ISSN: 2230-9926

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

IJDR

International Journal of Development Research
Vol. 09, Issue, 07, pp. 28637-28641, July, 2019

RESEARCH ARTICLE OPEN ACCESS

CYBERSECURITY CAPABILITY MATURITY MODEL FOR NETWORK SYSTEM

***Idi Mohammed and Aliyu Musa Bade**

Department of Computer Science, Yobe State University Damaturu, Nigeria

ARTICLE INFO

Article History:
Received 17th April, 2019
Received in revised form
03rd May, 2019
Accepted 09th June, 2019
Published online 28th July, 2019

Key Words:

Cybersecurity, Maturity capability model, comprehensive, Systematic, Network.

ABSTRACT

A maturity model is a set of characteristics, attributes, indicators or patterns that signify the capability and the sequence in a particular discipline. A maturity model, therefore, provides a point of reference which an organization can assess their level current practices, processes and methods, and establish objectives and priorities for improvement. This article aims to describe and compare the most used Cybersecurity Capability Maturity Models, as a result of a comprehensive and systematic review of published studies on Cybersecurity Capability Maturity Model and to develop a Cybersecurity Capability Maturity Model for Network system. Comparison with existing valid models were used for conceptual model validation.

Citation: Idi Mohammed and Aliyu Musa Bade. 2019. "Cybersecurity capability maturity model for network system", *International Journal of Development Research*, 09, (07), 28637-28641.

INTRODUCTION

A maturity model is a set of characteristics, attributes, indicators or patterns that signify the capability and the sequence in a particular discipline (Rea-Guaman, Sanchez-Garcia, Feliu, & Calvo-Manzano, 2017). A maturity model, therefore, provides a point of reference which an organization can assess their level current practices, processes and methods, and establish objectives and priorities for improvement. The software development industry has been widely adopting the usage of maturity models since 1993 when the Capability Maturity Model (CMM) for software was first introduced twenty years ago (De Bruin, Freeze, Kaulkarni, & Rosemann, 2005). CMM was the beginning of the many research for maturity models and since then there are many attempts to apply the framework in other application domain (De Bruin *et al*., 2005). The assessment of an organization's capabilities in an application domain or specific process can be analyzed using maturity model (Röglinger, Pöppelbuß, & Becker, 2012). There are several levels in a maturity model and process of maturity ins form through these levels of logical path in the maturity model. The organization's capabilities in specific application domain as well as process are indicated through the maturity levels in the maturity model (Röglinger *et al*., 2012).

****Corresponding author: Idi Mohammed,***
Department of Computer Science, Yobe State University Damaturu, Nigeria

Organization can use the maturity model to analyze the level of the their maturity and use the result as a guide and aim to achieve a higher maturity level for the organization, or to use it to control the organization's progress as well as assuring their Cybersecurity capabilities (White, 2011). The sequence of levels in maturity models start from an initial state and the level ends in a mature state(U.S. Department of Energy, 2014). The level of maturity of an organization can be determined using maturity model by evaluating elements that has been selected and rating the capabilities of the elements. Actions needed to be done to increase the level of maturity for the elements (Hansen, 2016). The total number of levels in a maturity models might differ from each model and the more level a maturity level have, the more difficult it will be to provide a description for each level (U.S. Department of Energy, 2014). The complexity of the maturity model will also increase as the number of levels increases. (Angel, Feliu, Calvo-Manzano, & Sanchez-Garcia, 2017). According to the review by (Angel *et al*., 2017), the C2M2 that are mainly revealed in scientific research papers are Cybersecurity Capability Maturity Model(C2M2), Systems Security Engineering Capability Maturity Model (SSE-CMM), Community Cyber Security Maturity Model (CCSMM) and National Initiative for Cybersecurity Education – Capability Maturity Model (NICE). This research explore more C2M2 that relevant to Cybersecurity in addition to C2M2, SSE-CMM, CCSMM and NICE. Comprehensive and systematic

review were carried-out in this research, Components validate and C2M2 for network system develop.

Literature Review: Cyber threats are one of the most serious and challenging types of operational risk facing modern organizations (Curtis, Mehravari, & Stevens, 2015). The national and economic security of the world depends on the reliable functioning of the information technology services that serve the Nation's critical infrastructure in the face of such threats. Beyond critical infrastructure, the economic vitality of the Nation depends on the sustained operation of the enterprise information technology (IT) services of organizations of all types (Paulk, Curtis, Chrissis, & Weber, 2006). Systematic and comprehensive literature review on Cybersecurity Capability Maturity Model for network related infrastructure are discuss in this section.

C2M2 for IT Services (Curtis *et al*., 2015): C2M2 for IT Services focuses on the evaluation of Cybersecurity practices related with typical enterprise IT services, along with allied enabling IT assets and the platform in which they operate. It is based on a combination of existing Cybersecurity Capability Maturity Models.

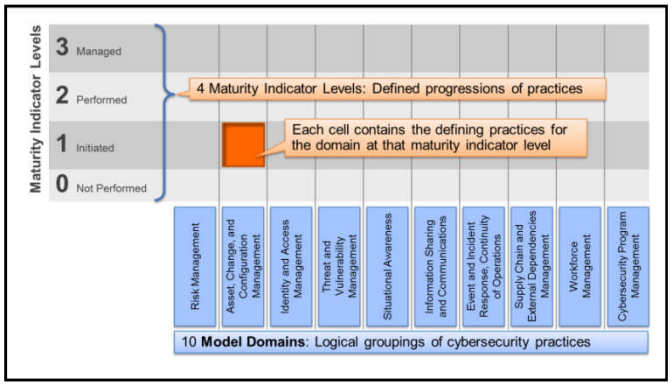


Figure 2.1. C2M2 for IT Services (Curtis *et al*., 2015)

As presented in Figure 2.1, the model is organized with ten (10) domains and four (4) maturity indicator levels.

Electrical Subsector Cyber Security Capability Maturity Model (ES-C2M2) (Adler, 2013): ES-C2M2 is an extended CERT CMM called the Electrical Subsector Cyber Security Capability Maturity Model, or ES- C2M2 (Adler, 2013). ES-C2M2 defines ten domains of Cyber Security performance: Risk, Asset, Access, Threat, Situation, Sharing, Response, Dependencies, Workforce, and Cyber. Each domain in ES-C2M2 encompasses several objectives. Each objective, in turn, consists of a set of Cyber Security practices. ES-C2M2 is reasonably uncomplicated, an organization can classify the practices vital for each objective in the related ES-C2M2 domains to progress towards the needed maturity levels. ES-C2M2 confirm Nothing Exists, Basic, Progressed, Advanced, Risk Management, Governance, Access control and Incidence Management.

Systems Security Engineering Capability Maturity Model (SSE-CMM): (Roger, Dorathy, James, Gloria, & Kerinia, 1995) The SSE-CMM was design with six maturity levels, namely ; not Perform, Performed Informally, Planned and Tracked, Well Defined, Quantitatively Controlled, and Continuously Improving (Angel *et al*., 2017).

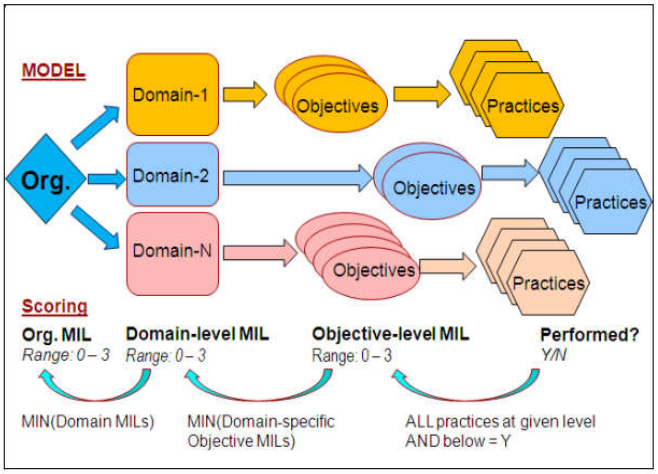
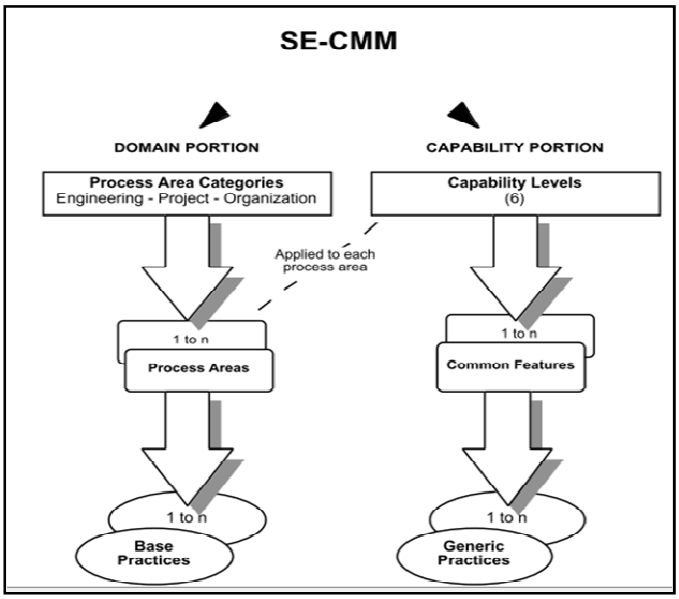


Figure 2.2 Electrical Subsector Cyber Security Capability Maturity (Adler, 2013)



The SSE-CMM model is considered a general model not focus more on Cybersecurity, but it is a model that has been adapted for that reason due to the lack of models particular to Cybersecurity (Angel *et al*., 2017).

Global Cyber Security Capacity Centre (GCSCC)

Cybersecurity Capability Maturity Model (C2M2) (GCSCC, 2014) The Global Cyber Security Capacity Centre-C2M2 was develop by Oxford University Global Cyber Security Capacity Centre in 2014. With the mission to increase the scale and effectiveness of cyber security capacity building, both within the UK and internationally(GCSCC, 2014) . This Model considered cyber security capacity in dimensions; devising cyber policy and strategy, encouraging responsible cyber culture within society, building cyber skills into the workforce and leadership , creating effective legal and regulatory frameworks and controlling risks through organization, standards and technology (GCSCC, 2014). The Model comprises of five levels of maturity in the Capability Maturity Model; Start-up, Formative, Established, Strategic and Dynamic. Graphical representation was not provided in the model documentation.

Community Cyber Security Maturity Model (CCSMM): The CCSMM is design to address the requirements of U.S

communities to develop a practicable and sustainable plan for Cybersecurity. The model defines five maturity levels; Initial, Established, Self-assessed, Integrated, and Vanguard (White, 2011).

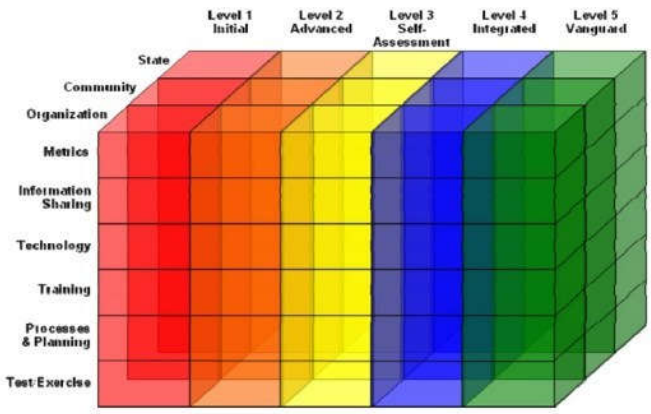


Figure 2.5. Community Cyber Security Maturity Model (White, 2011)

Community Cyber Security Maturity Model uses the community knowledge of Cybersecurity, Cybersecurity training and education, security policies and procedures and sharing of information within and outside organizations in order to evaluate their strength against Cyberattacks.

Capability Maturity Model and metrics framework for Cyber Cloud Security (CMMCCS) (Le & Hoang, 2017)**:** This Model address cloud computing Cybersecurity issues (Le & Hoang, 2017). It provides the guidance to support the organizations implement and enhance their cyber security capabilities on cloud system (Le & Hoang, 2017). CSCMM outline twelve (12) domains; Governance, Risk, and Compliance management, Audit and Accountability, Identities and Access Management, Data and Information protection, Incident response, Infrastructure and facilities security, Human resource management, Security awareness and training, Cloud application security, Virtualization and isolation, Interoperability and portability, and finally Cloud connections and communication security.

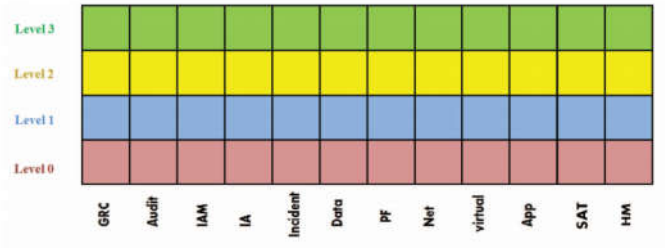


Figure 2.5. Capability Maturity Model and metrics framework for Cyber Cloud Security (CMMCCS) (Le & Hoang, 2017)

CMMCCS comprises four (4) maturity levels range from level 0, level 1, level 2 and level 3. No further description to were given to these maturity levels.

Cybersecurity Capability Maturity Model (C2M2) (Christopher *et al*., 2014) The C2M2 focuses on the implementation of Cybersecurity practices associated with the information technology (IT) and operations technology (OT) assets and the environments in which they operate (Christopher *et al*., 2014).

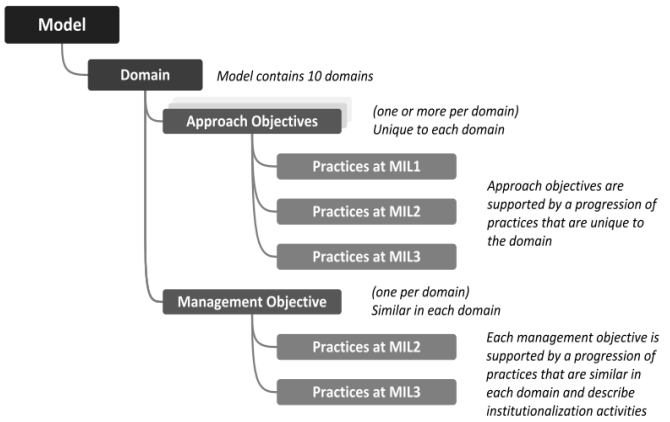


Figure 2.6. Cybersecurity Capability Maturity Model (C2M2) (Christopher *et al*., 2014)

The model also comprises of four maturity levels (i.e. no practices, initial practices, stable practices and practices stabilized) which are applied in parallel to each model domain. According to (Angel *et al*., 2017) the model regarded as descriptive rather than prescriptive. The Model focus on ten (10) sets of Cybersecurity practises

Identification of common Components: After literature review of existing seven C2M2s, twelve components were indentified, namely; 1) Noting exists. 2) Basic. 3) Progressed. 4) Advanced. 5) Innovative. 6) Legal Regulation. 7) Governance. 8) Technology Management. 9) Incidence Management. 10) Access Control. 11) Risk Management. 12) Security Culture.

Estimating Degree of Confidence of identified components : Degree of Confidence (DoC) is a real number in the range [0,1] that expresses the reliability of the estimate (Wood, 2018). DoC is calculate using the formula [1]. The obtain results will be refers to as score in the process.

$$\text{Degree of Confidence (DoC)} = \frac{Frequency\ of\ ceoncept}{Total\ Valid\ Models} \times 100 \quad ----[1]$$

Table 2.1 present the summary of comparison identified components against other valid models discuss in the Comparison against other models. The higher their score, the more significant the concepts are considered to the C2M2 domain. Concepts that have a low down score are likely for deletion. Table 2.2 shows five (5) categories of concepts based on their DoC are defined.

Table 2.1 Degree of Confidence Result interpretation

Doc Score (Range in %)	DoC Result
70-100	Very Strong
50-69	Strong
30-49	Moderate
11-29	Mild
0-10	Very Mild

(Othman, 2012)

As presented in Table 2.1, very strong DoC is assigned to concepts that appear frequently in the valid models, whereas Very Mild DoC is other end of the scale. Table 2.2 presents DoC values all identified concepts. From Table 2.2 and Figure 2.7, result of DoC show that two component of identified are liable to be drop. The components are Technology Management and Access Control. Figure 2.7. present graphical frequency of identified components and their strength.

Table 2.2 Comparison of identified components against other valid models with frequency and DoC values

Identified Components	Valid Models							Frequency	DoC
	C2M2 for IT Service(Curtis et al., 2015)	ES-C2M2 (Adler, 2013)	SSE-CMM (Roger et al., 1995)	GCSCC-C2M2 (GCSCC, 2014)	CCSMM (White, 2011)	CMMCCS (Le & Hoang, 2017)	C2M2 (Christopher et al., 2014)		
Noting exists	√	√	√	√			√	5	71
Basic	√	√	√	√	√		√	6	85
Progressed	√	√	√	√	√		√	6	85
Advanced	√	√	√		√		√	5	71
Innovative			√	√	√			3	43
Legal Regulation				√	√		√	3	43
Governance	√	√	√	√		√	√	6	85
Technology Management				√				1	14
Incidence Management	√	√	√	√		√	√	6	85
Access Control	√	√						2	28
Risk Management	√	√	√	√		√	√	6	85
Security Culture	√		√	√	√	√	√	6	85

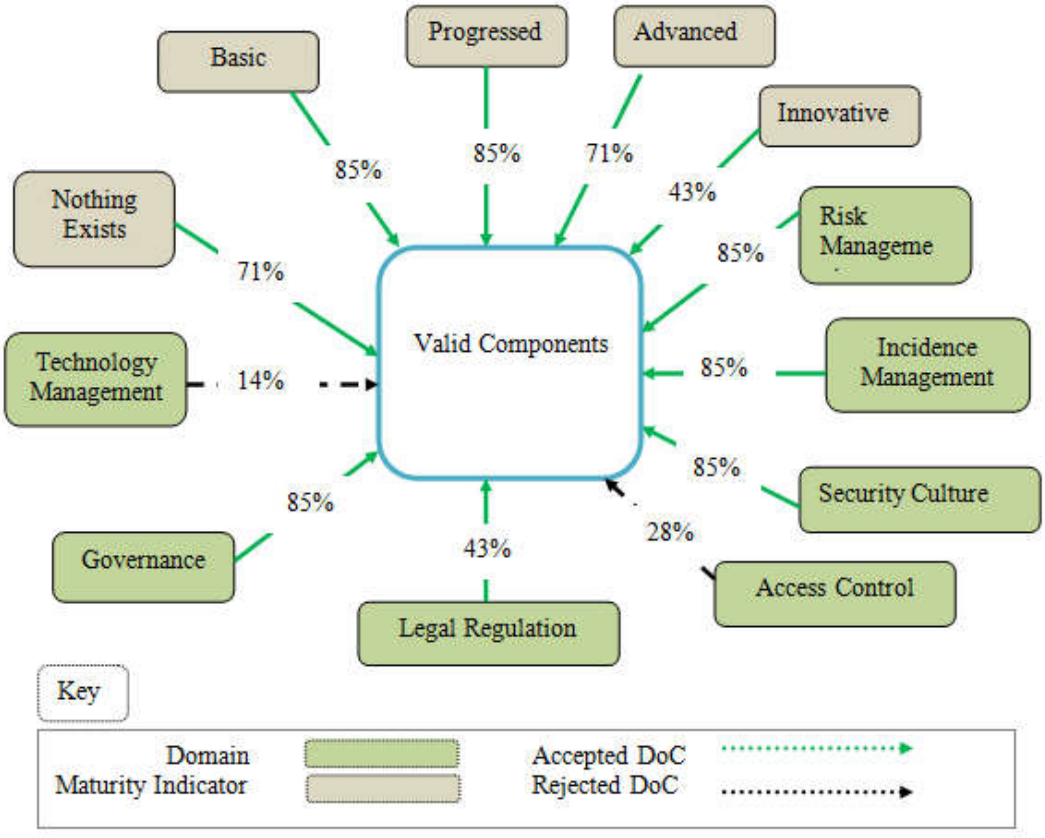


Figure 2.7. Star view of Comparison of identified components against other valid models with frequency and DoC values

RESULTS AND ANALYSIS

The features that were defined to evaluate the models were defined previously in section 2.8. After analysing the Cybersecurity capability maturity models obtained from the systematic review in section 2, a table was made summarizing the comparison among them. The comparative study shows that the C2M2s have a major similarity. The main variation is identified in the application sector which they are designed for. This research discover C2M2 (presented in figure) for that will suite any network system.

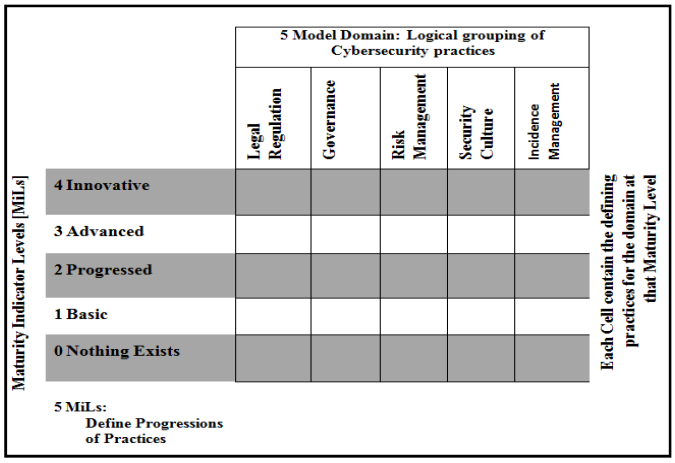


Figure 2.8. C2M2 for network system

Conclusion

An increase dependency on IT infrastructure by organizations has courses an increases in Cyberattacks to their operational. This research produced a five-level maturity model for evaluating Cybersecurity preparedness among network systems.

REFERENCES

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

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

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

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

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

Hansen, R. 2016. Cyber security capability assessment.

Le, N. T. and 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

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

Paulk, M., Curtis, B., Chrissis, M., & Weber, C. 2006. The Capability Maturity Model for Software. Software Engineering Project Management, 1–48. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:The+Capability+Maturity+Model+for+Software#0

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., Pöppelbu ß, J., & Becker, J. 2012. Maturity models in business process management. Maturity Models in Business Process Management, 18(2), 328–346.

U.S. Department of Energy. 2014. 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

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/

****