Building Cyber-Resilient Universities: A Tailored Maturity Model for Strengthening Cybersecurity in Higher Education

Maznifah Salam, Khairul Azmi Abu Bakar, Azana Hafizah Mohd Aman
Centre for Cyber Security-Faculty of Information Science & Technology, Universiti Kebangsaan Malaysia, Bangi, Malaysia

***Abstract*—This study explores Higher Education Institutions (HEIs) cybersecurity maturity and preparedness, developing a Cybersecurity Maturity Model (CSMM) for HEIs specific to the needs of these institutions. These HEIs face increasing cyber threats and cyberattacks from ransomware attacks, phishing attempts, and data breaches, considering increasing dependence on digital methods for administration, teaching, and research. Though cybersecurity is of paramount importance today, many institutions do not have proper structures with which they can evaluate and enhance their security practices. The study uses a mixed-method approach, whereby the integration of qualitative case studies and quantitative surveys would address this gap, subsequently allowing the identification, validation, and assessment of the key domains and criteria in a comprehensive cybersecurity framework. The research started with an investigation, followed by design, data collection, analysis, and reporting, which accounted for the major phases of the study. The data was collected through interviews, documentation reviews, and surveys involving cybersecurity experts and ICT management teams in various HEIs. The results revealed eleven important assessment domains, twenty-four criteria, and sixty-seven elements necessary for developing the CSMM: Governance, Risk Management, Infrastructure Security, Human Factors, Compliance, and Monitoring. The validation confirmed the model to be practical, reliable, and valuable in the overall sense, giving the institutions a structured avenue for assessing and improving their cybersecurity maturity.**

***Keywords*—Cybersecurity; HEIs; cybersecurity maturity model; mixed-method; governance**

I. Introduction

HEIs oversee the care of vast and delicate information. This fact owes to records for students, knowledge gained from research, finances and data in institutions. Higher cyber threats and cyberattacks in these institutions result from their inter-departmental and open characteristics in conjunction with the dynamics in this environment, making them more vulnerable than other sectors [1]. Cyber-attacks have grown exponentially; therefore, business organisations must understand cybersecurity threats and how to counter them most effectively in detail. These attacks usually aim at assessing, altering, or deleting sensitive information; extorting monetary benefits from users; or interfering with normal business processes. Cybersecurity involves techniques to protect computers and networks from unauthorized access and malicious uses such as data destruction and theft [2]. At that time, the initial days of cyberattacks were meant to boost the self-esteem of hackers and recognition. However, threats and attacks have been known to affect victims in varied ways: financial loss, impaired image, denial of service, and more [3].

The rise of cyberattacks focusing on HEIs highlights the crucial need for strong cybersecurity measures. Ransomware attacks, for example, have grown worldwide, causing massive interruptions in our educational institutions. Over 56 per cent of universities participating in a recent study were affected by ransomware within two years, thereby losing millions of dollars [4]. Additionally, there are many phishing attacks wherein cybercriminals manipulate users into providing their credentials. This situation occurs because employees do not receive enough training on this issue, and many individuals are unaware of it [5]. It could be explained that the student was cognizant of the danger but did not know how likely or how serious it could be when considering an attack by the hacker on his privacy or security [6]. The conclusions drawn by Rahman et al. (2019) were generated with respect to understanding that cybersecurity issues remain equally troubling for individuals as well as governments, companies, as well as law enforcement [7]. These vulnerabilities have been made worse by the COVID-19 pandemic. Institutions suddenly switching to remote learning had no choice but to rely on online platforms, but most lacked adequate security features [8]. Using weak access controls, outmoded software, and non-encrypted communication channels, systems were implemented fast without the necessary testing, making them susceptible to attacks targeting HEIs.

Despite their significance, most HEIs have cybersecurity budgets that are too small or do not even employ an IT specialist in this field. According to a recent CyberSecurity Malaysia (CSM) report in 2021, almost 40 per cent of Malaysian HEIs do not have an outlined framework for cybersecurity governance [9]. Malaysian HEIs without an established cybersecurity governance framework [10] are nearly 40 per cent. It is, therefore, essential to come up with structured, scalable, and cheap measures that can help assess and enhance the preparedness of our institutions regarding their information system security, such as customised models that allow maturity tracking. The model or framework's all-encompassing, general approach just may fail to account for all the industry-specific threats or intricate cybersecurity issues [11]. The rapid adoption of digital technologies within HEIs has significantly transformed the way institutions operate, communicate, and deliver education. Hybrids such as online learning platforms, virtual classrooms, and digital administrative systems have been very potent conduits through which innovations have been

brought into higher education institutions as their lifeblood. However, the rapid influx of these forms of education by HEIs has also heightened the risks of exposure to cyber threats, making student records, financial transactions, and critical research data tempting targets to all manner of cybercriminals through ransomware attacks, phishing attempts, and data breaches [1].

The pandemic of COVID-19 exacerbated the existing conditions, whereby institutions were entirely dependent on the digital platform, exposing areas in the existing cybersecurity foundations. The sudden emergence of demand for both distance education and hybrid education models revealed several vulnerabilities in the security infrastructure of institutions, exposing them to several types of cyber threats targeted at cloud-based systems, network access points, and communication channels [8, 10]. While many forms of cybersecurity standards-such as NIST, ISO/IEC 27001, or CIS Controls, have been used in industries like healthcare, finance, and government environments, these have not been available to HEIs in a typical sector-specific cybersecurity framework addressing internal unique challenges [12]. This particular concern will require some form of cybersecurity maturity model customised to the higher education sector, merging governance, risk management, and security monitoring practices.

An additional complication in HEIs is the presence of outdated systems of security, financial constraints, and the absence of cybersecurity capabilities within the institution [13]. If proper remedial measures are not introduced, cyber threats will evolve to ever-increasing levels of sophistication, leading to serious reputational damage, financial loss, and possible disruption to the academic environment [12]. The real challenge comes from the abysmally lacking a dedicated model to assess maturity levels suited explicitly to HEIs. This term, in general maturity level, concerns progress and development involving organisational indicators, which are people, process, technology, capability, and willingness to adopt quality improvement practices. Organisational maturity depends on the maturity model selected by the organisation [13]. The cybersecurity model in existence does not have the requisite specificity to address the role of students, faculty, and administrative personnel within these institutions and the added challenge of handling cybersecurity in a resource-constrained environment [14]. Based on Zammani et al (2021) studies, the assessment of maturity is not comprehensively implemented and remains low [15]. Because of that, a tailor-fitted Cybersecurity Maturity Model (CSMM) becomes necessary to evaluate the cybersecurity maturity of HEIs, understand the gaps for improvement, and lend structured guidance on enhancing institutional cybersecurity readiness.

The research is aimed at evolving a robust CSMM specifically tailored for HEIs to improve their resilience in cybersecurity. First, it enumerates crucial domains, criteria, and factors needed for measuring cybersecurity maturity in HEIs, thus laying down a structured framework for evaluating institutional security readiness. Qualitative and quantitative techniques are used in this study to validate these criteria, thereby ascertaining their relevance and effectiveness within the practical environment. The research also deals with the design and evaluation of a working CSMM that targets the salient cybersecurity challenges faced by HEIs, thus providing them with a strategic roadmap to improve their security infrastructure. Additionally, the study gives practical implementation recommendations for the proposed CSMM to support the HEIs in strengthening their cybersecurity governance against emerging threats. It is through its realisation of these objectives that the research gives insight into cybersecurity maturity assessment and a scientific approach through which HEIs can better their general security posture.

The methodology involves major inquiries directing the making of a viable CSMM for HEIs in pursuit of these research objectives: first, identification of the primary domains and criteria needed for gauging maturity in the area of cybersecurity for higher education institutions, providing a comprehensive evaluation procedure; then assessment of the methods that were applied in designing and validating a CSMM that specifically intends to tackle the cybersecurity problems inherent in HEIs by synthesizing qualitative and quantitative perspectives to broaden applicability. Finally, the effect of the CSMM designed for the study in measuring and improving readiness in cyberspace is tested to ensure that the system is practicable in real institutional environments. However, this study is a more systematic approach towards the institution's efforts to enhance its cybersecurity governance from within. Such efforts will provide an institution with a robust framework to minimise risks, mitigate the impact of ever-changing threats in cyberspace, and improve overall institutional resilience against attacks.

The primary concern of HEIs today is cybersecurity since the institutions process the most sensitive data and intellectual property. This research contributes towards academic discussions and applications of practical cybersecurity. Practically speaking, the CSMM may give an ordered view for HEIs to evaluate their cybersecurity posture, create priorities for investments in governance, and mitigate security risks. The study advances the theoretical understanding of the cybersecurity maturity model, especially in the education sector, by taking into consideration different unique challenges that HEIs face while incorporating qualitative and quantitative research methodologies, which ensures a validated and empirical model that is usable across various institutions of higher education [16]. Findings from this study, which are of policy importance, will be very useful to policymakers and education authorities interested in standardised cybersecurity practices in all HEIs. The policy agrees with laws like the Cybersecurity Act 2024 of Malaysia and the cybersecurity regulations of the European Parliament, ensuring that HEIs comply with both national and international standards in cybersecurity [17].

The continued evolution of digitalisation in HEIs makes cybersecurity a priority issue for institutional leaders and stakeholders. However, a lack of an education sector-specific cybersecurity maturity framework has rendered institutions incapable of adequately responding to cyber threats as they evolve. This study aims to propose such a framework, CSMM, which will offer HEIs a viable strategy towards greater cybersecurity resilience. The department covers different activities, including the use of technologies, processes, and policies, all aimed at protecting digital assets from threats such as malware, phishing, and unauthorised access. For educational

institutions, cybersecurity is indispensable in protecting student data, preserving academic record integrity, and generally facilitating digital learning [18]. This study adopts both qualitative and quantitative research approaches to ensure that the proposed model addresses specific challenges to cybersecurity in HEIs. The model also gives recommendations that facilitate improving the institutional cybersecurity strategy and governance.

This study endeavours to lay out a clear and coherent argument for the research. Section II of the study is applied to review all the literature pertaining to cybersecurity frameworks, maturity models, and the challenges HEIs face in cybersecurity. Section III details the research methodology, explaining the mixed-method approach and data collection techniques employed in this study. Finally, Section IV concludes the study by summarising the key findings, discussing the research's contributions, addressing its limitations, and providing recommendations for future studies. By structuring the study in this manner, the research ensures a logical progression from identifying cybersecurity challenges in HEIs to proposing a viable solution through the CSMM.

II. Related Works

Educational institutions, particularly organisations, are seriously concerned about the issue of keeping their data and information safe from hacking using the Internet. Over the years, HEIs have increased their dependence on technologies regarding research work and everyday running, exposing them to cyber threats. In this part, previous studies and applicable models concerning cybersecurity issues are discussed in addition to those factors missing in place for a customised CSMM for these institutions, alongside all their existing maturity models. The discussion focuses on five key areas: cybersecurity in HEIs, established cybersecurity frameworks, existing cybersecurity maturity models, cybersecurity-specific challenges in education, and the gaps in current approaches.

A. Existing Cybersecurity Frameworks

There indeed exist many established frameworks that offer basic principles to follow to boost cybersecurity. Nevertheless, most of those frameworks are not tailored or aligned with specific requirements at higher learning institutions. Considered herein are numerous widely used models of enhanced cybersecurity.

1) NIST Cybersecurity framework

- The NIST Cybersecurity Framework is a widely accepted approach for managing cybersecurity risks across various sectors. It was initially published in 2014. In 2018, Version 1.1 was rolled out with some key improvements, particularly in how supply chain risks were managed and how organisations could assess themselves more effectively. Come 2024 and this new Version 2.0, the evolution of the framework is set to go far beyond security and introduce fresh insights on how to continue to improve security measures over time for cyber governance. The new structure has five primary functions: Identify, Protect, Detect, Respond, and Recover [19].

2) ISO/IEC 27001

- The ISO/IEC 27001 Standard provides the framework for establishing an Information Security Management System (ISMS). Information security, in general, uses ISO/IEC 27001 as an international reference point. The standard was first published in 2005, after being developed jointly by ISO and IEC; it underwent a major revision in 2013 and was thus revised again in 2022 to keep abreast of changing security challenges. It focuses on implementing comprehensive policies and processes and conducting risk assessments to protect an organisation's valuable data assets. This standard helps organisations systematically manage and safeguard information security, addressing potential risks and vulnerabilities [20]. Many companies have embraced ISO/IEC 27001, but it is very resource-demanding, making it difficult for higher learning institutions to implement. However, budgetary constraints and limited staff often hinder HEIs from continuously monitoring, auditing and improving their compliance framework, making maintenance challenging [16].

3) CIS Controls

- The Centre for Internet Security (CIS) Controls provides a set of prioritised actions designed to help organisations safeguard their systems against cyber threats. The CIS framework consists of 18 essential controls, covering areas such as inventory management, incident response, and recovery [4]. This approach particularly appeals to organisations looking for practical, actionable steps to enhance their cybersecurity posture. However, while CIS Controls offer comprehensive guidance, they do not specifically address the unique needs of the educational sector, which often faces the challenge of balancing robust security measures with the need for academic openness and accessibility

4) Malaysian Cybersecurity Act 2024

- With a view to enhancing cybersecurity governance in all areas of the industry, including education, Malaysia has introduced the Cybersecurity Act 2024 as a significant leverage for strengthening the country's digital security [21]. Operative guidelines for enabling organisations to develop sound security policies, good risk management, and structured reporting of cyber incidents are defined in this law. This act, which will come into force on August 26, 2024, provides for the protection of critical national infrastructure, effective measures against cyber threats, and tight regulation of registered cybersecurity service providers' activities. This is because of the often-decentralised management of universities and differences in cyber readiness, which may raise unique issues regarding the adaptation of new standards that will need to be skilfully orchestrated.

5) Cybersecurity Maturity Models (CMM)

- Cybersecurity Maturity Models (CMM), road maps being structured for organisations, help organisations assess, strengthen, and continuously improve their

cybersecurity posture. With these models, we identify various security gaps and areas of improvement, allowing organisations to set priorities related to improving their cybersecurity stance, increasing resilience, and systematically addressing areas of concern [22]. These evaluate processes, systems, and policies at various stages of maturity so that the organisation is aware of its current standing in cybersecurity and how to improve it. Following these models truly is a structured way to improve security posture, systematically addressing vulnerabilities.

6) Capability Maturity Model Integration (CMMI)

- The Capability Maturity Model (CMM) is a project developed by the Software Engineering Institute (SEI) of Carnegie Mellon University for evaluating the improvement of software development processes. The model provided a means for organisations to assess their capabilities, find weaknesses, and improve their process under five levels of maturity from Level 1 (Initial) to Level 5 (Optimised) [22]. The CMMI hence provides a structured way for organisations to assess, improve, and optimise their cyber capabilities; however, the one-size-fits-all approach does not consider the specific needs of the education sector, where institutions may not have the required technical expertise or financial resources to complete the requirements. Therefore, the HEIs need a more adaptable cybersecurity maturity model that considers their open IT ecosystems, different user groups, and constraints of budget. A customised framework would allow universities to make improvements in security based on need, to comply with ever-changing regulations, and to enhance their programmatic approach towards cyber resilience without excessive complication. Cybersecurity models should therefore evolve to create a fine balance between stringent security and an academic environment's intrinsic need for flexibility [23].

7) Cybersecurity Capability Maturity Model (C2M2)

a) The Capability Maturity Model Integration (CMMI) was created by the Software Engineering Institute (SEI) at Carnegie Mellon University during the early part of this century to improve further the original Capability Maturity Model (CMM) [24]. In essence, CMM was introduced in the late 1980s specifically for the purpose of aiding organisations in enhancing their software development process [23]. However, industries realised that.

b) Nonetheless, CMMI had to be introduced as a common model of best practices, which consolidated process management, product development, service delivery, and cybersecurity into a framework [22]. Five maturity Levels from Level 1-Initial to Level 5-Optimized were introduced to assess, standardise, and continuously improve processes within an organisation in a structured manner.

8) Qatar Cyber Security Capability Maturity Model (Q-C2M2)

a) Developed in 2018 by the College of Law at Qatar University, the Qatar Cyber Security Capability Maturity Model (Q-C2M2) represents one of the major efforts by Qatar towards improving its national cybersecurity framework [25]. While not entirely a new model, Q-C2M2 adopts various key elements from existing cybersecurity frameworks to provide an orderly and holistic approach in assessing cybersecurity capabilities [26].

b) The model is intended to assess both government agencies and private organisations over five maturity levels concerned with core cybersecurity functions [20]. The adoption of a multi-framework approach would make the Q-C2M2 a standardised and scalable cybersecurity assessment tool that caters to the peculiarities of the cybersecurity landscape in Qatar.

9) Cybersecurity Capacity Maturity Model for Nations (CMM)

a) As a global cybersecurity capacity centre, and operator of the Global Cyber Security Capacity Centre (GCSCC), the CMM was established at Oxford Martin School University of Oxford in the year 2014 with the aim of enabling nations to assess, improve, and develop their capabilities in cybersecurity with its structured framework [27, 28, 29].

b) After its initial launch, the model was implemented in 11 different countries, leading to improvements in 2016 because of practical lessons learned from accurate assessments [30]. This was made possible by continuously going through this process and evolving to create a more comprehensive and adaptable tool to be helpful in improving the cybersecurity resilience of different national contexts [31].

c) This is an important instrument for countries wishing to fortify their respective cyberspace infrastructures. It can offer a transparent, structured approach for governments; hence, they can identify gaps and improvements for long-term strategies, which would be used to safeguard their digital ecosystems [32, 33].

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

a) The National Initiative for Cybersecurity Education (NICE) model was introduced in 2008 by U.S. President George W. Bush as part of a national effort to strengthen cybersecurity workforce development [34]. This initiative emerged in response to the growing need for highly skilled cybersecurity professionals capable of addressing national security challenges.

b) To achieve these objectives, NICE introduced a framework known as the NICE Component, which helps organisations plan and manage cybersecurity talent strategically. The first formal version of the NICE model, Version 1.0, was released in August 2014, providing a structured approach for organisations to identify cybersecurity job roles, competencies, and workforce needs [35].

11)Community Cyber Security Maturity Model (CCSMM)

a) The Cybersecurity Capability Maturity Model for Infrastructure Assurance and Security (CCSMM) was developed in San Antonio, Texas, by The Centre as part of an initiative to help states and communities build sustainable and

effective cybersecurity programs [30, 35]. The model was mainly designed to strengthen cybersecurity within the U.S. tax sector, addressing vulnerabilities in financial infrastructure and ensuring critical assets are protected.

b) Rather than serving as a one-size-fits-all solution, the CCSMM enables organisations to evaluate and enhance their cybersecurity programs through structured tests and exercises [36]. It focuses on collaboration between local, state, and federal authorities, helping them identify key assets, potential threats, and areas requiring stronger security measures [37]. The model's goal is to guide various sectors toward achieving an optimal level of cybersecurity maturity, ensuring they can effectively manage risks and respond to evolving cyber threats [38].

12)RAKKSA (Rangka Kerja Keselamatan Siber Sektor Awam

a) The RAKKSA version 1.0 was introduced in 2016 as a cybersecurity maturity model designed explicitly for public organisations in Malaysia [39]. Developed to strengthen cybersecurity governance, risk management, and compliance (GRC), RAKKSA provides a structured framework that helps public institutions assess their security posture, identify vulnerabilities, and implement necessary security measures.

b) Unlike generic cybersecurity models, RAKKSA was tailored to meet the specific needs of Malaysian public organisations, ensuring alignment with local regulations and policies. It aims to enhance cybersecurity readiness by guiding institutions through progressive security maturity levels, helping them improve resilience against cyber threats.

c) While RAKKSA was primarily designed for government agencies, its adoption in HEIs remains limited. The framework is still in its developmental stages and has not yet been widely implemented in the education sector, highlighting the need for further research and adaptation [39].

B. Some Common Mistakes

Whilst there are currently many frameworks and maturity models in the field of cybersecurity, unfortunately, all these do not meet the specific requirements of higher education institutions. Some of the major gaps in existing frameworks that have been indicated present serious challenges in achieving effective management of cybersecurity by HEIs. One such concern is the very limited application of available customisation - for example, most frameworks are specifically oriented either towards enterprises or critical infrastructure situated under much-defined, budget-ablative environments. HEIs operate mostly under open and cooperative frameworks with limited budgets; thus, practically making these frameworks quite cumbersome and more complex to apply [40]. Equity is, again, highlighted by another noticeable gap- the absence of holistic assessment tools. The current maturity models cannot provide a comprehensive yet easy-to-use evaluation mechanism that caters for the realities of operations at HEIs. Thus, these institutions would find it difficult to assess their cybersecurity posture and the areas for improvement accurately.

Thus, in existing frameworks, one of the critical points that is not addressed would be related to human factors like those of a culture of cybersecurity awareness and behaviour, as well as the role of the environment. As much as there is emphasis on the technical control side, the most critical and active role is played by individuals and governance [41]. The disconnect between cybersecurity frameworks and national policies like that of Malaysia's Cybersecurity Act produces mismatches in strategic objectives, making it difficult for institutions to align both their own and higher legislation and regulatory requirements [42].

A review of related works shows unique challenges that HEIs face with cybersecurity, given their openness and increasing dependence on digital technologies. While NIST, ISO/IEC 27001, and CIS Controls have a very strong basis, they have no such capacity to address the issues that are nuanced to educational institutions. Likewise, maturity models such as CMMI and C2M2 are meant for general organisational use; they are usually resource-consuming or so specific as to be out of the reach of HEIs with low technical and financial capacities. This study will, therefore, develop the CSMM specifically for HEIs to meet these specific challenges. Such CSMM would, therefore, address issues identified earlier by improvising a fusion of the technical and non-technical components-including governance, infrastructure, risk management, and human factors, offering practical, scalable, and systematic approaches towards HEIs evaluating and improving their cybersecurity maturity. This model, focusing primarily on the unique needs of HEIs, could have an impact in terms of enabling institutions to have strong, adaptable frameworks for constructing a secure and resilient digital environment.

III. RESEARCH METHODOLOGY

The research methodology is the heart of this study, giving a scheme to tackle the research questions while meeting the study objectives systematically. This section describes the comprehensive methodology used for the design and validation of a CSMM specifically for HEIs. It includes a clear explanation of research design, methods of data collection, sampling techniques, data analysis methods, and ethical considerations that guided the study. Through a mixed-method approach that synergistically joined qualitative and quantitative techniques, a holistic understanding of the cybersecurity maturity of the HEIs was arrived at. The approach facilitated multiple perspectives and presented a well-structured means to answer the study's objectives.

The outline of this section is methodically structured to cover key methodological elements. The first sub-section elaborates on research design, providing a background to the overall architecture and approach of the study. This is followed by an explanation of the phased data collection, where insights are drawn from different stakeholders in HEIs. Attention then turns to the sampling strategies, explaining how participants and data sources were selected so as to maximise relevance and representativeness. This part follows with a discussion of the methods for data analysis that were used to interpret the findings, such that the analysis was thorough and aligned with the goals of the study. Special attention to ensuring the reliability and validity of the research process to gain credibility and trustworthiness for the results. Finally, it discusses ethical issues during the study, e.g. informed consent, confidentiality of data, and respect for the rights of the participants.

The methodological setup strengthens the study's claim of making a credible and valuable contribution to the field of cybersecurity for HEIs. This means that by joining qualitative insights with quantitative rigour, the CSMM proposed is practical and valid from a scientific point of view.

A. Research Design

Underlying concept research gives a blueprint for performing complete procedures in the field, such as how data can be collected, analysed and interpreted. This study adopts a mixed-method exploratory design that entails using qualitative and quantitative approaches to answer the research questions effectively. Mixed methods were used for this study because they bring together the strengths of both qualitative and quantitative research, thus allowing a comprehensive picture of the research problem to emerge. As Creswell and Clark (2024) argue, mixed methods provide a balanced view, deep context, rich insights from qualitative research and measurable, statistically validated results from quantitative analysis [38]. The study was thus executed through two distinct phases: a qualitative phase, conceptualisation of current cybersecurity practices within HEIs, which has culminated in identifying those critical domains, criteria, and elements necessary for the CSMM development proposed in this study. It has provided a granular insight into challenges that HEIs encounter and how they can form a basis for designing the model.

The quantitative phase followed the qualitative course to validate the results of the previous stage. The phase's objective was to evaluate the usability, effectiveness, and overall applicability of the suggested CSMM. This phase is integrated from a larger sample into the model concerning practical and general real-world use across various HEI contexts. These two strands thus made sure that the research problem was substantially appreciated while adding value to the trustworthiness and reliability of the study output [43]. Providing qualitative as well as quantitative insights thus added value to the findings and, importantly, provided a firm basis to deal with unique cybersecurity challenges for HEIs.

B. Phases of the Study

The study execution entailed five stages of operationalisation, as schematised in Fig. 1.

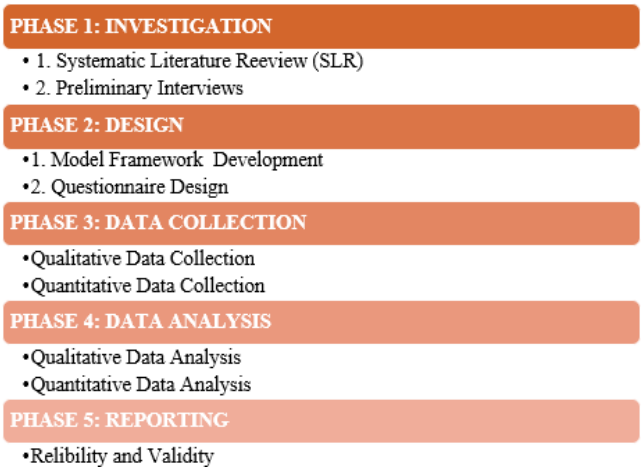

Fig. 1. Operational phases.

The framework addresses both technical and organisational aspects of cybersecurity, hence ensuring an institution-specific, holistic, and practical solution to the distinctive needs of HEIs. The Data Collection phase, the third phase, used a two-pronged approach to capture an exhaustive assessment of cybersecurity maturity levels at HEIs. The first stage of the collection consisted of qualitative data obtained using case studies, focusing on in-depth interviews, document analysis, and observational studies. These provided rich, contextual material about institutional cybersecurity practices and challenges. The latter collection activity was through quantitative data via surveys of 400 cybersecurity professionals and ICT managers, whose insights served to validate some of the data obtained during the qualitative phase. The integration of both qualitative and quantitative data also ensured that research was context-rich but substantively measurable and statistically evidenced, hence boosting the credibility of the CSMM proposed.

After the collection of data, the next step was to move to the Data Analysis phase for the refinement and validation of the CSMM. The use of thematic analysis, statistical evaluation, and the Analytic Hierarchy Process (AHP) served to prioritise the identified cybersecurity criteria to reflect accurate maturity for the critical factor in HEIs that would influence cybersecurity maturity [44]. The prioritisation of cybersecurity elements based on expert input and empirical data is further enhanced using AHP, making the model more applicable and reliable.

The last phase involved the Report, which consisted of collating, interpreting, and documenting the findings of the research to produce the final CSMM. Therefore, it also recommended HEIs on how to implement the model to improve their overall cybersecurity posture. The final output of this study gives a structured and validated way of assessing and improving cybersecurity maturity across HEIs and providing these institutions with a viable tool for addressing cyber threats and overall improved resilience in the more and more digitalised education landscape.

C. Data Collection Methods

Both qualitative and quantitative methods were combined for complete analysis, and a mixed-methods approach was used in this research. Qualitative research would provide an in-depth understanding of the experiences and perceptions held by participants. The other end of the spectrum was where the quantitative research produced data which could be measured to find out patterns and trends, thus making it a wholesome study of acquiring knowledge around that phenomenon.

1) Qualitative data collection

a) The qualitative phase investigated the practices, challenges and maturity levels regarding cybersecurity in higher education institutions.

b) It has employed a multiple-case study as appropriate for Yin to achieve a detailed understanding of cybersecurity within HEIs. The approach involved participants from various backgrounds, including ICT managers, cybersecurity experts, and senior administrators [45]. The data collection instruments used were semi-structured interviews and document reviews, which allow for a more comprehensive view. Typical interviews lasted between one to two hours and were recorded,

transcribed, and systematically coded. Also, in addition to the interviews, specific institutions such as cybersecurity policy, risk management and incident logs were reviewed for an enhanced context and additional insights. Face-to-face observations in workshops and IT meetings also added real-world practices and interactions to the findings.

c) The qualitative data collected through these procedures have been processed systematically and later analysed using ATLAS.TI software with its thematic coding and comprehensive analysis [46]. This kind of systematic procedure allowed key themes and patterns to be identified for a better understanding of the cybersecurity landscape in higher education institutions and the foundation to build on towards the following construct of the CSMM [47].

2) Quantitative data collection

a) The quantitative phase was focused on getting validation of domains and criteria that were identified during the qualitative phase. A well-structured questionnaire was distributed among cybersecurity practitioners and ICT management teams in institutions of higher learning. The questionnaire is designed under three clear sections. In Section A, the questionnaire collected demographic information with respect to the respondents' origins. Section B validated the CSMM, including 11 domains, 24 criteria, and 67 elements, each rated on a 5-point Likert scale running from 1 for Strongly Disagree to 5 for Strongly Agree. Section C collected feedback on the usability and relevance of the model to ensure its practical applicability. Prior to the full rollout, a small group of experts piloted the tools to refine the questionnaire to address ambiguities before enhancing reliability [9].

b) The survey was conducted among cybersecurity practitioners from the management core of Malaysian HEIs together with ICT officers, and therefore, purposively sampled as the identification of participants who should take part has become important [47]. The total sample size targeted for collation from respondents was 25 respondents to ensure the collection of sufficient data for carrying out statistical validation procedures. Data was captured via Google Forms, which were accessed and secured for confidentiality. All this data was analysed using the Statistical Package for Social Scientists (SPSS) software for scoring respondent data and validating findings. This fully structured and planned approach made this process not only robust but also reliable for the assessment of CSMM and its use within the targeted context.

D. Data Analysis Methods

In accordance with their research aims, the study considers specific data analysis methods that will help to make the findings true and credible. Thematic analysis, regarding the Braun and Clarke framework, was utilised in processing qualitative data. It involved getting familiar with the data, then generating initial codes and identifying themes, followed by identifying and revising to ensure they form tight links with the research aims. The systematic analysis of interviews, document reviews, and observations allows understanding to go in-depth into key issues and patterns pertaining to the study [48].

On the other hand, quantitative data analysis subjected the said data to relevant statistical methods to authenticate the model being proposed: descriptive statistics, which had been the initial processing tools in which profiles and responses from the respondents were entered. In contrast, reliability analysis (through Cronbach's Alpha) was then used to determine the internal consistency of survey items, which determined their dependability. The AHP was also used to rank criteria within the model. This enabled a systematic basis for ordering as per expert answers. Feedback about usability was viewed in simple percentage-based summaries for its practical applicability regarding the model. These methods would give us the rigour and robustness of analysis that is expected to give meaningful insights into the research objectives [49].

1) Qualitative data analysis

a) Qualitative data collected from interviews, document reviews, and observations were analysed thematically, under the direction of Braun and Clarke [50]. The analytical framework followed a systematic manner in relation to the data's purpose and the understanding of what it was about. Data familiarisation was the first step, involving deep immersion into transcripts and documents to identify key themes that emerged during the analysis [48]. During this phase, the researcher gained a panoramic view of the data while noting the recurring themes and patterns pertinent to cybersecurity maturity.

b) Then, the process advanced to coding-whereby initial codes were generated because of consistent patterns within the data and thereafter grouped into broader themes reflecting pivotal aspects of cybersecurity maturity from a framework for further analysis. Refining the themes ensured that they made sense and answered the research objectives. This meant that the identified themes went through an additional examination and validation process to ensure that the themes were more precise and relevant, especially in that the findings illustrate the qualitative perspectives collected in the study.

2) Quantitative data analysis

a) The data collected through quantitative surveys were subjected to analysis with respect to different statistical techniques to validate the proposed CSMM. Descriptive statistics, such as frequencies, means and standard deviations, were used to comprehend the profiles of respondents as well as their response types. This first stage produced good insight into how the data were distributed and central tendencies. Further, Cronbach's alpha was used to ensure the reliability of the survey instrument by testing the internal consistency of the items on the survey, establishing that the measures were cohesive and reliable enough for conclusions [49].

b) Moreover, the AHP was adopted for prioritisation of the different criteria within the CSMM on the grounds of responses from experts [50]. This methodology provided a systematised ranking of factors through the calculation of weightage and consistency ratios such that the model truly reflected well politically informed judgments. Feedback in terms of usability was also evaluated from the CSMM through simple summary percentage analyses, giving the practical relevance of perception from respondents. Combined, these statistical methods fully validated the model while proving

reliable and usable in a cybersecurity context. The model comprises eleven domains and twenty-four criteria to assess cybersecurity maturity in HEIs. The domains and their corresponding criteria are summarised in Table I.

TABLE I. DOMAINS AND CRITERIA FOR THE PROPOSED CSMM

Domain	Criteria
1. Governance	1.1. Cybersecurity governance
	1.2. Top Management
	1.3. Cybersecurity Policy and Procedure
2. Risk Management	2.1. Risk Assessment
	2.2. Risk Treatment
3. Compliance	3.1. Cybersecurity Standards and Best Practices
	3.2. Cybersecurity Auditing
4. Human Resource Security	4.1. Competence and Awareness Development
	4.2. ICT staff competency, training and awareness
5. Asset Management	5.1. Asset Inventory Management
	5.2. Information classification
6. Identity and Access Management	6.1. Identity Verification Mechanisms
	6.2. Access management
7. Third-party Management	7.1. Awareness and enforcement.
	7.2. Third-party effectiveness evaluation
	7.3. Experts and Expert Groups
8. System And Application Security Management	8.1. Network and System Infrastructure Security Control
	8.2. Security operations
9. Incident Management	9.1. Cybersecurity Incident Plan
	9.2. Cybersecurity Incident Simulation
10. Threat and Vulnerability Management	10.1. Cybersecurity threat and vulnerability management procedures
	10.2. Technology for threat and vulnerability management.
11. ICT Business Continuity Management	11.1. ICT Business Continuity Plan
	11.2. Simulation

E. Reporting

1) Reliability: Ensuring reliability gives a guarantee of uniformity and precision throughout data collection and analysis of the processes. This study maintained qualitative reliability by developing a detailed case study protocol that would apply to all interviews. Thus, uniformity in the way the interviews were conducted minimised the variations and, therefore, strengthened the credibility of the qualitative findings [45]. The protocol provisioned areas for systematic exploration of relevant themes while maintaining consistency across all interactions.

For the quantitative part, reliability was measured by calculating the Cronbach's Alpha values for the items of the survey. All these figures surpassed the threshold of 0.7, indicating that the instrument was revealed to have high internal consistency and that the items measured the constructions reliably in an accurate way. Such a kind of statistical validation could add robustness to quantitative analysis, making sure that the data collected will be reliable for meaningful conclusions. All these measures combined put more weight on the reliability of the study. Thus, its data supported the findings' validity [50].

2) Validity: Validity is one of the cornerstone points of research, ensuring that what was measured was what was intended to be measured. For the qualitative aspect of the study, validity was taken care of through triangulation of data, in which multiple sources were integrated, such as interviews, document reviews, and observations. This approach has increased the credibility of the findings through cross-referencing insights from different perspectives, thereby allowing for bias reduction and providing a holistic understanding of the research context involved. It was one of the robust mechanisms that ensured the strengthening of the qualitative outcomes' trustworthiness [49].

In the quantitative phase, an assessment of validity was conducted via reviews of the questionnaire by experts. This validated the aspects of face validity and content validity, thus ensuring that the specific items in the survey were appropriate and relevant to the objectives of the study, being transparent and easily interpretable by potential respondents. Feedback from the experts also ensured that the instrument captured the intended constructions, further enhancing the validity and reliability of the quantitative data. These stringent processes in both phases of the research ensured that the study produced valid and credible results.

IV. CONCLUSION

The CSMM is developed from the literature review, using a quantitative and qualitative approach. However, it is different from the others, as it treats the uniqueness of all HEIs, including limited resources, old-fashioned systems, and open academic environments that demand flexible yet secure solutions. This model provides two significant innovations. The first domain expansion is, of course, non-generic, including human and governance matters to better relate to institutional culture and identify gaps in leadership. Secondly, the CSMM has been designed with usability in mind; with its eleven domains and twenty-four criteria, a more efficient structure for HEIs functionally operating with limited resources offers a more complete and efficient approach for increasing cybersecurity maturity.

Some findings confirm existing research on governance, infrastructure security, and awareness training in HEIs. Lack of awareness and human error are among the substantial causes of cybersecurity breaches. A validated CSMM gives HEIs a structured yet practical approach to assessing and improving cybersecurity maturity. With this model, the institutions can systematically discover their vulnerabilities while developing and enhancing the obvious and resource-wise productive cybersecurity strategies. As a result, investing shall be directed towards the most important investments, i.e., weaknesses. The CSMM also helps deliver customised training to strengthen human factors, such as expanded awareness and ability to

respond to cyber threats, thereby improving the overall cybersecurity posture for the institution.

The assessment of the maturity level in cybersecurity for an HEI uses the domains and criteria defined in this model to evaluate the current state of the institution. This allows the identification of the gaps and weaknesses and a spearhead in focusing the institution's effort and resources on the areas that need the most attention. As an additional benefit, the CSMM guides the refinement of governance structures for effective policy enforcement of cybersecurity measures. By such a personalised approach, HEIs can tailor the model to address their unique problems, such as limited resources, legacy systems, and open academic environment demands. Therefore, the combination of workable tools with adaptability makes the CSMM an asset for enhancing cybersecurity in educational institutions.

The study's qualitative and quantitative findings are revealed here. It is a thematic analysis of the eleven domains used to determine the maturity levels of cybersecurity at higher learning institutions. Evaluation of these broad areas was then followed by quantitative validation to validate the relevance or otherwise of the areas assessed and to reveal which Infrastructure Security or Governance turned out to be most emphasised. Thematic analysis of qualitative data, which includes the conclusion in deriving eleven major domains for the assessment of cybersecurity maturity in HEIS, found that the integrated findings formed a practical and robust CSMM specifically intended for HEIS. Quantitative validation confirmed the relevance and importance associated with these domains, while defining Infrastructure Security and Governance as of paramount importance.

While the research draws important insights into cybersecurity maturity models geared towards HEIs, the study must admit some limitations. One limitation comes from its focus on a particular geographical context—mainly Malaysian HEIs—thereby restricting the extent to which findings can be generalised to regions where infrastructure and regulatory environment function differently. Additionally, the research takes self-reported data from ICT professionals and cybersecurity experts, which might pose issues related to bias. The level of applicability of the model to any HEI might change, especially as some operate on a shoestring, while others enjoy loads of resources for their operations; hence, testing it across various institutional backgrounds would be worthwhile. Finally, the matter of integrating emerging technologies into enhancing cybersecurity maturity, be it AI or machine learning, was not studied.

While on the findings of this study, several areas could be explored and which could further develop and refine the proposed CSMM. The first important direction could be to make the model applicable across various geographical regions, especially in developing countries, where additional challenges exist on account of lack of resources and infrastructure. Maturing on the model could also involve integrating cybersecurity threat intelligence in real time. As cybersecurity threats change rapidly, it would be very beneficial if adaptive measures could be integrated that use artificial intelligence (AI) and machine learning (ML) to predict and respond to newly arising threats.

Future research could investigate incorporating user behaviour analytics (UBA) in the CSMM, given that human error remains a major threat to cybersecurity. Insights into the effects of user behaviour patterns on institutional cybersecurity may aid in designing interventions that are more targeted and effective. Additionally, exploring how the maturity model can be modified to suit various sizes and types of organisations (small colleges versus big universities) would assist in further fine-tuning its scalability and flexibility.

Another interesting orientation would be to investigate the long-term impact of placing and running a CSMM on an organisation's resilience and response times to cyber threats, therefore truly assessing its effectiveness over time.

ACKNOWLEDGMENT

This publication could not have been accomplished without the institution's extraordinary assistance. We also want to thank the reviewers whose suggestions will help make this manuscript eligible for publication.

REFERENCES

[1] Alasmary, H., et al. (2020). Cybersecurity in education: Challenges and solutions. IEEE Access, 8, 185586–185600. https://doi.org/10.1109/ACCESS.2020.3023459

[2] Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. Sensors, 23(15), 1–20. https://doi.org/10.3390/s23156666

[3] Majid, M. A., Akram, K., & Ariffin, Z. (2021). Model for successful development and implementation of Cyber Security Operations Centre (SOC). PLOS ONE, November. https://doi.org/10.1371/journal.pone.0260157

[4] Center for Internet Security (CIS). (2021). Critical security controls for effective cyber defense. Retrieved from https://www.cisecurity.org.

[5] Cybersecurity Ventures. (2022). Phishing in education: A growing concern. Cybersecurity Reports. Retrieved from https://cybersecurityventures.com.my

[6] Abdulsahib, A. A. (2023). Anatomy of Network Security Execution through Utilizing SPSS to Evaluate Public Wi-Fi. Asia-Pacific Journal of Information Technology & Multimedia, 12(1).

[7] Rahman, M. J. A., Hamzah, M. I., Yasin, M. H. M., Tahar, M. M., Haron, Z., & Ensimau, N. K. (2019). The UKM Students Perception towards Cyber Security. Creative Education, 10, 2850-2858. https://doi.org/10.4236/ce.2019.1012211

[8] Litan, A. (2021). The impact of remote learning on cybersecurity in higher education institutions. Cyber Threat Intelligence Review, 5(3), 88-102.

[9] Johnson, K. (2021). Ransomware attacks in higher education. Journal of Cybersecurity Trends, 4(2), 32–45.

[10] CISA. (2022). Cybersecurity best practices for educational institutions. Cybersecurity & Infrastructure Security Agency.

[11] NIST. (2018). Framework for improving critical infrastructure cybersecurity. Retrieved from https://www.nist.gov

[12] Parker, R., & Santamaría, D. (2020). Higher education cybersecurity: Addressing risks and vulnerabilities. Cybersecurity Journal for Academia, 8(1), 33-51.

[13] 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.

[14] Tewari, R., Pandey, A., & Sharma, M. (2020). Emerging cyber threats in universities: A strategic risk management approach. Journal of Information Security & Risk Management, 7(4), 99-118.

[15] Zammani, M., & Razali, R. (2021). Organisational Information Security Management Maturity Model. International Journal of Advanced Computer Science and Applications, January. https://doi.org/10.14569/IJACSA.2021.0120974

[16] Harper, L., & Thorne, J. (2024). A tailored cybersecurity maturity model for higher education institutions: Addressing sector-specific challenges. International Journal of Cybersecurity Studies, 6(2), 45-63.

[17] CSM. (2021). Cybersecurity framework compliance for educational institutions. Cybersecurity Malaysia.

[18] Vigneswari, T., Pramila, S., Gomathi, M. v, & Madhumitha, M. (2023). Enhancing Cybersecurity in Educational Institutions: Challenges and Strategies. Eureka Publication.

[19] National Institute of Standards and Technology (NIST). (2020). Cybersecurity Framework. Retrieved from https://www.nist.gov/cyberframework.

[20] International Organization for Standardization (ISO). (2022). ISO/IEC 27001: Information security management systems requirements. Retrieved from https://www.iso.org.

[21] Harper, S., & Thorne, L. (2024). Cybersecurity Act 2024: Implications for Malaysian education sector. Journal of Information Security, 8(2), 45–60.

[22] CMMI Institute. (2018). Capability maturity model integration. Software Engineering Institute.

[23] Paulk, M. C., Weber, C. V., Garcia, S. M., Chrissis, M. B. C., & Bush, M. (1993). Key practices of the capability maturity model version 1.1.

[24] Chrissis, M. B., Konrad, M., & Shrum, S. (2011). CMMI for Development: Guidelines for Process Integration and Product Improvement (3rd ed.). Addison-Wesley.

[25] Brown, R. D. (2018). Towards a Qatar cybersecurity capability maturity model with a legislative framework. Qatar University Press, 36. https://doi.org/10.1088/1758-5090/abb063.

[26] Azmi, R., & Kautsarina. (2019). Revisiting cyber definition. In European Conference on Information Warfare and Security, ECCWS, 2019-July (pp. 22–30). https://doi.org/10.4018/978-1-7998-3149-5.ch001.

[27] Garba, A. A., Bade, A. M., Yahuza, M., & Nuhu, Y. (2020). Cybersecurity capability maturity models review and application domain. International Journal of Engineering & Technology, 9(3), 779. https://doi.org/10.14419/ijet.v9i3.30719.

[28] Barclay, C. (2014). Sustainable security advantage in a changing environment: The cybersecurity capability maturity model (CM2). Proceedings of the 2014 ITU Kaleidoscope Academic Conference: Living in a Converged World - Impossible Without Standards?, IEEE, 275–282.

[29] Gourisetti, S. N. G., Mylrea, M., & Patangia, H. (2020). Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis. Future Generation Computer Systems, 105(2), 410–431.

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

[31] Ibrahim, A., Valli, C., McAteer, I., & Chaudhry, J. (2018). A security review of local government using NIST CSF: A case study. Journal of Supercomputing, 74(10), 5171–5186. https://doi.org/10.1007/s11227-018-2479-2.

[32] Christopher, J. D., et al. (2014). Cybersecurity capability maturity model (C2M2). U.S. Department of Energy. Retrieved from https://energy.gov/oe/cybersecurity-critical-energy-infrastructure/cybersecurity-capability-maturity-model-c2m2-program

[33] Curtis, P., Mehravari, N., & Stevens, J. (2015). Cybersecurity capability maturity model for information technology services (C2M2 for IT services), version 1.0.

[34] Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education cybersecurity workforce framework.

[35] Mylrea, M., Gourisetti, S. N. G., & Nicholls, A. (2018). An introduction to buildings cybersecurity framework. In 2017 IEEE Symposium Series on Computational Intelligence, SSCI 2017 - Proceedings (pp. 1–7). IEEE. https://doi.org/10.1109/SSCI.2017.8285228.

[36] Maleh, Y., Sahid, A., & Belaissaoui, M. (2021). A maturity framework for cybersecurity governance in organizations. EDPACS, 63(6), 1–22. https://doi.org/10.1080/07366981.2020.1815354.

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

[38] Zhao, W., & White, G. (2017). An evolution roadmap for community cybersecurity information sharing maturity model. In Proceedings of the Annual Hawaii International Conference on System Sciences (pp. 2369–2378).

[39] Rahim, A., et al. (2022). A Malaysian framework for cybersecurity maturity in public institutions. Journal of Cybersecurity Research, 10, 100–120.

[40] Smith, R., et al. (2022). Customizing cybersecurity frameworks for educational institutions. IEEE Transactions on Security and Privacy, 15(3), 123–138. https://doi.org/10.1109/TSP.2022.303234.

[41] Kumar, A., & Zhao, H. (2020). The role of human factors in cybersecurity maturity models. Journal of Cybersecurity Studies, 9(4), 75–90.

[42] CSM. (2021). Cybersecurity trends and challenges in Malaysian HEIs. Retrieved from https://www.cybersecurity. 35

[43] Creswell, J. W., & Plano Clark, V. L. (2018). Designing and conducting mixed methods research (3rd ed.). Los Angeles, CA: Sage.

[44] Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews. EBSE Technical Report.

[45] Yin, R. K. (2014). Case study research: Design and methods (5th ed.). Thousand Oaks, CA: Sage.

[46] ATLAS.ti. (2023). Qualitative data analysis software. Retrieved from https://atlasti.com

[47] Saunders, M., Lewis, P., & Thornhill, A. (2015). Research methods for business students(7th ed.). Harlow, UK: Pearson.

[48] Lochmiller, C. R. (2021). Conducting thematic analysis with qualitative data. Qualitative Report, 26(6), 2029–2044. https://doi.org/10.46743/2160-3715/2021.5008

[49] Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2014). Multivariate data analysis (7th ed.). Upper Saddle River, NJ: Prentice Hall.

[50] Saaty, T. L. (1980). The analytic hierarchy process: Planning, priority setting, resource allocation. New York: McGraw-Hill