ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 4, 762-769 (2020)

www.astesj.com

Special Issue on Multidisciplinary Sciences and Engineering

xASTESJ

ISSN: 2415-6698

An Explanatory Review on Cybersecurity Capability Maturity Models

Adamu Abdullahi Garba[1,*], Maheyzah Muhamad Siraj[2], Siti Hajar Othman[2]

[1]*Yobe State University Damaturu, Computer Science, Yobe State University Damaturu, 1144, Nigeria*

[2]*School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia, 81310, Malaysia*

ARTICLE INFO

Article history:
Received:26 June, 2020
Accepted:14 August, 2020
Online: 28 August, 2020

Keywords:
Cybersecurity Maturity Model
Capability Maturity Model
Security Models
Confidentiality

ABSTRACT

Cybersecurity is growing exponentially day by day in both the public and private sectors. This growth also comes with a new and dynamic cyber-threats risk that causes both sectors' performance to halt. These sectors must update their cybersecurity measures and must understand the capability and maturity of their organization's cybersecurity preparedness. Cybersecurity maturity models are widely used to measure how ready an organization is when it comes to cybersecurity. The main aim of this article is to conduct a comprehensive review of the current cybersecurity capability maturity models using a systematic review of published articles from 2011 to 2019. A comparative study was conducted based on Halvorsen and Conradi's taxonomy. The review indicated almost all the cybersecurity maturity model consists of similar elements like maturity levels and processes but significantly lacks the validation process, it was observed each of the models were predominantly designed for a specific purpose and also for different organization size and application domain.

1. Introduction

Cybersecurity is a method of protecting organization assets, through the identification of threats that can compromise the critical information stored in the organization systems, it also involves the protection, identification, and responding to threats. However, cybersecurity evolves from computer security which means securing the physical components of a computer system from any damage, to information security which means securing the stored information in a computer system from unauthorized assess by maintaining it Confidentiality, integrity and availability (CIA) then to cybersecurity which includes both computer security and information security and also adding the security of information being transferred across a different medium (wired & wireless) and also access from anywhere. The advancement of the cybersecurity domain is dated back to the 1950s. The field of cybersecurity emerged as a result of Robert Morris testing the worlds' network vulnerability in 1980 when he uses a virus he created to test the size of the internet, to protect organization assets, an organization needs to improve their cybersecurity practices. The knowledge of cybersecurity has also been used negatively, the Russian in the 1980s attacked around 400 military computers in the US which include the pentagon computers[1–3]. Therefore, knowledge of cybersecurity capability maturity models is essential as the research area is new and growing exponentially, critical review in the existing models and their applications is important to know, to fill this gap this paper intends to answer the following objective:

- To identify currently available cybersecurity capability maturity models available for this study from 2011 to 2019 using systematic review (SR).
- To identify the main difference between the cybersecurity capability maturity model and their levels
- To understand the application of the cybersecurity capability maturity models.

This paper consists of eight sections, section 1 is the introduction, the second section 2 discusses on the evolution of cybersecurity capability maturity models, section 3 discusses on the method used in conducting the research, section 4 explains the Review on cybersecurity capability maturity models, section 5 explains the results and discussion of the comparative analysis of the identified models, it further discusses the importance of the research and explained how the objective was achieved, section 6 explains the future direction of the research and from where other authors can continue to explain the research direction and lastly, section 7 is the conclusion.

*Corresponding Author: Adamu Abdullahi Garba, adamugaidam@gmail.com

1.1. Review Method and Protocol

The systematic literature review is defined as " a well-defined study or methodology for identifying, analyzing, and also interpreting all available evidence related to a specific research question [4,5]. This method was mostly used in medicine [6], but not now it has been adopted by many fields of studies like social science, information system, and computer science, software engineering [5]. In this study systematic review, "which aims for exhaustive searching, quality assessment, inclusion, and exclusion criteria which are typically narrative with tabular form was adopted "[7]. The aim or analysis of this method is to explain what is known for practices, what remains unknown, and recommendation for future research.

This systematic search started with a well-developed review protocol based on the procedures of the SR review. The protocol includes: background study as evolution, review method, research objectives, and data extraction criteria, and for this study. This section helps to increase the accuracy of the review and also reduces bias in conducting the research. Table 1 describes the review criteria.

Table 1: Inclusion and exclusion criteria

Included article	Excluded article
Full text and available	Full text but not available
Year of publication from 2011 – 2019	Outside range of the year
Published in English	Non-English
Only focus on the domain (cybersecurity)	Were outside domain
Must be a model	Not related to objectives
Found in the selected database.	Duplicated studies

1.2. Inclusion and exclusion criteria

This section is mainly to set up the criteria of inclusion and exclusion for the researchers to follow when doing the study. This research considers the following articles (emerald, IEEE explore, Scopus, the web of science and science direct) published in English, also published from 20011 to 2019 in the digital database. Table 1 shows the steps used in conducting the research.

As part of Step1, we searched articles that have the phrase "cybersecurity", "security model" AND "maturity", from different databases. After following the protocol mention in table 1, we collected 220 articles relevant to your objective

Step 2 is where we used the inclusion and exclusion criteria to determine article very close to your objective by reading abstract [5], we removed all the papers that do not have the word "cybersecurity model" and "cybersecurity capability maturity model". At the end of this phase, we only obtained 30 articles.

Step 3, the article obtained in step 2 was critically analyzed and read fully with more depth analysis. Based on the full- text, the previous criteria were applied to identify the actual articles that are related to our objective. The articles used are fully cybersecurity oriented. At the end of this phase, only 7 articles were obtained. These seven articles are selected based on table 1 criteria.

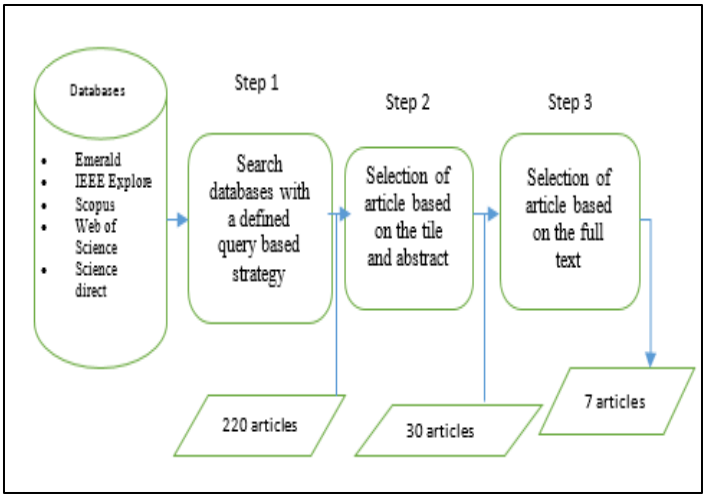

Figure 1. Search and selection of articles considered for this study.

2. Cybersecurity Capability Maturity Models

The cybersecurity Capability maturity model has emerged from the capability maturity model been design from the quality management field in the 1930s. it becomes popular in the 1990s when it was first developed by software engineering institutions [8]. Today all these models are based on this basic model, the model has a set of a structured set of operations and activities that improve over time [9]. the model is later being adapted into many fields of studies to identify or measure the maturity level of an organization or process or even product quality as they are widely known. The capability maturity model (CMM) which was for software industries has some key elements for an effective software development process[10] the model has 5 basic process maturity levels called, initial, repeatable, defined, managed, and optimizing [11]. A best- practices and process efficiency is provided for every five levels of each process for evaluating the maturity [12]. Also [13] conducted a study regarding the capability maturity models, in his research he identified and compares many maturity models for software domain and product quality, while [14] surveyed maturity models specifically for knowledge management to find out how far it contributed to the measurement of knowledge management, but the study only emphases on one special type of maturity model, therefore it is not suitable for general mapping of the maturity model research, the model was designed for software products as guidance as well as for management excellence in producing quality software"[15].

The cybersecurity maturity model offers a framework for assessing the maturity of a security program and guidance on how to reach the next level [16]. The cybersecurity maturity model provides a pathway that enables the organization to measure where they are along that path. This can be a valuable tool not only for improving Cybersecurity efforts but also for collaborating with upper management and getting the support needed to enhance Cybersecurity culture in organizations. There are various Cybersecurity Maturity Models from which to choose, Based on the systematic review performed regarding the currently available Cybersecurity models published to the knowledge of the author from 2011 to 2019 are; Cybersecurity Capability Maturity Model (C2M2), Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), Oil and Natural Gas Subsector

Cybersecurity Capability Maturity Model (ONG-C2M2), National Initiative for Cybersecurity Education-Cybersecurity Capability Maturity Model (NICE-C2M2), Community Cyber Security Maturity Model (CCSMM), African union maturity model for cybersecurity (AUMMCS) and Federal Financial Institute of Examination Council Capability Maturity Model (FFIEC- CMM). These identified models are selected because they focus on cybersecurity, other models were found during the SR but were not fully focusing on cybersecurity, like the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), The NIST CSF differs from the C2M2, as NIST doesn't consider the CSF a maturity model, Instead of 10 domains, NIST represents five Cybersecurity functions: identity, protect, detect, respond and recover Models identified section 5 shows Comparisons Cybersecurity Capability Maturity Models results then followed by a discussion on the Comparisons Cybersecurity Capability Maturity Models.

3. Methodology

Based on the systematic review performed regarding the currently available cybersecurity capability maturity models published, the author has identified the following: C2M2, ES-C2M2, ONG-C2M2, NICE-C2M2, CCSMM, FFIEC- CMM, and AUMMCS as explained in the previous section. The author adapted Halverson and Conradi taxonomy of software process improvement (2001), this taxonomy consists of 21 features peculiar to software process and is grouped into 5 categories: **general, process, organization, quality**, **and result**. Each category refers to:

- **General**: the features that describe the overall attribute of improvement.
- **Process:** the feature that explains the way the organization uses the features.
- **Organization**: this explains the relationship between the features and organization and how they work simultaneously.
- **Quality:** this explains the feature related to the quality dimension.
- **Result:** this explains the feature of the results as the result of using the environment, the cost of achieving the result. In this paper, only **general, process, organization, and result**s are adapted as the other one has no relation to Cybersecurity Capability Maturity Models. The feature that falls under each category is modified to suit Cybersecurity terms as shown in Table 2 below.

Table 1: Halverson and Conradi taxonomy

Category	Feature
General	Cybersecurity oriented
	Origin
	Purpose
	Prescriptive/ descriptive
	Maturity level
Process	Field Applicable
	Define role
	Depth of assessment
	Assessment
	Assessor
Organization	Actors
	Organization size
	Level of documentation
	Organization Environment
Result	Implementation cost

The features related to ***General*** group are defined below:

- **Cybersecurity Oriented:** this feature depicts which model was purposely designed for Cybersecurity maturity.
- **Origin:** this criterion is used to know the country, lab, organization that created or design the model e.g. the US.
- **Prescriptive/Descriptive**: the criteria used here is either Prescriptive: if the model is enforcing a rule to be used if the model is adapted, while descriptive: if a model is describing or classifying its objectives and how to follow it, not enforcing rules.
- **Maturity Level**: the criteria are used to understand the level of maturity for each model number 1- 5 are used, the more level a mode is the more level of the maturity increases.
- **Field Applicable**: the criteria is used to know the area where the model is applicable criteria include: organization, paper lab. University.
- **Define Role**: this feature explains how well the roles and functions are evaluated using " Yes" if a role is defined and else " No" is used.
- **Depth of Assessment:** the criteria are used here is either "General" if the assessment is not in-depth and "specific" if the assessment is in-depth that is more than one level.
- **Actors**: the criteria used here are " management, staff, communities or states " to know who is using the model directly.
- **Organization Size**: this criterion is used to know the size of the organization for appropriate adaption, criteria used here are: large, medium, small, or all.
- **Level of Documentation**: criteria use are either "high" when a model has implementation guide and other supporting documents that will help adaptor to implement the model, "medium "is when no more details are available on the implementation guide but there are white papers and other supporting documents, "low" in both implementation and white paper are not available but other introductory documents are available.
- **Organization Environment**: criteria "Overall" is used if the model focuses on the entire organization while " Explicit" if the model focuses on a specific unit or department in the organization.
- **Assessment:** the feature is explained by the name of a process to be assessed in the organization e.g. risk, maturity, customer, employee, organization.
- **Assessor:** the criteria use in this feature are " internal" if the assessor is from the environment the model is implemented, " external" if the assessor comes from outside the workplace, and "internal and external" where the assessor can be both.

- **Validation Method**: this criteria is use to know the method of validation includes: survey, case study. Experiment.
- **Implementation Cost**: this criteria is use to know how much to spend when implementing the model.

4. Review

This section explains the main structure and domain found in the identified maturity models based on their focus on cybersecurity. Based on the SR the identified from scientific articles are C2M2, ES-C2M2, ONG-C2M2, NICE-C2M2, CCSMM, FFIEC- CMM, and AUMMCS models.

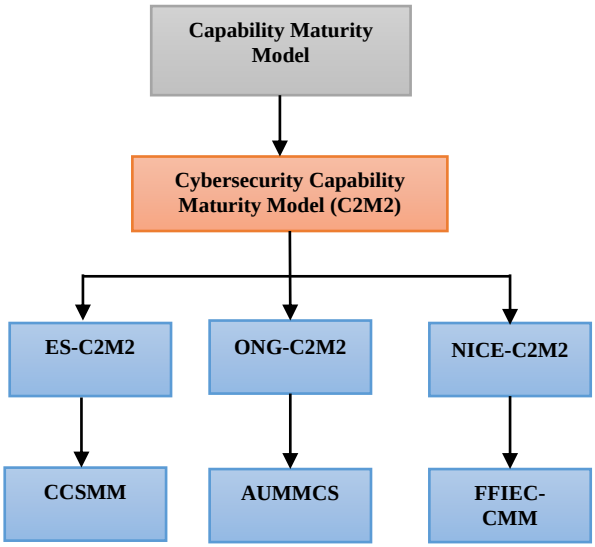

Figure 2: Descriptive diagram of maturity models

Figure 2 above elaborates more on the identified maturity models, it indicates C2M2 is the origin or the first model to be designed in the cybersecurity domain, The difference from the models is either from the number of levels like C2M2 has 4 levels while CCSMM has 5 levels, application area, also C2M2 can be assessed both internally and externally while CCMM can only be asses externally. However, the most important concept of all is that they are only design for cybersecurity specifications, i.e cybersecurity orientation.

4.1. Cybersecurity Capability Maturity Model (C2M2)

The Cybersecurity Capability Maturity Model was designed by Carnegie Mellon University in collaboration with the US Department of Energy in 2014 [17]. The model has ten domains and each domain is a grouping of cybersecurity practices. Also, many objectives are grouped to be in one domain which represents achievements the model contains ten domains with grouped objectives and Maturity levels. (Appendix *A shows the domain and also the maturity level*)

4.2. Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)

The Electricity Subsector Cybersecurity Capability Maturity Model was designed by the department of energy USA to protect the electricity subsector from any form of cybersecurity attacks. [18]. This model was designed as a subsector of the C2M2 i.e. Independent guidance. Both models' general purpose is almost the same, which is to improve cybersecurity capabilities by allowing continuous benchmarking. This model also has ten domain and are the same as the C2M2. The model was developed with the main four primary sector functions as listed below.

- Generation
- Transmission
- Distribution
- Markets

There is a difference between the models in reporting of incidents, C2M2 mentioned ISACs in general in the DOE form while ES-C2M2 threat and vulnerability incident are reported to electricity sector information sharing and analysis center specifically [18]. The model is purposely for electricity sector organizations.

4.3. Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2)

The Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model was developed or derived from ES-C2M2 first version, the main reason for this model was to address the threats and vulnerabilities uniquely characterized by the Oil and Gas subsector. This model can be used to support cybersecurity capabilities in the ONG subsector, it enables organizations to evaluate and benchmark their capabilities. The ONG-C2M2 was designed to address problems in the oil and gas sector only. The development process was extensively cantered with public and private sector experts through pilot facilitation, working sessions. This model uniquely includes the exploration, gathering, production, processing storage, and transportation of petroleum liquids and natural gas. The critical areas where threats can occur, from exploration to storage as technology is used to do all the processes, where security has been not tightened well, an attacker from nowhere can hinder the process or even stops the organizational activities. The ONG-C2M2 and the ES-C2M2 are derived from the C2M2, therefore they share the same domain and maturity levels only place of applications, and the purpose of design differs. This is the reason the author did not repeat the same tables to avoid repetitions, see Appendix *A shows the domain and also the maturity level*)

4.4. National Initiative for Cybersecurity Education Capability Maturity Model (NICE)

The NICE model was designed by then US President George Bush under the directive of national security in 2008, [19]. The model was designed purposely to select the staff with cybersecurity background and skills. The model comprises three key components focusing on staff security structure at the management and the role of staff, the model was officially published in 2014 [19]. The model consists of three domains: Process and Analytics, Integrated Governance, and Trained Professionals and Enabling Technology, which also three maturity levels (*limited level, progressing level, and optimized level*).

4.5. Federal Financial Institute of Examination Council Capability Maturity Model (FFIEC- CMM)

The Federal Financial Institute of Examination Council Capability Maturity Model was published to guide or navigate the increasing complexity of the cyber risk landscape. This assessment tool was designed to help managers assess their institution's cybersecurity preparedness, evaluate its risk, and determine what risk management practices and controls are needed to attain the desired state. This tool has two-part as shown below:

- **The Inherent Risk Profile**: these are risks posed to the organization by technologies and connection types, delivery channels, online and mobile products, and other external threats.
- **Cybersecurity Maturity**: this helps the organization to measure the level of risk and corresponding controls. The level starts from baseline to innovation. The model contains five domains and some assessment factors

4.6. African Union Maturity Model for Cybersecurity (AUMMCS)

The African union maturity model for cybersecurity was made available in 2014 by the center for the cybersecurity at the University of Johannesburg on security and protection of personal data at the convention of African member states, this model covers three sections: *electronic transactions, personal data protection and promoting cybersecurity and combating cybercrime* [20]. The model was intended to help member states of the African Union to evaluate their cybersecurity status against a specific part of the convention. This model can be utilized in two ways: one as a self-assessment by a specific country against the specification of the convention, two as a comparison by the AU between different member states in other to see how they can compare themselves as requirements are concerned. The model only covers the promotion of cybersecurity and combating cybercrime[20]. The model has four objectives:

- A national culture of cybersecurity does exist.
- A national Cybersecurity policy does exist.
- Public-private partnerships, initiated by the government, do exist.
- Cybersecurity capacity building on all levels, driven by the government, does exist.

The model also has four MLS maturity levels:

- ML0: Nothing Exists At All.
- Ml1: Very Basic Position.
- Ml2: Progressed Position.
- Ml 3: Stable Position.

4.7. The Community Cybersecurity Maturity Model (CCM2)

The community cybersecurity maturity model was developed in San Antonio Taxes by the Centre for Infrastructure Assurance and Security (CIAS) [21]. this model was designed to the needs of state and community to the development of a practical and sustainable program of cybersecurity in taxes United States. This model identified the character of community and state as their cyber-security program mature, such aspect includes knowledge, security policies, procedures, information exchange, and cybersecurity training and education. The main importance of this model is to respond to the linkage that exists among states since more communities made up a state. Also, the model is shown in a three-dimensional way [21]. This model is made up of five maturity levels with the lowest initial level showing characteristics for communities that do not share a minimal level of cyber preparedness in the four key areas knows as *Awareness, information sharing, processes and procedures, and integration.* [21]. An example, like top managers at level one, would have little or even no awareness of any cybersecurity threat and its damage, also have little or no information sharing on the cyber event between entities within organization cities or states. Also, few processes or procedures would be in place in the community to handle any cyber threat and lastly, lack of or no mechanism in place (security exercise) to evaluate the level of preparedness of the community or its capacity to respond to any threats. Initially, the model focus on designing the roadmap for the community to follow than later was identified that it is not yet robust enough to adequately represented what is needed for a community to be secure individual community must have a certain level of security as well program necessary to address prevention and detection of cyber threats. The model shows how important information sharing is with other communities so that current threats picture can be obtained and to be able to alert other communities that might be affected and share measures are taken. The model was then expended to include three-dimension to include a third axis that will indicate characteristics and activities at an individual organizational level as well as at a state level.

4.8. Comparative Evaluation of Cybersecurity Capability

The section shows a well and detailed explanation of the identified maturity models, a descriptive diagram of the maturity models, also tables 3 shows a summary of the comparisons among the models using the adopted taxonomy features from Halverson and Conradi's taxonomy of software process improvement.

4.9. Maturity Model

Note: 1 yet to be determined

Table 3 indicated how Halverson and Conradi's taxonomy features were used in explaining the identified cybersecurity capability maturity models. The features give a full description of all the models, such as their origin, reasons for creating the model, number of maturity levels, where it is applicable, who can use the model in the organization, how depth the implementation guidelines, etc. This description will help other organizations to see the features of each model and where it can be applied. Furthermore, the table can be an inside for top management of an organization that has less knowledge of cybersecurity to decide or decide on what type of model would suit their organization. The research aims to identify models from 2011 to 2019, but mostly relevant material from 2011 to 2019 was used, this is because only a few models are specifically cybersecurity oriented, those what were identified but did not fit the inclusion criteria includes like Control Objectives for Information and Related Technology Organization (COBIT), Project Management Maturity Model (OPMM) and Siemens Knowledge Management Maturity Model (KMMM) were not used in this research.

Table 3: Comparative review on cybersecurity capability maturity model

Model / Features	C2M2	ES-C2M2	ONG-C2M2	NICE-C2M2	CCSMM	FFIEC-CMM	AUMMCS
Cybersecurity Oriented	Yes	Yes (derived fromvC2M2)	Yes (derived from ES-C2M2)	Yes	Yes	Yes	Yes
Origin	The US.Dept of Energy	The US.Dept of Energy	The US.Dept of Energy	The US.Dept of Energy	CIAS	US Federal Financial Institute Of Examination Council	Centre For Cyber Security At The University of Johannesburg
Maturity level	4	3	4	3	5	5	4
Purpose	Assessment of cybersecurity capabilities for any organization comprises of a maturity model evaluating a tool	Tailored to energy subsector	Tailored to the oil and natural gas subsector	Tailored to three areas: process and analytics, integrated governance, skilled practitioners and technology for work development	Tailored to communities yardstick to know the security posture	Tailored to as assessment tools to identify organizational risk and determine their cybersecurity maturity	Tailored to ensuring citizens and government and business are protected African member states
Actors	Management	Management	Management	Staff	Communicates	Management/ Employees	States
Organization Size	large	large	large	large	Medium	large	All
Level of Documentation	Medium	Medium	Medium	Medium	Low	High	Medium
Organization Environment	Overall	Overall	Overall	Explicit	Explicit	Explicit	Overall
Define role	Yes	Yes	Yes	Yes	No	No	No
Depth of Assessment	Specific	Specific	Specific	General	Specific	Specific	General
Field Applicable	Organization	Electricity	Oil and Natural Gas	Workforce	Communities	Financial Organization	African states
Prescriptive/ descriptive	Both	Both	Both	Both	Descriptive	Both	Both
Assessment	Organization maturity	Electricity grid protection	Oil and gas protection	Organization maturity	Community protection	Organization maturity	Data protection
Assessor	Internal and external	Internal and external	Internal and external	Internal and external	external	external	external
Implementation Cost	1	1	1	1	1	1	1i

5. Result and Discussion

Cybersecurity has been growing exponentially day by day both in private and public sectors, so also cyber threats. These threats are dynamic and organizations need to be updated on the measures they should adopt to secure the critical assets. In this article, a review was carried out to identify the most recent mechanism used in protecting and also identifying the maturity of cybersecurity in an organization. The research is limited to models from 2011 to 2019 and also those designed specifically for cybersecurity as specified in the first objective. Table 3 elaborated on the comparisons of the identified models, the table shows most of the models have basic similarities, such as domains and levels, but also differ in some areas which include the level of implementation and guidelines, the actor's role, the field of application, and also assessment. Objective two of this article was to identify the maturity and the level of the models, the models have almost similar maturity description. Some models use levels like C2M2, while others use the baseline to innovation and others use initial to vanguard to describe how maturity increase from one level to the next. Overall they have basic similarities.

However, some models were derived from other models like in the case of the ES-C2M2, and the ONG-C2M2 models are derived from C2M2. Most models are more specific than generic. The last objective was to understand the application domain of the identified models. Most of the models' application domain includes organization, oil and gas section, communities, banking sectors, and even continent as a form of guidelines as shown in table 3. Certain models are designed to be used for the entire organization like C2M2 while other are not like NICE-C2M2. The complete adoption of a model seems to be impossible as the most model is designed for a specific purpose as in NICE-C2M2 which was designed for skilled staff. This discussion further shows that organization can assess their needs before selecting an appropriate model to measure their cybersecurity maturity level.

6. Research Direction

This paper explains the cybersecurity maturity models properties and their similarities and Applications domain, based on the reviews of all the available models, no any author explains the validation process of the proposed model before implementation, therefore, a future research can focus on how cybersecurity capability maturity models are evaluated and also cost of implementation of the model in an organization as no model explains the financial standpoint.

7. Conclusion

In conclusion, cybersecurity measures is an essential entity to be known by all organizations, identifying organizational maturity level and knowledge on cybersecurity is a most, also knowing what model to be used in identifying the maturity level is important. There is limited research on cybersecurity capability maturity models and their application as the research area is new and growing exponentially. This research will serve as the first step in knowing the relevant cybersecurity capability maturity models available and also areas of application. However, all the identified models are fully based on cybersecurity but adopting can be impossible, however, the models can be adapted and customized. Tables 3 give a clear view of all the models and how to choose a suitable model for any organization based on the features used. Furthermore, only C2M2 focuses on the entire organization while others focused on cybersecurity. Lastly, all models found after the SR lacks cost implementation, therefore, to know how much to spend for implementing any model depends highly on the size of the organization and the number of critical assets to be protected.

Conflict of Interest

The author declares no conflict of interest

Acknowledgment

This journal would not have been possible without the exceptional support and guidance of my supervisors Dr. Maheyzah Muhamad and Dr. Siraj Siti Hajar Othman. Their enthusiasm, knowledge, and exacting attention to details have been an inspiration and kept this journal work on track. I would also like to thank all the reviewers that gave their comments to make this paper acceptable to the community of knowledge.

References

[1]. M. Dunn Cavelty, "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities," Science and Engineering Ethics, **20**(3), 701–715, 2014, doi:10.1007/s11948-014-9551-y.
[2]. Nicholas R., The Cybersecurity Dilemma, Duke University, 2011.
[3]. R.W. Taylor, Cyber Crime and Cyber Terrorism, 4th ed., Pearson Education, Inc., United State, 2019.
[4]. Z. Soltani, N.J. Navimipour, "Customer relationship management mechanisms: A systematic review of the state of the art literature and recommendations for future research," Computers in Human Behavior, **61**, 667–688, 2016, doi:10.1016/j.chb.2016.03.008.
[5]. Kitchenham, Guidelines for performing Systematic Literature Reviews in Software Engineering, Durham Durham, UK, 2007, doi:10.1145/1134285.1134500.
[6]. A.D. Oxman, "Systematic Reviews: Checklists for review articles," BMJ, **309**(6955), 648–651, 1994, doi:10.1136/bmj.309.6955.648.
[7]. M.J. Grant, A. Booth, "A typology of reviews: An analysis of 14 review types and associated methodologies," Health Information and Libraries Journal, **26**(2), 91–108, 2009, doi:10.1111/j.1471-1842.2009.00848.x.
[8]. M.C. Paulk, "A History of the Capability Maturity Model for Software," The Software Quality Profile, **1**(1), 5–19, 2009.
[9]. C. V Weber, S.M. Garcia, M. Bush, "Key Practices of the Capability Maturity Model," 1993.
[10]. Y. Goksen, E. Cevik, H. Avunduk, "A Case Analysis on the Focus on the Maturity Models and Information Technologies," Procedia Economics and Finance, **19**(15), 208–216, 2015, doi:10.1016/s2212-5671(15)00022-2.
[11]. R.M. Adler, "A dynamic capability maturity model for improving cyber security," 2013 IEEE International Conference on Technologies for Homeland Security, HST 2013, 230–235, 2013, doi:10.1109/THS.2013.6699005.
[12]. P. Byrnes, M. Phillips, "-- ~ 47L ~ Software Engineering Method Description ESC-TR-96-002," (April), 1996.
[13]. D. Budgen, M. Turner, P. Brereton, B. Kitchenham, "Using Mapping Studies in Software Engineering," Ppig, **2**, 195–204, 2008.
[14]. N. Khatibian, T. Hasan gholoi pour, H. Abedi Jafari, "Measurement of knowledge management maturity level within organizations," Business Strategy Series, **11**(1), 54–70, 2010, doi:10.1108/17515631011013113.
[15]. G.B. White, "The Community Cyber Security Maturity Model The Center for Infrastructure Assurance and Security," Proceedings of the 40th Hawaii International Conference on System Sciences, (June), 1–8, 2007, doi:10.1109/HICSS.2007.522.
[16]. L. Johnson, Cybersecurity framework, 2020, doi:10.1016/b978-0-12-818427-1.00012-4.
[17]. W. Miron, K. Muita, "Technology Innovation Management Review

Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure," Technology Innovation Management Review, **4**(October), 33–39, 2014, doi:10.22215/timreview/837.

[18]. A. Sorini, E. Staroswiecki, 8. Cybersecurity for the Smart Grid, Elsevier Ltd, 2017, doi:10.1016/B978-0-12-805321-8.00008-2.

[19]. J.A.C.-M. and I.D.S.-G. Angel Marcelo Rea-Guaman, Tomás San Feliu, "Comparative Study of Cybersecurity Capability Maturity Models Angel," Computer Standards and Interfaces Software Process Improvement and Capability Determination Conference 2017, **60**, 1–2, 2018, doi:10.1016/j.csi.2018.05.002.

[20]. S.H.B. Von Solms, "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, 2015, doi:10.1109/SAI.2015.7237313.

[21]. G.B. White, "The community cyber security maturity model," 2011 IEEE International Conference on Technologies for Homeland Security, HST 2011, 173–178, 2011, doi:10.1109/THS.2011.6107866.

Appendix A

Table 4: C2M2 Domain description

Domains	Grouped Objectives
Asset, Change and Configuration Management	Manage Asset inventory Manage Asset configuration Manage changes to Asset Management Activities
Cybersecurity Program Management	Established Cybersecurity Program Strategy Sponsor Cybersecurity Program Established And Maintain Cybersecurity Architecture Perform Secure Software Development Management Activities
Event and Incident Response, Continuity of Operation	Detect Cybersecurity Events Escalate Cybersecurity Events And Declare Incidents Respond To Incident And Escalated Cybersecurity Events Plan Continuity Management Activities
Identify and Access Management	Established And Maintain Identities Control Assess Management Activities
Information Sharing and Communications	Share Cybersecurity Information Management Activities
Risk Management	Established Cybersecurity Risk Management Strategy Manage Cybersecurity Risk Manage Activities
Situational Awareness	Perform Logging Perform Monitoring Established And Maintain A Common Operating Picture Management Activities
Supply Chain and External Dependencies Management	Identify Dependencies Manage Dependency Management Activities
Threat And Vulnerability Management	Identify And Respond To Threats Reduce Cybersecurity Vulnerabilities Management Activities
Workforce Management	Assign Cybersecurity Responsibilities Control The Workforce Life Cycle Develop a Cybersecurity Workforce Increase Cybersecurity Awareness Management Activities

Table 5: C2M2 Maturity level description

Maturity indicator level MIL	Level description
Level 0	This level has no practices or processes defined. There is no stable environment for activities. MIL 0 is given as a result of the domain objective not achieved.
Level 1	This level contains a set of initial practices. This level activities are usually ad hoc and chaotic. MIL 1 is scored if there is an initial practice performed
Level 2	This level has more stable practice compared to MIL, more confidence is achieved at this level as the result of the performance and is sustained over time.
Level 3	At MIL 3 policy is applied to the practices to further stabilize the operations in the organization and is guided by top-management directives. Also, the staff s' are fully trained and fully funded.

Table 6: ES-C2M2 and ONG-C2M2 domain description

Domain	Practices
Risk	Risk Assessment
Assets	Asset, Change, and Configuration Management
Access	Identity and Access Management
Threat	Threat and Vulnerability Management
Situation	Situational Awareness
Sharing	Information Sharing And Communication
Response	Event And Incident Response, Continuity Of Operations
Dependences	Supply Chain And External Dependencies Response Management
Workforce	Workforce Management
Cyber	Cybersecurity Program Management

Table 7: ES-C2M2 and ONG-C2M2 maturity level

Maturity Level	Description
MIL 0 " Not Performed"	This level describes the domain has achieved nothing.
MIL 1 " Initial"	This level shows only initial practices are performed
MIL 2 "Performed"	The level is characterized by having well-documented practices, stakeholders' involvement, and provision of standards or guidelines for practice implementation.
Mil 3 "Managed "	This level shows all practices and activities are fully guided by policy, also practice is only assigned to adequate skills personal. The formed policy are periodically evaluated for improvement