Cybersecurity Maturity Model for Higher Education Institution: Systematic Literature Review

Maznifah Salam[1†], Khairul Azmi[2††] and Ahmad Tarmizi[3††]
p107187@siswa.ukm.edu.my khairul.azmi@ukm.edu.my atag@ukm.edu.my
Universiti Kebangsaan Malaysia, Malaysia

Abstract
The cybersecurity maturity model is made to evaluate how mature an organization's cybersecurity strategy is and help it take its cybersecurity capabilities to the next level. Even though there are several cybersecurity scenarios and models in the literature review, it was found that there is a lack of research and knowledge on the models and the level of effectiveness of cybersecurity maturity used in specific sectors, especially higher education institution. The study was done by completing a complete assessment and thoroughly evaluating all studies published between 2017 and 2022. To do this, strategies were used to find, screen, and determine the eligibility of studies using databases as Emerald Insight, IEEE, Web of Science, and Science Direct. The quality of the studies was then evaluated, and data were extracted and analysed. The thematic analysis also revealed three main themes: (1) cybersecurity issues and factors, (2) the level of cybersecurity maturity, and (3) the things that affect how well cybersecurity maturity works. The study looked at the current state of cybersecurity concerns and found that, according to the existing cybersecurity maturity model, the model hasn't changed enough for higher education institution to use a general solution or a specialised technique for higher education institution. With this thorough review of the literature, we try to summarize the current state of the cyber security maturity model, give researchers a complete list of references, and encourage the reader to learn more about this new field.

Keywords:
Cyber security, maturity, model, higher education institutions

1. Introduction

Many countries worldwide are susceptible to a wide variety of cyber dangers due to their heavy reliance on information and communication technology (ICT) for their social, political, and economic activities [1]. When it comes to cybersecurity, organisations have a long way to go. Cybersecurity and information security are so similar that many people use them interchangeably [2]. Cybersecurity means protecting assets by dealing with the risks of how information is processed, stored, and sent over the internet [3]. Cybersecurity has become an essential part of the world we live in today. The rise in cybercrime has put more pressure on businesses to ensure they have implemented enough security measures. Threats are anything or anyone that could cause damage to their assets. Most organisations don't believe that the IT department is solely responsible for cybersecurity, which is a false idea. But, as the paper by Rahman et al. says, cybersecurity is everyone's job [4]. Having secure and solid cybersecurity will protect our system on every device that the organisation has

People and businesses must be ready to deal with threats wherever and whenever they happen. Organizations need security assessments to ensure their cybersecurity is good enough to keep up with cyber threats that change quickly. Management must support cybersecurity from the top down and make sure that all related initiatives have the same amount of flexibility to guide their performance in cybersecurity [5,6,7,8,9]. This will help management stay relevant when directly or indirectly supporting cybersecurity. Many corporate executives and management don't know enough about the actual cybersecurity threats to their vital infrastructure. The media and researchers focus on high-profile assaults like those on Sony Pictures Entertainment, Target Corporation, and the Democratic National Convention. [10]. Even at higher education institutions, attacks are getting more and more dangerous. The Stars website said in November 2019 that UiTM had a data breach in February and March 2018 but did not tell the public. The report says that between 2000 and 2018, the records of 1,164,540 students were stolen. The Universiti Malaya (UM) E-Pay Cashless Payment and Records portal has reportedly been hacked and changed as late as October 18, 2019 [11].

Singapore's The Straits Times (ST) recently reported that our Navy, Tentera Laut Diraja Malaysia (TLDM), had leaked the sensitive document through the Dark Web website [12] (Hakim, 2020). ST says that the hack came from emails sent by TLDM employees. About 70 documents that have been stolen were made public. This information leak included a conversation between a US Navy ship and TLDM, which the Malaysian Army Forces has denied. According to a report from IBM Security and the Ponemon Institute, the average size of a data breach in 2019 was 25,575 records. The total cost of a data breach worldwide is $3.92 million. The information was gathered from July 2018 to April 2019, and each lost record costs $150 [13]. This report comprises in-depth interviews with more than 500 companies from all over

Manuscript received November 5, 2024
Manuscript revised November 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.11.23

the world. Because the cost is so high, any organisation must implement high-security measures to stop a data breach. In September 2019, 30 million customer records were stolen from Malaysia's well-known airline Malindo Airways (OD). This was due to a data breach [14]. Two people who used to work for the company's e-commerce service provider, GoQuo (M) Sdn Bhd, did this at the company's development center in India. Captain Mushafiz Mustafa Al-Bakri, the CEO, said that police reports had been filed in Malaysia and India. He also said that the National Cyber Security Agency (NCSA), the JPDP, and other authorities abroad had been told about this case [17]. The Ministry of Communication and Multimedia is still waiting for this report from Malindo Air, according to another report from Astro Awani. It doesn't say when it wants it, but it wants it as soon as possible [15].

Organisations should do security assessments to ensure their cybersecurity is as safe as possible. Hitman and Mattord (2017) say that security assessment looks at a system to see if it meets the security model, security standards, or pre-set procedures. Policies and procedures for operational controls are standard countermeasures to protect organisational assets from attacks and vulnerabilities [5]. Organizations can improve their efficiency and overall performance with the help of a cybersecurity assessment. When management and organisation are done well, these benefits are at their highest. Cybersecurity assessments should be done with the help of specific/appropriate criteria based on their maturity in cybersecurity. The maturity model is a standard way to judge how well something works. The security maturity model aims to find methods, processes, and procedures that an organisation can use to improve the security of its ICT [6]. Assessing a company's cybersecurity can help it work better and more efficiently. Maturity models can be thought of as a group of pieces that explain different parts of an organization's growth (maturity) [7]. Also, a maturity model is often used to analyse basic business processes or specific parts of an organisation because it is a more organised and systematic way to do business. Maturity models are an essential set of tools organisations can use to measure how prepared they are for cybersecurity and how well they follow the rules.

These things show that cybersecurity is important and needs to be appropriately handled. To keep cybersecurity up to date with how cybercrime is changing, organisations need security assessments to ensure their cybersecurity is good [3,4,6]. Indicators are given to show how ready the organisations are to deal with cyberattacks and what needs to be done to fix the problem. Because cybersecurity has been in the news a lot this decade, scientists have done more research on it. Few studies have been done on how to make a process improvement framework based on standards. Based on the report paper by CMMI in 2018, some of the available frameworks are based on the Capability Maturity Model. However, in an article by Ozkan et al. (2018), these frameworks were criticised for their implementation costs, applicability, and reliability. This paper shows some of the cybersecurity maturity models used in the past few years. In the next section, we will discuss how the article's study was done. In the third section, we look at the literature. The fourth part will be a discussion, and the last part will be the conclusion, which will discuss what needs to be done next.

2. Methods

This part will focus on the findings from the above full-text review. We started with a few pieces of paper. Then, we use the SLR method to determine their importance to our research topics. Lastly, we get the needed information and organise it based on the research question.

2.1 Step 1: Question Formulation

The first step in doing an SLR is to develop a straightforward, focused review question that will set the scope and focus of the review. This review aims to define definitions, elements, and methods for creating best practices for an organization's cybersecurity maturity model based on an international standard. Three questions have been suggested to help structure the answer to this question: What is the current cybersecurity maturity model, what is the difference between the levels of these models, and what are the characteristics of these models?
Two things were used to come up with the research question. All of the articles were about the available model of maturity.

2.2 Step 2: Finding

The relevant articles used Shaffril et al. as three systematic identification processes, screening, and eligibility [9]. This method aims to develop search terms that will bring up enough relevant literature to cover all the critical issues related to the review [10]. This information comes from reputable journals and databases, academic work that has already been published, professional reports from institutions and organisations, websites, government records, and books. Including literature relevant to the cybersecurity maturity model is a plus in this study and its review activities.

i. Identification: Selection of criteria and evaluation

This section provides an overview and history of the works reviewed. There is a complete analysis of the literature on technological aspects, people, security processes, and cybersecurity sophistication, which are still significant research topics.

Using the basic search parameters, this choice turned up articles like Figure 1. A cybersecurity maturity model is an idea behind the proposed study. So, the search criteria for papers include the words "cybersecurity," "maturity," and "model." We used a few critical indexed electronic scientific resources from six databases to look for publications. So,

once all the relevant keywords were chosen, search strings were made for the databases of Emerald Insight (www.emerald.com), Web Of Science (https://www-webofscience-com), IEEE (ieeexplore.ieee.org), and Science Direct (www.sciencedirect.com).

ii. Screening

The screening was the second step. Articles were added to or taken out of the study based on a specific set of criteria, either with the help of the database or by author's hand screening b (see Table 1). Kraus et al. (2020) put a lot of emphasis on the idea of "research field maturity." Because of this, this review's screening process only looked at articles published between 2017 and 2022. This time frame was chosen because there were enough published studies for a representative review. The authors sought empirical research papers because they had first-hand information. Notably, only those written in English were looked at so there wouldn't be any confusion. After taking out duplicates, findings that peers didn't review, and articles that weren't written in English, the literature pool was made up of papers. The study looks at these types of publications: journals, white papers, reports, theses, conferences, and workshops. All of these were written in English and published between 2017 and 2022. They are also in the digital database. If the title and scope don't match, any content that doesn't fit this time frame is left out.

TABLE 1. THE SELECTION CRITERION IS SEARCHING

Criterion	Inclusion	Exclusion
Language	English	Non-English
Timeline	2017-2022	< 2017
Literature type	Journal (only research articles)	Book chapter, conference proceeding
Subject Area	Computer Science	Besides Computer Science

iii. Eligibility

A comprehensive literature review helps find, evaluate, and understand all available research on a specific subject. The secondary part of this study is a structured literature review that confirms the theories and assumptions employed to study the cybersecurity maturity level of the organizations, as shown in Figure 1.

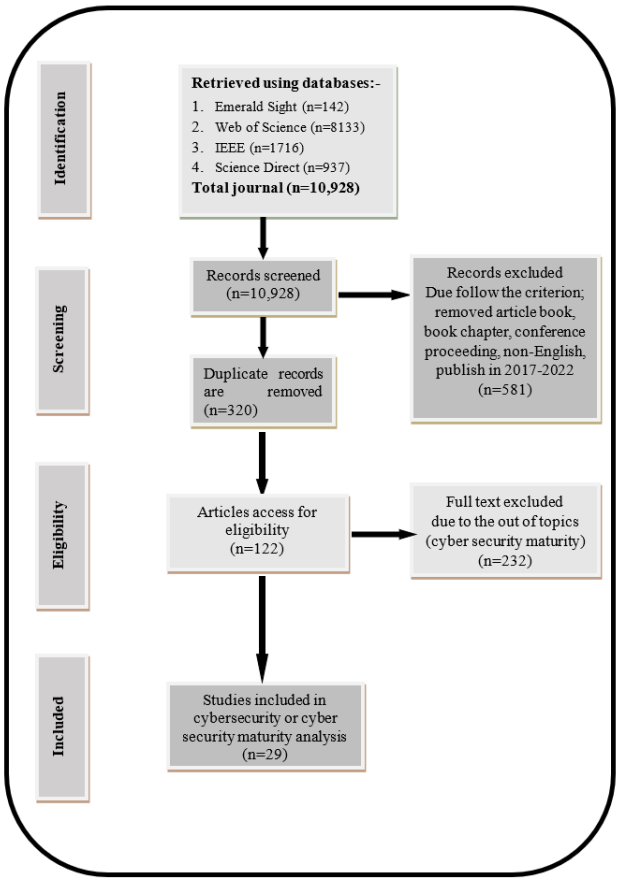

Figure 1: Flow diagram of the searching study

The rest of the papers are checked by hand to see if they meet the criteria for inclusion. This can be done by reading the title, abstract, or the whole paper. At the title screening stage, 581 articles were thrown out, and at the abstract screening stage, 320 articles were thrown out. After the authors realised that they were already in another database, five more articles were taken out. At this stage, 84 articles were taken out because they didn't focus on cybersecurity or cybersecurity maturity, were in the form of review papers, or didn't talk about cybersecurity, cybersecurity capability, or even cybersecurity maturity.

A search for "Title" and "Abstract" turned up 145 articles for the first group of papers in Emerald. On the other hand, the "Topic" search in the Web of Science, which included Title, Abstract, Author Keywords, and Keywords Plus, turned up 8133 articles, of which 1716 were the same as IEEE. Lastly, the "Advanced Research" search on "Article Title" in Science Direct turned 937 articles. So, one scientific paper was chosen for the first group of articles. For the second group of articles, the Web Science search turned up 16 articles, 11 of which were already looked at in the first group.

On the other hand, the search in IEEE turned up three articles, 58 of which have already been looked at and are the same as articles from other groups. Overall, 232 scientific papers were thrown out because they weren't about cyber security maturity. When the abstracts of all of them were looked at, 122 articles (four from the first group and eleven from the second) met the criteria for this literature review. So, the selection phase led to 29 scientific papers that needed to be looked at.

2.3 Step 3: Quality Appraisal

The goal of this step was to read each paper individually to find new information, differences, and features that correspond to existing cybersecurity maturity models. This was done by evaluating and interpreting the final group of publications shown in Figure 1. The synthesis was done using an integrative method, which is especially helpful when comparing multidisciplinary works with ideas of resilience that are similar, different, and changing simultaneously. The results were then used to build a conceptual knowledge base that works well with the current cybersecurity maturity model.

In Table 2, you can see an overview of the chosen articles. Also, titles that met the keyword requirements were looked for in all the work mentioned in accepted publications. In Table 2, you can see an overview of how the papers were chosen. In the end, this meant that there were 29 articles to review.

TABLE 2. A SUMMARY OF THE PAPER SELECTION RESULTS

No	Source	Raw Data	Screening	Duplicate	Excl.	Incl.
1.	Emerald Insight	142	20	11	8	1
2.	Web Of Science	8133	319	172	131	16
3.	IEEE	1716	145	58	84	3
4.	Science Direct	937	77	59	9	9
Total		**10,928**	**571**	**300**	**232**	**29**

2.4 Step 4: Reporting and Utilising Results

In the section on reporting and using results, all the research is summed up in terms of the information gathered from concepts, literature reviews, case studies, and reports [10]. Most of the time, synthesised results can be used in a new way to help make new connections between ideas that have been looked at separately in the literature. Section 3 of this article summarises the results of the review question. Then, it puts together and applies what it learned in a description that helps other organisations understand each model and how it can be used.

3. Analysis of selected literature

Cybersecurity experts could learn a lot by looking at the maturity models in their industry to learn more about the maturity models in their field. A maturity model is a tool that can be used to assist an organization in developing a domain-specific framework of information that could be used to guide evaluations and improvements [11].

In this paper, a few cyber security models have been discovered to be currently used in organisations. Next, there will be a further explanation of the types of models.

The following maturity models have been identified as listed: -

i. Cybersecurity Focus Area Maturity (CYSFAM) Model
ii. Cybersecurity Maturity Assessment Framework (SCMAF)
iii. Holistic Cybersecurity Maturity Assessment Framework
iv. Community Cyber Security Maturity Model (CCSMM)
v. *Cyber security Capability Maturity Model (C2M2)*
vi. National Initiative for Cyber Security Education Capability Maturity Model (NICE)
vii. Cyber security Capacity Maturity Model for Nations (CMM)
viii. The Framework for Improving Cyber Security Critical Infrastructure (NIST)
ix. Qatar Cyber Security Capability Maturity Model (Q-C2M2)
x. Cyber security Maturity Model Certification (CMMC)
xi. The Cyber Security Maturity Assessment Framework (CMAF)

i. Cybersecurity Focus Area Maturity (CYSFAM) Model

Ozkan and his team came up with the Cybersecurity Focus Area Maturity (CYSFAM) Model as a way to measure how good cybersecurity was in 2020. The CYSFAM comprises 11 sub-domains (focus areas) in the cybersecurity domain. To make them easier to understand and manage, the above focus areas are put into two groups: technical and organisational. As CYSFAM is a maturity model, it has parts for assessment and measurement.

CYSFAM differs from other models because it is mainly based on international standards and frameworks. It is designed for all kinds of organisations and is set up as a focus area maturity model, which is the only one for cybersecurity. Practitioners can use CYSFAM's 144 assessment questions/capabilities, grouped into 11 focus

areas, to evaluate and improve their cybersecurity skills. The paper gives an overall approach to cybersecurity that can help organisations get a big-picture view of the field. Planning for improving capabilities is made more accessible by analyzing and visualizing how the capabilities depend on each other. Since cybersecurity experts tested CYSFAM and showed how it works in a case study company, it gives organisations a good place to start their cybersecurity efforts. CYSFAM is known as a focus area maturity model that is mainly based on standards.

Since most assessment questions come from standards and frameworks, CYSFAM makes it easier to be aware of and follow standards. Due to its high level of detail, CYSFAM can also give concrete advice on improving processes [43].

ii. Cybersecurity Maturity Assessment Framework (SCMAF)

A Cybersecurity Maturity Assessment Framework (SCMAF) is proposed for higher education institutions (HEIs) in Saudi Arabia in 2021. The main thing that SCMAF does is provide HEIs in Saudi Arabia with a continuous, thorough, user-friendly, up-to-date, and aligned with local and international security standards and cybersecurity assessment process. SCMAF is a simple assessment tool that can be used online through a web-based service or offline by downloading. This is done to protect the privacy of the organisations' data. A complete, custom framework for HEI in Saudi Arabia to measure their level of cybersecurity maturity (SA) [44]. The framework took both SA cybersecurity regulatory and international cybersecurity standards into account. Institutions can use this framework to self-evaluate the security of their IT-based systems to figure out how safe they are. So, they must work on their weaknesses, plan to deal with them, and keep improving. SCMAF can also be used in other fields besides education, like healthcare and industrial organisations.

iii. Holistic Cybersecurity Maturity Assessment Framework (HCMAF)

Aliyu and his team in 2020 came up with the Holistic Cybersecurity Maturity Assessment Framework (HCMAF), which can be used by higher education institutes (HEIs) in the UK to evaluate their cybersecurity. The novel HCMAF includes all security regulations, privacy regulations, and best practices that HEIs must follow. It can be used as a self-assessment tool or a cybersecurity audit tool. The proposed framework sets up a set of metrics for measuring the competency or maturity of an organisation based on a set of already-known best practices, skills, or standards. It includes the General Data Protection Regulation (GDPR), the Payment Card Industry Data Security Standard (PCI DSS), and the Data Security and Protection Toolkit (DSPT). It can be used to do a gap analysis against 15 security requirements. This framework is based on a Capability Maturity Model (CMM) process. The proposed model has 15 security categories and six maturity levels. It is implemented online and can be used as a self-assessment and an audit tool. This lets organisations do a gap analysis and get compliance and audit reports and graphical representations of their security posture [45].

iv. Community Cyber Security Maturity Model (CCSMM)

The Centre developed the CCSMM for Infrastructure Assurance and Security (CIAS) in San Antonio, Texas. This idea was made to help states and society set up a cyber security programme that will work and last in the US tax sector [13].

The unique intelligence of the CCSMM helps define the goals of some tests and exercises that can be used to measure how well existing programs work [14]. The CCSMM is meant to be used by communities and state and federal law enforcement agencies working together. Its goal is to help the community decide what is most important, the most likely targets, and what needs to be protected (and to what extent). With these goals in mind, plans could be made to help each part of the community reach the right level of cybersecurity maturity.

v. Cyber security Capability Maturity Model (C2M2)

Carnegie Mellon University and the US Department of Energy developed the Cyber Security Capability Maturity Model in 2014 to help critical infrastructure companies evaluate and improve their cyber security policies. The C2M2 was first used in 2014, and in 2019 it got an upgrade. The Capacity Centre's goal is to help organisations of all kinds and industries figure out how to continue improving their cyber security and operational resilience. The C2M2 defines maturity models as "a collection of features, traits, signs, or patterns that categorise a discipline's capacity and evolution.

vi. National Initiative for Cyber Security Education Capability Maturity Model (NICE)

In 2008, George W. Bush made the NICE model because national security told him to. The method was created so that people with skills in cyber security could be hired. The model has three important parts: the security structure for managers and their roles, the security structure for personnel, and the goal of creating a workforce with a technological profile in cybersecurity and the proper knowledge and skills. These goals are met by the NICE Component's focus on the organization's security structure, especially in talent management and workforce planning. Only version 1.0 of the model came out in August 2014 [13]. Before an organisation can use this model, it must know how many people work in each of the three domains [16] and also be able to show proof that it works.

vii. Cyber security Capacity Maturity Model for Nations (CMM)

The Global Cyber Security Capacity Centre (Capacity Centre), which is part of the Oxford Martin School and is based at the University of Oxford, came up with the Cyber Security Capacity Maturity Model for Nations (CMM). The goal of the Capacity Centre is to use the Cyber Security Capacity Maturity Model to make cyber security capacity building bigger and better in the UK and worldwide. The CMM is explicitly designed for countries that want to improve their cyber security. The CMM was first used in 2014, but it was changed in 2016 after it was used to review 11 countries' cyber security capabilities [14].

viii. The Framework for Improving Cyber Security Critical Infrastructure (NIST)

The National Institute of Standards and Technology (NIST) developed the Framework for Improving Critical Infrastructure Cyber Security. Organisations of any size can use the tools, no matter how good their cyber security skills are or how significant their cyber security risk is. Because this is a framework rather than a model, it is constructed differently than previous models [14], [16]. The framework is meant to help organisations self-evaluate their risk so that their cyber security strategy and investments are more rational, practical, and valuable. The cyber security outcomes of the Framework Core make it easier for people to evaluate their assets and cyber security events [12, 13].

ix. Qatar Cyber Security Capability Maturity Model (Q-C2M2)

In 2018, the College of Law at Qatar University came up with the Qatar Cyber Security Capability Maturity Model (Q-C2M2). The Q-C2M2 is built on several existing models to create a complete assessment method to improve Qatar's cyber security framework [14, 19]. The Q-C2M2 uses five maturity levels to measure the capability maturity of a government agency or non-state organisation at the core function level [19]. The Q-C2M2 is still in the early stages of research, so it is not yet ready to be used. It's a framework that could provide detailed assessment models to Qatari organizations.

x. Cyber security Maturity Model Certification (CMMC)

Together with Carnegie Mellon University and the Applied Physics Laboratory at Johns Hopkins University, the US Department of Defense (DoD) set up the Cyber Security Maturity Model Certification (CMMC). When each level of cyber security maturity is reached, CMMC will look at it and ensure that best practices and certifications are implemented. The most recent version of the CMMC came out in 2020 [14, 18, 20]. The CMMC employs a five-level maturity model comprised of procedures and practices. For an organisation to reach a certain level of maturity, as in CMMC, it must meet the requirements for the processes and methods that go with that level. This also means that all the needs for the levels below have been met.

xi. The Cyber Security Maturity Assessment Framework (CMAF)

The European Union Agency for Cyber Security (ENISA) is the EU's organisation for ensuring that cyber security is high and the same all over Europe. The researchers came up with the framework to standardize the different levels of maturity that organisations can have, especially the ones that can be measured. To solve this problem, a new evaluation framework named the Cyber Security Maturity Assessment Framework (CMAF) was implemented. It helps an organisation do a gap analysis and gives them a visual analysis of their security posture.

CMAF was known to give a complete, business-like appearance to cyber security, the integration of security measures, the ability to participate in challenging environments, and how easy it was to use.

4. Discussion

At the end of this section, judging criteria were specified. Appendix 1 was made after the systematic review compared the models used to measure cybersecurity maturity.

In Appendix 1, it is shown that different models have some things in common, like domains and levels, but also have some things that are different, like the level of implementation and guidelines, the field of application, and the assessment. The second part of the paper was to determine how old and mature the models were. Some models use levels like C2M2 and Q-C2M2 and the baseline for innovation or the beginning to vanguard approach, respectively, to show how maturity moves from one level to the next. They are made up of some basic parts. All the models have their ways of judging them, but Q-C2M2 doesn't have one. Instead, CMMC will be judged by third-party auditors.

Here is a summary of what was found.

i. More models like C2M2, CMMC, CCM2, and Framework for Improving Cyber Security Critical Infrastructure have been changed to be used in cyber security.

ii. SCMAF and HMAF model has been proposed to the HEI due to the cyber-attacks on specific organisations.

iii. Models like C2M2, CMMC, and CCM2, which cover all parts of the organisation, cover all security qualities (confidentiality, integrity, and availability).

Model Name	Purposes	Target	Evaluation method	ef.
1. Cybersecurity Focus Area Maturity (CYSFAM) Model- 2021	To accompany information security capabilities.	Standard-based focus area maturity model for generic organizations	Organizational Self-Assessment Methods	[44]
2. Cybersecurity Maturity Assessment Framework (SCMAF)- 2021	Cybersecurity maturity assessment framework for HEI in Saudi Arabia	For HEIs in Saudi Arabia	Self-assessment	[45]
3. Holistic Cybersecurity Maturity Assessment Framework (HCMAF)- 2020	To assess the cybersecurity in HEIs in the UK.	For Higher Education Institutes (HEIs) of the United Kingdom.	Self-assessment	[46]
4. Cyber security Maturity Model Certification (CMMC)- 2020	To protect information from the Defense Industrial Base sector (DIB).	U.S. Department of Defense (DoD)	Assessment by third-party auditors	[12]–[14]
5. National Capabilities Assessment Framework (NCAF)- 2020	NCSS-National Cyber Security Strategy) for European countries	National Level	National Self-Assessment Methods	[14]–[18]
6. Framework for Improving Cyber Security Critical Infrastructure -2018	A framework intended to guide security and risk management activities.	Organization	Organizational Self-Assessment Methods	[16]–[23], [42]
7. Qatar Cyber Security Capability Maturity Model (Q-C2M2) -2017	The model is used for benchmarking, measuring, and developing Qatar's cyber security framework.	Organizations in Qatari	None	[23], [24], [38], [42]
8. Cyber security Capacity Maturity Model for Nations-CMM -2016	Increase the scale and effectiveness of cyber security capability.	National	Work with local organizations according to the national context.	[14], [21], [26]–[30]
9. Cyber security Capability Maturity Model (C2M2) -2014	Program improvements and strengthen the resilience of cyber security operations.	Organization of all sectors, types, and sizes	Self - Assessment Methods and toolkits	[12], [14], [28], [29], [31], [32], [40]
10. National Initiative for Cyber Security Education Capability Maturity Model (NICE) -2014	Organizations cyber security workforce development, planning, training, and education.	Organizations in the US	Self - Assessment Methods and organizations toolkits	[33]–[35], [41]
11. The Community Cyber Security Maturity Model-CCM2 -2006	Community status in cyber readiness and their preparation.	Community (local or state government)	Assessment in the community	[23], [36]–[38]

Accessibility of models in the models that were looked at.

iv. Compared to other models, like the C2M CMMC, NICE and CCSMM have more general ways of judging than others, like the C2M CMMC. More specific models, like the Framework for Improving Cyber Security Critical Infrastructure (NCAF), CYSFAM, SCMAF, and HMAF, give more information about how to classify and evaluate their processes and improve the maturity indicator levels.

This study concludes that cyber security maturity models help management take better care of their organizations' security. The NICE model chooses employees with cyber security experience and knowledge. The goal of the CCMM model is to meet the needs of both the government and the public for a long-term cyber security programme in the US tax system [22]. The most important thing about this model is that it considers the relationship between the states, which comprise many communities. The cyber security maturity models have brought innovation down a new path that needs more research. They employ a segmented, specialised approach and assume introspective security.

5. Conclusion

Lastly, all the models found during the review make it hard to use a single model: they must work in different organizational, cultural, governance, and maturity contexts. So, industrialized countries have models that are well known. This study shows that the higher of education doesn't give a complete overview of all cyber security issues to reach the maturity of cyber security. So, this suggests that the higher education need to know about existing models and how to evaluate them. Even though the approaches listed are all about cyber security, it may be challenging to use them. Cybersecurity covers all strategies, approaches, protocols, standards, policies, procedures, process, guidelines, measures, tools, technology systems, mechanisms, software, hardware, actions, training, and assurance that preserve the basic security objectives known as the CIA triad: Confidentiality, integrity, and availability.

Acknowledgment

The authors would like to express their gratitude to the anonymous reviewers and the Editor for their insightful comments on the article, which aided in its improvement in terms of quality and presentation.

References

[1] Abdullah, F., Salwa Mohamad, N., Yunos, Z., Malaysia, C., & Kembangan, S. (2018) Safeguarding Malaysia's Cyberspace against Cyber Threats: Contributions by CyberSecurity Malaysia. Journal of Cyber Security, 1, 22–31.

[2] ISACA, (2017) IT asset valuation, risk assessment and control implementation model. IT Asset Valuation, Risk Assessment and Control Implementation model, vol. 3, pp. 1–9.

[3] M. Ahlmeyer (2016) Issues in information systems securing the internet of things: a review. vol. 17, no. Iv, pp. 21–28. http://www.iacis.org/iis/2016/4_iis_2016_21-28.pdf

[4] M. J. A. Rahman, M. I. Hamzah, M. H. M. Yasin, M. M. Tahar, and N. K. Ensimau (2019) The UKM students perceptions towards cyber security.

[5] Qashqari, A. A., Munshi, A. M., Alturkstani, H. A., Ghwati, H. T., & Alhebshi, D. H. (2020). The Human Factors and Cybersecurity Policy. International Journal of Computer Science and Network Security, 20(4), 1–5.

[6] T. Yvon (2020) Exploring Factors Limiting Implementation of the National Institute of Standards and Technology Cybersecurity Framework. ProQuest 28028658 Published, Colorado Technical University.

[7] M. A. Boutwell (2019) Exploring Industry Cybersecurity Strategy in Protecting Critical Walden University.

[8] S. Tariq, S. Lee, H. K. Kim, and S. S. Woo (2019) Information and operational technology security systems, vol. 11398, pp. 39–45, 2019.
http://link.springer.com/10.1007/978-3-030-12085-6

[9] A. Rabii et al. (2020) Information and cyber security maturity models: a systematic literature review. Information and Computer Security, vol. 28, no. 4, pp. 627–644.
https://doi: 10.1108/ICS-03-2019-0039.

[10] Z. Mazlina (2020) Model pengukuran kematangan pengurusan keselamatan maklumat organisasi. UKM.

[11] B. Y. Ozkan and Marco Spruit (2018) A questionnaire model for cybersecurity maturity assessment of critical infrastructures. Springer, vol. 11398, pp. 39–45.

[12] Y. Angeline (2019) Records of more than a million UiTM students leaked online. The Stars Malaysia. https://www.thestar.com.my/tech/tech-news/2019/01/25/uitm-students-data-breach

[13] A. Hakim (2020) Sensitive TLDM Documents Hacked & Leaked On Dark Web. New Strait Times.
https://www.msn.com/en-my/news/national/sensitive-tldm-documents-hackedand-leaked-on-dark-web/ar-BB182UxE?li=BBr8Hnu&ocid=mailsignout

[14] IBM (2019). Cost of a Data Breach Report 2019. In IBM Security.

[15] S. Augustin (2020). Malindo Air hauled to court over Data Breach. FMT News.
https://www.freemalaysiatoday.com/category/nation/2020/02/20/malindo-air-hauled-tocourt-over-data-breach/

[16] A. Awani. (2019). KKMM masih tunggu laporan isu pencerobohan data penumpang. Astro Awani.
http://www.astroawani.com/video-malaysia/kkmm-masih-tunggu-laporan-isupencerobohan-data-penumpang-1810075

[17] Bernama (2019). Kebocoran data pelanggan telah ditangani, kata Malindo Air. Astro Awani.
http://www.astroawani.com/berita-malaysia/kebocoran-data-pelanggan-telahditangani-kata-malindo-air-218664

[18] R. A. Caralli, J. H. Allen, P. D. Curtis, D. W. White, and L. R. Young (2010) Resilience Management Model, Version 1.0 Improving Operational Resilience Processes. Carnegie Mellon SEI, no. May, p. 259.
http://www.cert.org/resilience/%0Ahttps://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9479%0Ahttps://resources.sei.cmu.edu/asset_files/TechnicalReport/2010_005_001_15230.pdf

[19] A. Abdullahi Garba, A. Musa Bade, M. Yahuza, and Y. Nuhu (2020) Cybersecurity capability maturity models review and application domain. International Journal of Engineering & Technology, vol. 9, no. September, p. 779.
https://doi: 10.14419/ijet.v9i3.30719.

[20] Carnegie Mellon University and The Johns Hopkins University Applied Physics Laboratory LLC (2020) Cybersecurity Maturity Model Certification (CMMC) Version 1.02. no. Cmmc, pp. 1–23.
https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf

[21] M. Bartsch and S. Frey (2018) Cybersecurity Best Practices. Springer Fachmedien Wiesbaden.
https://doi: 10.1007/978-3-658-21655-9.

[22] A. A. Garba, M. M. M. M. Siraj, and S. H. S. H. Othman (2020) An explanatory review on cybersecurity capability maturity models. Advances in Science, Technology and Engineering Systems, vol. 5, no. 4, pp. 762–769.
https://doi: 10.25046/AJ050490.

[23] A. A. Gabra, M. B. Sirat, S. Hajar, and I. B. Dauda (2020) Cyber security awareness among university students: A case study. Journal of Critical Reviews, vol. 7, no. 16, pp. 825–833.
https://doi: 10.31838/jcr.07.16.108.

[24] A. A. Garba, M. M. Siraj, S. H. Othman, and M. A. Musa (2020) A Study on Cybersecurity Awareness Among Students in Yobe State University, Nigeria: A Quantitative Approach. International Journal on Emerging Technologies, vol. 11, no. 5, pp. 41–49.
https://www.researchtrend.net

[25] Z. Hitchcox (2020) Limitations of Cybersecurity Frameworks that Cybersecurity Specialists Must Understand to Reduce Cybersecurity Breaches.

[26] Y. Alshboul and K. Streff (2015) Analyzing information security model for small-medium sized businesses. 2015 Americas Conference on Information Systems, AMCIS 2015, no. August.

[27] U. M. Mbanaso, L. Abrahams, and O. Z. Apene (2019) Conceptual Design of a Cybersecurity Resilience Maturity Measurement (CRMM) Framework. The African Journal of Information and Communication, no. 23, pp. 1–26.
https://doi: 10.23962/10539/27535.

[28] M. Nicho (2018) A process model for implementing information systems security governance. Information and Computer Security, vol. 26, no. 1, pp. 10–38.
https://doi: 10.1108/ICS-07-2016-0061.

[29] M. Mylrea, S. N. G. Gourisetti, and A. Nicholls (2018) An introduction to buildings cybersecurity framework. 2017 IEEE Symposium Series on Computational Intelligence, SSCI 2017 - Proceedings, vol. 2018-Janua, no. November 2017, pp. 1–7.
https://doi: 10.1109/SSCI.2017.8285228.

[30] R. Azmi and Kautsarina (2019) Revisiting cyber definition. European Conference on Information Warfare and Security, ECCWS, vol. 2019-July, no. July, pp. 22–30.
https://doi: 10.4018/978-1-7998-3149-5.ch001.

[31] R. D. B. J.D. (2018) Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework. International Review of Law, vol. 2018, no. 4.
https://doi: 10.29117/irl.2018.0036.

[32] A. M. Rea-Guaman, I. D. Sanchez-Garcia, T. S. Feliu, and J. A. Calvo-Manzano (2017) Maturity models in cybersecurity: A systematic review.
https://doi: 10.23919/cisti.2017.7975865.

[33] A. Ibrahim, C. Valli, I. McAteer, and J. Chaudhr (2018) A security review of local government using NIST CSF: a case study," Journal of Supercomputing, vol. 74, no. 10, pp. 5171–5186.
https://doi: 10.1007/s11227-018-2479-2.

[34] M. B. C. Mark C. Paulk, Bill Curtis (2009) Capability Maturity Model. Information Security Management Metrics, pp. 201–203.

https://doi: 10.1201/9781420052862.axf.

[35] P. D. Curtis (2015) Evaluating and Improving Cybersecurity Capabilities of the Energy Critical Infrastructure. pp. 0–5.

[36] J. D. Christopher et al. (2014) Cybersecurity Capability Maturity Model (C2M2).
https://energy.gov/oe/cybersecurity-critical-energy-infrastructure/cybersecurity-capability-maturity-model-c2m2-program

[37] M. Mylrea, S. N. G. Gourisetti, C. Larimer, and C. Noonan (2018) Insider threat cybersecurity framework webtool & methodology: Defending against complex cyber-physical threats. Proceedings - 2018 IEEE Symposium on Security and Privacy Workshops, SPW 2018, pp. 207–216.
https://doi: 10.1109/SPW.2018.00036.

[38] A. M. A. M. Rea-Guaman, T. San Feliu, J. A. J. A. Calvo-Manzano, and I. D. I. D. Sanchez-Garcia (2017) Comparative study of cybersecurity capability maturity models. Communications in Computer and Information Science, vol. 770, no. November, pp. 100–113.
https//doi: 10.1007/978-3-319-67383-7_8.

[39] B. Yigit Ozkan and M. Spruit (2019) A Questionnaire Model for Cybersecurity Maturity Assessment of Critical Infrastructures. vol. 11398 LNCS.
https://doi: 10.1007/978-3-030-12085-6_5.

[40] B. Y. Ozkan and M. Spruit (2020) Assessing and Improving Cybersecurity Maturity for SMEs: Standardization aspects," arXiv, no. August.
http://arxiv.org/abs/2007.01751

[41] US DoE (2019) Cybersecurity Capability Maturity Model (C2M2)
https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0-0%0Ahttps://www.energy.gov/sites/prod/files/2019/08/f65/C2M2 v2.0 06202019 DOE for Comment.pdf

[42] W. Newhouse, S. Keith, B. Scribner, and G. Witte (2017) National Initiative for Cybersecurity Education Cybersecurity Workforce Framework.

[43] M. Barrett (2018) Framework for improving critical infrastructure cybersecurity.

[44] R. D. Brown (2018) Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework," Qatar University Press, p. 36.
https://doi: 10.1088/1758-5090/abb063.

[45] Ozkan, B. Y., Van Lingen, S., & Spruit, M. (2021). The Cybersecurity Focus Area Maturity (CYSFAM) Model. https://doi.org/10.3390/jcp1010007

[46] Almomani, I., Ahmed, M., & Maglaras, L. (2021). Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia. PeerJ Computer Science, 7, e703. https://doi.org/10.7717/peerj-cs.703

[44] Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. Applied Sciences (Switzerland), 10(10). https://doi.org/10.3390/app10103660

[45] Ariffin, K. A. Z., & Ahmad, F. H. (2021). Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0. *Computers and Security*, *105*, 102237. https://doi.org/10.1016/j.cose.2021.102237

[46] Rahman, M. J. A., Hamzah, M. I., Yasin, M. H. M., Tahar, M. M., & Ensimau, N. . (2019). The UKM students perceptions towards cyber security.

Maznifah Salam received degree in Information Technology from University of Technology MARA, Malaysia and master's degree in Computer Security from Universiti Putra Malaysia. She is currently pursuing her study as PhD candidate in Universiti Kebangsaan Malaysia. Her primary research interests include cybersecurity, information security auditing and computer networks.

Khairul Azmi Abu Bakar received degree in Computer Engineering from Iowa State University, USA and master's degree in communication and Computer from Universiti Kebangsaan Malaysia. He was awarded Ph.D. degree in Electrical Engineering from University of Strathclyde, United Kingdom for the study on free-riding nodes in an open MANET. He is currently a senior lecturer at Center for Cyber Security under Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia. Prior to that, he was a staff researcher at MIMOS Berhad which is a Malaysia`s national applied research and development center in microelectronic and ICT. He has been involved in many R&D projects in the field of micro-controller, smartcard, security systems under open-source platform. His primary research interests include network security, internet of things and computer network. He is also a IEEE member.

Ahmad Tarmizi Abdul Ghani is a senior lecturer at the Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia. His research topic is in Service Oriented Architecture focusing on Microservice Architecture. Blockchain is also one of his research interests as it is related to distributed and decentralized architecture similar to Microservice architecture. He obtained his first degree in Information Technology from the Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia. He hold the Master degree from University of Reading, United Kingdom in Network and E-Business Centred Computing and a Ph.D holder in Computer Science from Universiti Kebangsaan Malaysia.