Modified Cybersecurity Capability Maturity Model (MC2M2), General Deterrence Theory and The Human Angle of Cybersecurity Risk

[1]Nnaa, L, L., [2]Nwaocha, V. & [3]Longe, O.B.
[1&3]Department of Information Systems, American University of Nigeria, Yola, Nigeria
[2]Department of Computer Sciences, National Open University of Nigeria, Abuja, Nigeria
E-mail: lawrence.nnaa@aun.edu.ng, onwaocha@noun.edu.ng, Olumide.longe@aun.edu.ng

ABSTRACT

This chapter re-assesses the reality of human security risk through the theoretical and conceptual framework of the Modified Cybersecurity Capability Maturity Model (MC2M2) and the General Deterrence Theory. The focus is to review the underlying issues of cyber security threat towards rethinking a way forward to mitigating threat posed by humans.

Keywords: General Deterrence Theory, Modified Cybersecurity Capability Maturity Model (MC2M2), Enterprise, Angle of Cybersecurity Risk

iSTEAMS Multidisciplinary Conference Proceedings Reference Format
Nnaa, L,L., Nwaocha, V. & Longe, O.B. (2019): Modified Cybersecurity Capability Maturity Model (MC2M2), General Deterrence Theory and The Human Angle of Cybersecurity Risk. Proceedings of the 22nd iSTEAMS Multidisciplinary SPRING Conference. Aurora Conference centre, Osogbo, Nigeria. 17th – 19th December, 2019. Pp 119-122. www.isteams.net/spring2019.
DOI - https://doi.org/ 10.22624/AIMS/iSTEAMS-2019/V22N1P10

1. INTRODUCTION

The biggest threat that businesses face today is tied to cybersecurity. This is the result of business migration from the analog and traditional systems to digital technologies which is celebrated as the pathway for organizational efficiency, productivity, growth and competitiveness. The risk of cybersecurity threat is enormous and sometimes demotivating for brands that may wish to migrate their operations to the cyberspace. Such losses could go from losing millions of dollars in profit to the total grip of the operations of the organization (Russ, 2017). Even though measures and countermeasures are recommended as a pathway to mitigating such threats, the cybercriminals do not rest on their oars; they continue to evolve new means of eroding the cybersecurity systems of organizations thereby exposing them to greater risk.

Generally, Information Technology Security Experts advocates for the building of strong, resilient and robust mechanisms to mitigate the threat of cybersecurity. Some of these mechanisms are system related especially when it comes to the servers and internet facilities but with the realization of human security components, human behavior and tendencies are also factored into the mix (Andress, 2011). Within this context of building strong mechanisms, the Cyber Security Capability Maturity Model (C2M2) has been advanced as a way of appraising the current security mechanisms to identify areas of Strength, Weakness, Opportunities and Threats (SWOT) of the security architecture of the organization towards improvement to achieve robustness, resilience and efficiency.

In this chapter, a key focus is placed on assessing the Modified Cyber Security Capability Maturity Model (MC2M2) for building a robust and resilient cybersecurity architecture that can withstand the growing threats in the local and globalized cybersecurity space. Following the tenets of the General Deterrence Theory, this chapter focuses on the human aspect of the Cyber Security Maturity Model which present indicators for assessing countermeasures that have been put in place to ensure that the human component of the organization does not expose the organization to an unwarranted cybersecurity attack.

2. HUMANS, THE NEW WINDOW OF ATTACK

One strand of a cybersecurity attack that has emerged over the years is the increasing social engineering risk. Smart right? Cybercriminals recognize that the mechanism for preventing cybersecurity risk for most organizations are becoming more advanced with the influence of protective technologies and firewalls (Alavi et al, 2015). It is nearly impossible for an outsider to successfully compromise the security architecture of the organization, of course, the focus of most organizations operating in cyberspace in either developing or developed countries is to protect their online resources from the prying eyes of attackers. But again, the changes in the working environment means that employees are now empowered in cyberspace more than ever. Staff is entitled to official emails, laptops and internet resources, working within the organization or remotely (Russ, 2017). Therefore, without the right orientation, training, policies and information, these staff become windows through which the organization cybersecurity systems and resources are penetrated to the advantage of the hackers. Such attacks come through the form of phishing, malicious spyware, spoofing, trojan and loads of other methods that are targeted at gaining access through user actions and inactions.

The real cybersecurity threat is no longer outside the organization, it is more inside. While Symantec report of 2017 showed that the volume of cybersecurity threats was growing by over 13% per annum, Cisco notes that over half of the risk faced by organization stems from multiple operations, employees and lines (Russ, 2017). Viewed from this lens, the greatest threat facing organizations is not the attackers but the internal employees from the management to the intern whose negligence, unprofessionalism and lack of due diligence continue to cost the organization (Chang, 2017). In recognition of these threats, the General Deterrence Theory has emerged as a dominant theme for reengineering the cybersecurity architecture of the organization, especially from the human dynamics. Developed by Schuessler (2009), the theory posits that measures be put in place to counter anti-social acts of employees which may expose the organization to risk. Such includes training, policies, reprimands and adoption of best practices among others. Fortunately, the Cybersecurity Capability Maturity Model includes some metrics for appraising human weakness and strength with a view to improving the security architecture.

3. DEALING WITH THE HUMAN SECURITY COMPONENT FROM THE PERSPECTIVE OF THE MODIFIED CYBERSECURITY CAPABILITY MATURITY MODEL (MC2M2)

The Cybersecurity Capability Maturity Model as shown in Fig. 1 below is a tool and an indicator, as a tool, it helps organizations to appraise their cybersecurity architecture for loopholes and as an indicator, it provides a guide for organizations to follow in improving their security architecture with a focus on both people and systems. This is hinged on a clearly defined approach of rating ten (10) distinct domain of an organization security architecture. These ten domain includes risk management; asset change and configuration management; identity and access management; threat vulnerability assessment; situational awareness; information sharing and communication; incidence response; supply chain management; workforce management; and cybersecurity program management.

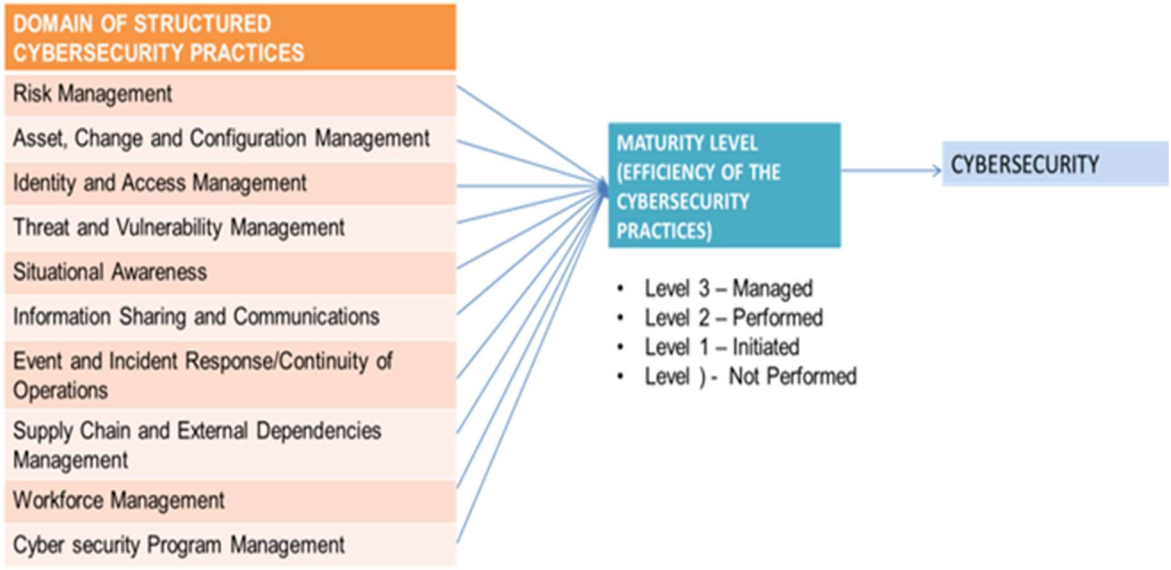

Fig 1. Cybersecurity Capability Maturity Model
Source: Huntsman (2019)

By sieving out human-related indices from the C2M2 model, the MC2M2 Model comes to light as noted in figure 2 below. In essence, situational awareness, information sharing/communication, incidence response and workforce management could determine whether the organization is more vulnerable or not. Using the abstracted domains from the C2M2 framework, MC2M2 aligns with the General Deterrence Theory which justifies a clearly defined framework for mitigating cybersecurity risk from the human angle (Jason, 2018). Thus, the best approach to dealing with the growing threat from insiders (employees and managers) going by the MC2M2 standpoint is to ensure that employees are aware of the situation, they receive the right communication (orientation), they are trained to respond to threats and the workforce management is efficient enough to minimise risk of attack. Fig 2 depicts the Modified Cybersecurity Capability Maturity Model (MC2M2)

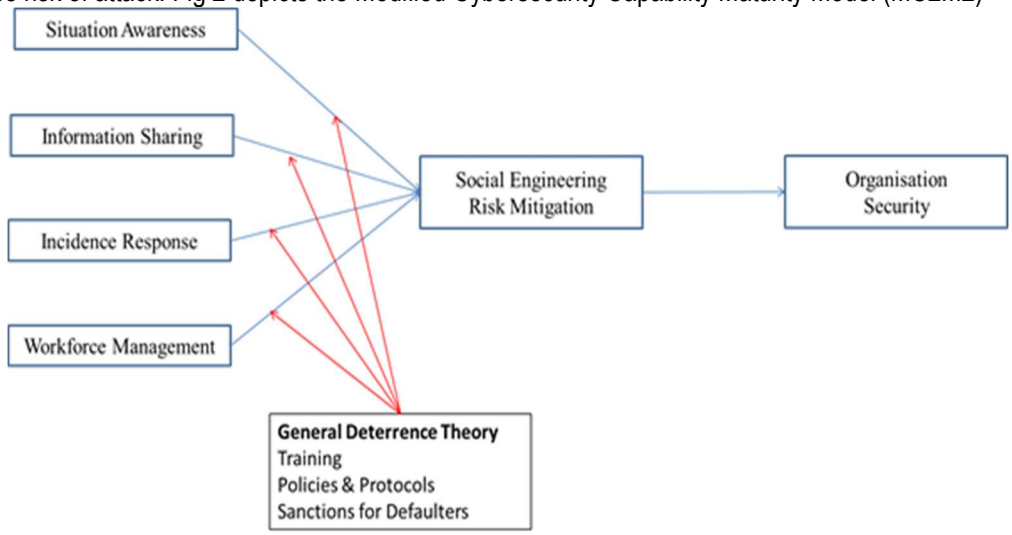

Fig 2: Modified Cybersecurity Capability Maturity Model (MC2M2)
Source: Author (2019)

3. COULD THIS BE A WAY FORWARD

As severally noted throughout the chapter, the era of engineering and re-engineering the cybersecurity architecture through more machines and software is fast phasing out. People architecture needs to be re-engineered towards complementing the asset and software modification to achieve resilience and optimal cybersecurity. Fortunately, MC2M2 offers a good starting ground for assessing "what is" compared to "What should be" or "What ought to be". The outcome of the comparative analysis would invariably form the basis for optimizing the overall human resource architecture towards countering the human-related risk aspects of the growing cybersecurity threats facing most organizations. This is not only backed by reason but the General Deterrence Theory which clearly emphasizes the need for policies, processes and measures to regulate employee actions in the workplace. However, this does not usurp the need for further research and refinement of thought.

REFERENCES

1. Alavi, R., Islam, S., Mouraditis, H. and Lee, S. (2015) Managing Social Engineering Attacks-Considering Human Factors and Security Investment. Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance.
2. Andress J. (2011) The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Elsevier, UK.
3. Chang, E. (2017). Clever hackers love call centers to tap into sensitive information. Available from https://www.thestreet.com/story/13964029/1/clever-hackers-love-call-centers-to-tap-into-sensitive-information.html [Accessed: 20th August, 2019]
4. Huntsman (2019) C2M2 Compliance. [Online] Available from: https://www.huntsmansecurity.com/solutions/cyber-security-compliance/c2m2-compliance/ [Accessed: 20th August, 2019]
5. Jason, C. (2018) The Cybersecurity Maturity Model: A Means To Measure And Improve Your Cybersecurity Program. [Online] Available from: https://www.forbes.com/sites/forbestechcouncil/2018/11/01/the-cybersecurity-maturity-model-a-means-to-measure-and-improve-your-cybersecurity-program/#48ee2fd680bc [Accessed: 20th August, 2019]
6. Russ, B. (2017) Cybersecurity threats proliferating for midsize and smaller businesses. [Online] Available from: https://www.journalofaccountancy.com/content/dam/jofa/issues/2017/jul/cyber-july-2017.pdf [Accessed: 20th August, 2019]