IBTC Bank, Federal Mortgage Bank, and Polaris Bank all located in Damaturu are chosen to measure their Cybersecurity preparedness using the developed model. Fully in-structured interview are performed with information technology officers in case study. Results analysis show that all organizations in case study are at iv) Advanced level.

ABSTRAK

Keberkesanan strategi keselamatan siber bagi negara Nigeria boleh memberi kesan yang serius terhadap pendirian keselamatan siber negara tersebut dan memberi kesan yang signifikan terhadap perlindungan infrastruktur teknologi informasi kritikal Negara berkenaan. Untuk mengukur kekuatan dan kelemahan keselamatan siber, organisasi boleh melaksanakan *Cybersecurity Capability Maturity Model* (C2M2). Ramai pembangun telah membangunkan pelbagai model berorientasi keselamatan siber untuk memperkuatkan amalan untuk melindungi infrastruktur kritikal. Walaubagaimanapun, model-model ini sama seperti model berorientasi keselamatan yang lain dimana ia tertakluk kepada keadaan ketidakpastian dan strategi perlindungan infrastruktur kritikal yang komprehensif adalah untuk dapat mengurangkan pendedahan kepada risiko dan menangani ketidakpastian. Model *Cybersecurity Capability Maturity Model* (C2M2) untuk organisasi kewangan Nigeria adalah sebuah model yang berorientasikan keselamatan untuk menentukan tahap kekuatan keselamatan siber bagi organisasi-organisasi kewangan di Nigeria. Model yang dibangunkan ini menyediakan lima (5) tahap kematangan iaitu: i) Tiada apa-apa wujud, ii) Asas, iii) Kemajuan, iv) Lanjutan, dan v) Inovatif. Matlamat penyelidikan ini adalah untuk membina satu model yang dapat mengesahkan tahap kekuatan keselamatan siber bagi organisasi kewangan di Nigeria. Tujuh (7) organisasi merangkumi syarikat kewangan: Guarantee Trust Bank, United Bank for Africa, Union Bank of Nigeria, First Bank of Nigeria, Stanbic-IBTC Bank, Federal Mortgage Bank dan Polaris Bank yang terletak di Damaturu telah dipilih bagi diukur tahap kesediaan keselamatan siber bagi organisasi berkenaan menggunakan model yang dibangunkan ini. Temu bual secara berstruktur telah dilakukan terhadap pegawai teknologi maklumat bagi kajian kes ini. Analisis keputusan menunjukkan bahawa semua organisasi dalam kajian kes berada di tahap iv) Lanjutan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Cisco Inc define Cybersecurity as the practice of protecting network systems from digital attacks (Cisco, 2018). These attacks are usually planned at accessing, changing, or damaging sensitive data or interrupting common business processes(Cisco, 2018). Implementing efficient Cybersecurity procedures is mostly difficult today because the number of devices are more than the number of people (Cisco, 2018). Possible Cybersecurity threat nowadays as identify by Cisco Inc includes; Ransom ware, Malware, Social engineering and Phishing.

Cyberspace offer avenue for communications, Cybercriminals are lawbreakers that violet the use of Cyberspace whereas Cybersecurity is mean to protect Cyberspace. Also Cybersecurity is all about protecting data that is initiated in electronic form.

Cybercrime has become a new trend that is progressively rising as the IT continues to penetrate every aspect of our daily life and no one can guess its future (Omodunbi, Odiase, Olaniyan, & Esan, 2016). Casey consider Cybercrimes to be any illegal activities that involves computers and internet, including crimes that do not rely heavily on computers (Casey, 2005). According to (Adesina, 2017) Cybercrimes refers to any criminal activities which take place through the internet. Thus in general, Cybercrime refers to any crimes committed with the use of internet as tools to target any victim. It consist of crimes that have been made by computers, such as dissemination of computer viruses, network intrusions, identity theft and stalking.

For any organization to achieve the security of its cyberspace against cyber crime, the organization need to evaluate the level of their Cybersecurity capability

and search for their problem and solve them. Cybersecurity Capability Maturity Model (C2M2) is used as a tool to analyze the capability maturity level of organization to protect it critical infrastructure in cyberspace.

1.2 Problem Background

The development of the information technology (IT) and the increase access to web resources has give rise to new opportunities for financial transactions, as well as those who engage in illegal activities. Financial systems, all over the globe, play fundamental roles in the development and growth of the economy (Dai, Huu, & Zoltán, 2017). The rise of, and rapid progress in, IT based systems, are primary to essential changes in how financial organizations interact with their clients. Internet banking has turn into the self-service deliverance canal that allows banks and various other business to provide information and offer services to their clients more handiness via the internet (OECD, 2008). However, the presence of bank in the cyberspace has also give chance to cyber criminals to infiltrate into customers sensitive information such as credit card information. Over twenty years, dishonest cyber space groups have continued to use the internet to commit offenses; this has suggested mixed reaction of panic in the society along with a rising unease concerning the state of cyberspace security (Barclay, 2014).

Earlier to the year 2001, the trend of cyber crime was not internationally related with Nigeria (Adesina, 2017). From then, the country has acquired an international dishonor in cyber criminality, particularly identity theft, aided through the use of the internet. Since the issue of cyber security is raising attention in the mind of Nigerians, This dissertation give an overview of Cybercrime issues in Nigeria financial organizations, identify the categories of attack against the financial institutions in Nigeria, identify who are those actors and finally explain the challenges of mitigating such criminalities and to examine current Cybersecurity maturity models and propose a model that will be use by Nigerian financial organizations to evaluate their critical IT infrastructures applicability.

1.3 Problem Statement

Nigeria has a status for having a class of Cyber Threat actors popularly called 419 scams. These 419 scammers trick people into revealing their financial identities in other to use it and making money transfer. While these abuses have resulted in real financial damages, these Cyber Threat actors are seen as funny in the society. However, this is far from actuality and our image of Nigerian Cyber Threat actors must to be reorganized. Research carryout by professionals (Ibikunle & Eweniyi, 2013) shows that Nigeria has only 1,500 certified Cybersecurity Professionals and that the Nigeria is the most targeted nation of such attacks in Africa (Odumesi, 2014).

Strengthen the negative aspects of the problem is inadequate standards against which the Nigerian financial organizations can measure their current security status. To properly secure IT critical infrastructure and accurately report on its readiness to survive Cyberthreat, the Nigerian financial organizations need a common measurement tools in addition to NCSS standard controls and AUMMCS-1, to provide a framework for assessing and reporting Cybersecurity readiness. The Inadequate standard tools, Inadequate IT security professionals, immature cyber laws are the weakness to secure critical IT infrastructure among Nigeria financial organizations (Hassan, 2012).

To truly be effective, a Cybersecurity program must continually evolve and improve. This research focuses on addressing inadequate standard tools by developing a Cybersecurity capability maturity model for Nigeria financial organizations.

1.4 Research Aims

The main aim of this research is to develop a Cybersecurity Capability Maturity Model (C2M2) for Nigeria financial organizations.

1.5 Research Objectives

The objectives of the research are:

(a) To identify and investigate Cybersecurity capability security domain components based on the existing Cybersecurity capability models which are relevant to the financial organizations

(b) To develop Cybersecurity capability maturity model specific for critical IT Infrastructure security in financial organizations

(c) To evaluate the maturity level of the Cybersecurity capabilities for critical IT infrastructure among Nigeria financial organizations.

1.6 Research Questions

This research is carried out based on the following questions

(a) What are the Cybersecurity capability security domain components based on the existing Cybersecurity capability models relevant to the financial organizations.

(b) How to develop the Cybersecurity capability maturity model specific for critical IT infrastructure security in financial organizations.

(c) How to evaluate the maturity level of the Cybersecurity critical IT infrastructure among Nigeria financial organizations.

1.7 Research Scope

In order to reach the objectives stated above, the scope of this study is limited to the following:

(a) The study is focusing on Cybersecurity Capability Maturity Models and specially to Nigeria finacial organizations.

(b) Research assessment is accomplished by performing a fully in-structured interview with IT Officers in order to assess the maturity level of the selected case study as mention above.

1.8 Research Significance

The main significance of this research is to contribute to the development of the Cybersecurity area that will be easy for the Nigeria Financial organizations to apply to their organization in other to evaluate their strength in protecting their critical IT Infrastructure against any Cyberthreat.

1.9 Research Structure

This dissertation is structured into six chapters. To accelerate understandings to the dissertation, a brief overview of the contents of each chapter are as follows:

Chapter 1 Introduction of the research and serves as a road map to reader through brief description on the contributions of this dissertation.

Chapter 2 Literature Review for the dissertation through previous related published papers. This includes the reviews of research related to the method and process of C2M2 development.

REFERENCES

Adesina, O. S. (2017). Cybercrime and Poverty in Nigeria. *Canadian Social Science*, *13*(4), 19–29. https://doi.org/10.3968/9394

Adler, R. M. (2013). A dynamic capability maturity model for improving cyber security. *2013 IEEE International Conference on Technologies for Homeland Security (HST)*, 230–235. https://doi.org/10.1109/THS.2013.6699005

Angel, M. R.-G., Feliu, T. S., Calvo-Manzano, J. A., & Sanchez-Garcia, I. D. (2017). Comparative Study of Cybersecurity Capability Maturity Models, *770*, 114–127. https://doi.org/10.1007/978-3-319-67383-7

Barclay, C. (2014). Sustainable security advantage in a changing environment: The cybersecurity capability maturity model (CM2). *Proceedings of the 2014 ITU Kaleidoscope Academic Conference: Living in a Converged World - Impossible Without Standards?, K 2014*, 275–282. https://doi.org/10.1109/Kaleidoscope.2014.6858466

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing Maturity Models for IT Management. *Business & Information Systems Engineering*, *1*(3), 213–222. https://doi.org/10.1007/s12599-009-0044-5

Butkovic, M. J., & 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

Caralli, R., Knight, M., & Montgomery, A. (2012). Maturity models 101: a primer for applying maturity models to smart grid security, resilience, and interoperability, (November), 1–10. Retrieved from http://resources.sei.cmu.edu/asset_files/WhitePaper/2012_019_001_58920.pdf

Casey, E. (2005). Computer Crime and Digital Evidence. *Elsevier Ltd*, 429–435.

CBN. (2018). Risk-based Cybersecurity framework and guidelines for deposit money banks and payment service providers. *Animal Genetics*, *39*(5), 561–563. Retrieved from https://www.cbn.gov.ng/Out/2018/BSD/RISK BASED CYBERSECURITY FRAMEWORK Exposure Draft June.pdf

Christopher, J. D., Gonzalez, D., White, D. W., Stevens, J., Grundman, J., Mehravari, N., … Dolan, T. (2014). Cybersecurity Capability Maturity Model

(C2M2). *Department of Homeland Security*, (February), 1–76. Retrieved from https://energy.gov/oe/cybersecurity-critical-energy-infrastructure/cybersecurity-capability-maturity-model-c2m2-program

Cisco. (2018). Cisco 2018 Annual Cybersecurity Report. *Science and Engineering Indicators 2018*, 1–8. https://doi.org/10.1002/ejoc.201200111

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

Curtis, P., Mehravari, N., & Stevens, J. (2015). Cybersecurity Capability Maturity Model for Information Technology Services (C2M2 for IT Services), Version 1.0. *Defense Technical Information Center*, (April).

Dai, N., Huu, P., & 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

De Bruin, T., Freeze, R., Kaulkarni, U., & Rosemann, M. (2005). Understanding the Main Phases of Developing a Maturity Assessment Model. *Australasian Conference on Information Systems (ACIS)*, (December), 8–19. https://doi.org/10.1108/14637151211225225

Depoy, J., Phelan, J., Sholander, P., Smith, B., Varnado, G. B., & 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

Eshun, F. A. (2009). THE ROLE TELECOMMUNICATION ON BANKING SERVICES IN GHANA, 1–71.

Ferraiolo, K. (2000). The Systems Security Engineering Capability Maturity Model. *International Systems Security Engineering Association*, 64. Retrieved from https://csrc.nist.gov/csrc/media/publications/conference-paper/2000/10/19/proceedings-of-the-23rd-nissc-2000/documents/papers/916slide.pdf

FFIEC. (2015a). FFIEC Cybersecurity Assessment Tool, *3506*(1557).

FFIEC. (2015b). FFIEC Cybersecurity Assessment Tool Overview for Chief Executive Officers and Boards of Directors, *1*(June), 1–5.

GCSCC. (2014). Cyber Security Capability Maturity Model (CMM). *Global Cyber Security Capacity Centre University of Oxford*, (Cmm), 1–45. Retrieved from http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM Pilot version A.15.12.2014.pdf

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

Hansen, R. (2016). Cyber security capability assessment.

Hassan, A. (2012). Cybercrime in Nigeria: Causes, Effects and the Way Out. *ARPN Journal of Science …*, *2*(7), 626–631. Retrieved from http://www.ejournalofscience.org/archive/vol2no7/vol2no7_11.pdf

Humphrey, W. S. (1988). Characterizing the Software Process: A Maturity Framework. *IEEE Software*, *5*(2), 73–79. https://doi.org/10.1109/52.2014

Ibikunle, F., & 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

Jaquire, V., & Von Solms, S. (2017). Developing a cyber counterintelligence maturity model for developing countries. *2017 IST-Africa Week Conference, IST-Africa 2017*, (Cci), 1–8. https://doi.org/10.23919/ISTAFRICA.2017.8102288

Karokola, G., Kowalski, S., & Yngström, L. (2011). Secure e-government services: Towards a framework for integrating it security services into e-government maturity models. *2011 Information Security for South Africa*, (C), 1–9. https://doi.org/10.1109/ISSA.2011.6027525

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

László, K. (2009). Possible Methodology for Protection of Critical Information Infrastructures.

Lazarus, S. I., & Holloway, R. (2017). Causes of Socioeconomic Cybercrime in Nigeria, (October). https://doi.org/10.1109/ICCCF.2016.7740439

Le, N. T., & 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

Le, N. T., & Hoang, D. B. (2017). Capability maturity model and metrics framework

for cyber cloud security. *Scalable Computing*, *18*(4), 277–290. https://doi.org/10.12694/scpe.v18i4.1329

Limba, T., Plėta, T., Agafonov, K., & Damkus, M. (2017). Cyber security management model for critical infrastructure. *Entrepreneurship and Sustainability Issues*, *4*(4), 559–573. https://doi.org/10.9770/jesi.2017.4.4(12)

Mehravari, N. (2001). Everything you always wanted to know about PPRA. *Positive Living (Los Angeles, Calif.)*, *10*(2), 35–37.

Merriam, S. (2009). Qualitative Research A Guide to Design and Implementation Revised, 9.

MICT. (2014). National Cybersecurity Strategy, *Feel safe*. Retrieved from https://www.cert.gov.ng/file/docs/NATIONAL_CYBESECURITY_STRATEGY.pdf

Odumesi, J. O. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology*, *6*(3), 116–125. https://doi.org/10.5897/IJSA2013.0510

OECD. (2008). PROTECTION OF ‘ CRITICAL INFRASTRUCTURE ’ AND THE ROLE OF INVESTMENT POLICIES RELATING TO NATIONAL SECURITY May 2008 This report is published under the OECD Secretariat ’ s responsibility and was prepared by Kathryn Gordon (Senior Economist , OECD) and, (May). Retrieved from http://www.oecd.org/daf/inv/investment-policy/40700392.pdf.

Olayemi, O. J. (2014). Full Length Research Paper A socio-technological analysis of cybercrime and cyber security in Nigeria, *6*(3), 116–125. https://doi.org/10.5897/IJSA2013.0510

Omodunbi, B. A., Odiase, P. O., Olaniyan, O. M., & Esan, A. O. (2016). Cybercrimes in Nigeria: Analysis, Detection and Prevention *, *1*(1).

Othman, S. H. (2012). *Metamodelling Approach for Managing Disaster Management Knowledge*.

Paulk, M. C., Curtis, B., Chirssis, M. B., & V., W. and C. (1993). Capability maturity model, version 1.1. *IEEE Software*, *10*(4), 18–27. https://doi.org/10.1109/52.219617

Rea-Guaman, A. M., Sanchez-Garcia, I. D., Feliu, T. S., & Calvo-Manzano, J. A. (2017). Maturity Models in Cybersecurity: a systematic review. *Iberian Conference on Information Systems and Technologies, CISTI*.

https://doi.org/10.23919/CISTI.2017.7975865

Roger, B., Dorathy, K., James, A., Gloria, C., & Kerinia, C. (1995). Maturity Model Systems Engineering Capability Maturity Model Project, (November). Retrieved from http://resources.sei.cmu.edu/asset_files/MaturityModule/1995_008_001_16355.pdf

Röglinger, M., Pöppelbuß, J., & Becker, J. (2012). Maturity models in business process management. *Maturity Models in Business Process Management*, *18*(2), 328–346.

Saco, R. M. (2008). Maturity Models. *Industrial Management*, *50*(4), 11–15. https://doi.org/10.1081/E-ESCM-120047797

Schukat, M. (2014). Securing critical infrastructure. *DT 2014 - 10th International Conference on Digital Technologies 2014*, 298–304. https://doi.org/10.1109/DT.2014.6868731

Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying critical infrastructure sectors and their dependencies: An Indian scenario. *International Journal of Critical Infrastructure Protection*, *7*(2), 71–85. https://doi.org/10.1016/j.ijcip.2014.04.003

U.S. Department of Energy. (2014a). Electricity subsector cybersecurity capability maturity model, (February), 89. Retrieved from http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf

U.S. Department of Energy. (2014b). Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2), (February). Retrieved from http://energy.gov/sites/prod/files/2014/03/f13/ONG-C2M2-v1-1_cor.pdf

US Department of Homeland Security. (2014). Department of Homeland Security Cybersecurity Capability Maturity Model White Paper.

Vicente, A. (2007). Information Security Management Maturity Model.

Von Solms, S. H. B. (2015). A maturity model for part of the African Union Convention on Cyber Security. *Proceedings of the 2015 Science and Information Conference, SAI 2015*, 1316–1320. https://doi.org/10.1109/SAI.2015.7237313

Wendler, R. (2012). The maturity of maturity model research: A systematic mapping study. *Information and Software Technology*, *54*(12), 1317–1339. https://doi.org/10.1016/j.infsof.2012.07.007

White, G. B. (2011). The community cyber security maturity model. *2011 IEEE International Conference on Technologies for Homeland Security, HST 2011*, 173–178. https://doi.org/10.1109/THS.2011.6107866

Wood, M. (2018). Simple Methods for Estimating Confidence Levels, or Tentative Probabilities, for Hypotheses Instead of P Values, (March). Retrieved from http://woodm.myweb.port.ac.uk/