Jurnal Pengurusan 67 (2023) 31 – 41
https://doi.org/10.17576/pengurusan-2023-67-03

The Role of Cybersecurity on the Performance of Malaysian Higher Education Institutions

(Peranan Keselamatan Siber terhadap Prestasi Institusi Pengajian Tinggi Malaysia)

Balla Moussa Dioubate
Wan Daud Wan Norhayate
Zainol Fakhrul Anwar
Salleh Fauzilah
(Faculty of Business and Management, Universiti Sultan Zainal Abidin)
Hilmi Mohd Faiz
(Pusat Pengajian Pendidikan Jarak Jauh, Universiti Sains Malaysia)
Lee Ooi Hai
(Edustats Solutions)

ABSTRACT

Cybersecurity, as a security management requirement, is essential to understanding data security in higher institutions. This study aims to explore the role of cybersecurity in the performance of Malaysian higher education institutions through semi-structured qualitative interviews with 10 cybersecurity risk management officers from 10 public universities. The data were analysed using thematic analysis to identify the themes and sub-themes that revealed the strengths and deficiencies of the current cybersecurity frameworks. Results showed that cybersecurity implementation is considered a successful innovation in Malaysian universities and has contributed to protecting the data of students and staff, which in turn allowed the universities to improve their reputation. This study contributed significantly to the understanding of the performance and applicability of cybersecurity in universities. It showed the efficient use of resources, identification and detection of risk exposures, and improved cybersecurity communication between the technical team and top management are essential for a good decision-making process.

Keywords: Cybersecurity; risk management; Higher Institution of Education

ABSTRAK

Keselamatan siber, sebagai keperluan pengurusan keselamatan, adalah penting dalam memahami keselamatan data di institusi pengajian tinggi. Kajian ini menilai peranan keselamatan siber terhadap prestasi institusi pengajian tinggi Malaysia melalui temu bual kualitatif separa berstruktur dengan 10 orang pegawai pengurusan risiko keselamatan siber dari 10 buah universiti awam. Data dianalisis menggunakan analisis tematik untuk mengenal pasti tema dan subtema yang mendedahkan kekuatan dan kekurangan rangka kerja keselamatan siber semasa. Keputusan menunjukkan bahawa melaksanakan keselamatan siber dianggap sebagai satu inovasi yang berjaya di universiti Malaysia dan telah menyumbang kepada melindungi data pelajar dan kakitangan, yang membolehkan universiti meningkatkan reputasi mereka. Kajian ini menyumbang secara signifikan kepada pemahaman tentang prestasi dan kebolehgunaan keselamatan siber di universiti. Ia menunjukkan penggunaan sumber yang cekap, pengenalpastian dan pengesanan pendedahan risiko, dan komunikasi keselamatan siber yang lebih baik antara pasukan teknikal dan pengurusan atasan adalah penting untuk proses membuat keputusan yang baik.

Kata kunci: Keselamatan siber; pengurusan risiko; Institusi Pengajian Tinggi

Received 09 September 2021; Accepted 23 February 2023

INTRODUCTION

With the inevitable changes that accompany the industrial era's transformation, the emergence of new risks that could harm many aspects of businesses, including higher education institutions, has become highly likely. Modern universities use cyberspace to fulfil legislative requirements and deliver services to faculty, students, parents and guardians, funding agencies, governments, accrediting organisations, and other stakeholders. Despite the benefits of cyberspaces, they also represent considerable dangers and problems to universities' well-being and operations. It is related to the recent growth and expansion of cybercrime (Badamasi & Utulu 2021). However, computer attacks are not limited to significant businesses or organisations, and educational institutions are becoming more conscious of the cyber threats to which their information assets are vulnerable. Because of the sensitive data they collect, universities are susceptible to cyber-attack. It leads to a preliminary evaluation of possible risks in educational project execution, which has a detrimental impact on the financial performance of

a single educational organisation and the whole growth of the academic sector (Suray et al. 2019). Cybersecurity attacks are a critical issue for higher education institutions because these attacks jeopardise student data and harm the integrity and reputation that institutions have meticulously built over time. However, asset and cyber vulnerability assessments help to strengthen institutional cybersecurity efforts. It favours prioritising critical protection methods (Cheng & Wang 2022). According to Boranbayev et al. (2015), the loss or dissemination of sensitive information in higher education institutions and research centres has resulted in property damage, financial loss, reputational harm to the university, inability to pay, and ultimately, loss of profits.

Universities are especially vulnerable because they manage information on scientific and technological breakthroughs, personal information about their employees and students, academic records, and other related matters (Dioubate & Daud 2022; Tixteco et al. 2017). For instance, the University of San Francisco has made significant investments in cybersecurity over the past three years to protect against the illicit movement of funds away from the university and the data theft of students, parents, faculty, and alumni, as well as to improve operational process development (Grajek 2020). Universities in the United Kingdom possess vital intellectual property for research and supplementary academic materials, making them attractive hacking targets. Universities face cybersecurity threats that might disrupt the operation of a university website and may take the form of a targeted attempt to obtain sensitive information from websites and their users (Walker 2020; Bandara 2014). According to Lane (2007), the cybersecurity environment in Australian organisations is complicated and prone to obscurity. As a result, a solid foundation is required to adopt cybersecurity practices in higher education institutions successfully. Cybersecurity must be emphasised, and protecting the company and academia is a challenging balancing act.

Several Australian higher education institutions are waiting to talk about improving their data security management. According to Kang et al. (2015), most Malaysian higher education institutions must incorporate ethical hacking into their security development life cycles. The exponential growth of information technology has provided hackers with better tools, increasing difficult in ensuring cybersecurity. Methods and techniques of ethical hacking can help reduce security concerns. Officials at higher education institutions have been unable to protect their data from adversarial hackers because of a deficiency in penetration assessment skills.

This study aims to explore the role of cybersecurity on the performance of higher education institutions in Malaysia and evaluate the strengths and weaknesses of the current cybersecurity methods utilised in Malaysian public universities. Most Malaysian public universities employ the International Standard ISO/IEC 27001: 2013 as its ISMS specification. Some additional frameworks are also used in higher education institutions, such as Hazard Identification and Risk Assessment (HIRA), ISO/IEC 27000 related to Information Security Management, Key Risk Indicators (KRI), Malaysian Public Sector Information Security Risk Assessment System (MyRAM), Quality Management System (ISO 9001:2015), Malaysian Standard (MS ISO 31000:2018), Enterprise risk management framework, ISO/IEC 27005:2018, and the Standard and Industrial Organization for Risk Management (SIRIM). Thus, this research detailed the importance of cybersecurity in risk control and protecting organisational information in the current security threat landscape of higher education institutions. The results of this research are highly valuable for the educational system because it showed that controlled effective cybersecurity contributed to forming decision-making.

Cybersecurity management is a continuous process that allows for the identification, analysis, evaluation and treatment of cybersecurity risks. Establishing the cybersecurity management process moves from an organisational level to one that considers risk in the light of the higher education institutions' overall management and mission. The review showed that universities using the ISO/IEC 27001 standards for cybersecurity management practically contributed to controlling cybersecurity risks. Implementing the standard increased the likelihood of universities controlling the cybersecurity risk to protect their reputations. Organisational performance of higher education institutions improved after the implementation of cybersecurity management practices. Cybersecurity risk management practices are linked to specific measures and affect university's performance.

However, looking at risk-related university performance measures involves exploring its financial and non-financial performance to determine how well the university is doing. Financial performance includes making money, spending on operating costs every year, affecting cash flow, being accountable, and obtaining research grants from outside the country or the world. Non-financial measures include global ranking, reputation, academic performance, good governance, talent management, university human resource successor readiness and the effect of risks on business continuity. In addition, securing physical and digital data enhances the security of the university's information system. System information security is essential to the university's reputation.

Information system security contributed to the practical protection of the university's data communication process in relation to confidentiality, integrity and availability. A secure information system may improve the management of the examination process, student and staff data, and the commercial performance of the institution. Cybersecurity can be implemented well by integrating it into business strategies and decision-making processes at universities to keep risks within

acceptable limits and make it easier for universities to take advantage of opportunities.

The rest of the paper is divided as follows. The first part is a detailed review of previous studies, and the second part expounds on the methods used to collect and analyse data. The study's results are summarised in the third part and are discussed in the fourth part. The final section concludes the study, including recommendations for future research.

LITERATURE REVIEW

CYBERSECURITY

Cybersecurity risks are associated with the probability of threats that exploit an organisation's assets or its subset (Chee & Sin 2020). In recent years, information systems have become more susceptible to unintended operator errors and natural and artificial disasters because of computer connectivity and the ease with which many people can access cybersecurity systems (Boltz 1999; Talet et al. 2014). Accepting risks and associated assets without protection or control, avoiding risks through risk-mitigation strategies and transferring risks to third parties are all viable risk-control strategies. Control implementation is founded on management practices that are optimally linked to resources and the strength of security solutions based on the business' commercial activities. Professionals, legislators and decision-makers are becoming increasingly concerned with cybersecurity. It is crucial for a society to defend itself against cyber threats through preventative and reactive measures requiring ongoing surveillance while protecting individual liberty and avoiding mass surveillance (Fadzline 2020). Computer security, also known as cybersecurity or IT security, safeguards computer systems against hardware, software, or data damage and service interruption or misdirection (Roca 2019). It increases return on investment and business opportunities for long-term growth while decreasing firm risks and knowledge security from various threats (Sheikhpour & Modiri 2012). In contrast, the absence of comprehensive cybersecurity regulations results in security breaches and attacks on the organisation's records. Therefore, the primary objectives of ensuring cybersecurity implementation are to prevent and minimise asset loss, maintain data security and enhance cybersecurity management (Hashim & Razali 2019).

CYBERSECURITY MANAGEMENT

Cybersecurity is necessary for security management and understanding an organisation's total security profile is vital (Talet et al. 2014; Webb et al. 2014). Cybersecurity management has been included in many commercial and government organisations worldwide (Zachman 2014). Comprehensive cybersecurity management, including monitoring systems, is required for a robust information technology security setup (Talet et al. 2014). Clinch (2009) reported that the International Standards ISO/IEC 27001 and ISO/IEC 27002 were used to develop a cybersecurity management system. Cybersecurity management is commonly used to reduce uncertainty and its repercussions, which increase the likelihood of organisational success (Talet et al. 2014). Security management is defined as the architecture (principles, structure, and technique) of successful risk management by the Standards Association of British and New Zealand (Standard & Standard 2009). It is a managerial need and a component of organisational systems that involve critical checking and management procedures. Furthermore, according to the international standards organisation ISO/IEC (2011), integrated cybersecurity management initiatives tend to minimise and control corporate risks.

According to Hashim and Razali (2019), a cybersecurity management strategy assists many firms in efficiently minimising business risks. The cybersecurity management method attempts to integrate IT security with business performance to ensure efficiency in the operational management of university digital platforms used for teaching, learning, research, community development and administration (Taylor 2006; Taylor 2017). As part of contemporary governance settings, higher education institutions must implement a corporate strategy for managing cybersecurity, including a process model for security systems and developing a security management model for e-learning systems (Bandara et al. 2014). However, a good cybersecurity technology necessitates operational management methods that enable an effective e-business environment (Boltz 1999; Talet et al. 2014). Finally, a comprehensive security programme at higher education institutions emphasising risk reduction may minimise exposure. As a result, in recent decades, cybersecurity management has developed into a critical component of enterprise management (Whitehead 2020). It comprises threat management and control methods, hazard preparation, appraisal, interpretation and reactions (Purohit et al. 2018).

CYBERSECURITY IN UNIVERSITIES

Shoki et al. (2014) mentioned that the structure for cybersecurity management techniques and organisational performance in Malaysian public universities have yet to be developed. The current and conventional cybersecurity management strategy is inadequate and lacks a structured management approach because it focuses primarily on the standards outlined in the University Good Governance Index (UGGI). The importance of setting the risk parameter, understanding major risk exposures and considering risk factors in all decisions is emphasised in the UGGI. However, the cybersecurity management methods and technologies used in the process and the risk management approach should be

adequately discussed. Cybersecurity approaches such as the Risk Management - Principles and Guidelines (MS ISO 31000:2020) and the Committee of Sponsoring Organisations (COSO) are common and primarily used to assist businesses. As a result, most of the literature on cybersecurity in higher education institutions focuses on cybersecurity management and other proposed security frameworks (Ulven & Wangen 2021).

Cybersecurity frameworks provide a reference point for organisations to understand current cybercrime patterns and the best ways to combat them. It also justifies assessing cybersecurity initiatives' efficacy, dependability and integrity (Badamasi & Utulu 2021). The role of cybersecurity in Malaysian universities is linked to knowledge production, strength, value enhancement and reputation protection. It ensures the universities' long-term viability and credibility. As a result, cybersecurity educates students, faculty, staff and partner companies with whom the university works on best practices in security management. It also outlines what is expected of university partners in relation to cybersecurity. Implementing cybersecurity was a successful innovation in Malaysian higher education institutions. It has contributed by increasing security and reducing cyberattacks that harm universities' reputations and economic profits; for example, participating in regulations that require all systems under their control to adhere to high-security standards (Ekpoh et al. 2020). However, to help universities become competitive higher education institutions in the global education market, management must increase awareness and investigate a new paradigm for imposing cybersecurity in these universities (Shoki et al. 2014).

POLICY IMPLEMENTATION THEORY

Public policy implementation was one of the earliest issues discussed by policy experts. The primary step in the public policy process is the implementation stage. Policy implementation, a critical task in the bureaucracy, is not a standardised method but rather depends on the form of policy, with each form having a different degree of implementation difficulty (DeLeon & DeLeon 2002). According to Mazmanian and Sabatier (1983), implementing a fundamental policy decision, generally through legislation, may also take the form of critical presidential directives or judicial judgements. This selection should ideally describe the problem(s) to be solved, the goal(s) to be pursued and the various implementation processes. Typically, the process begins with the passage of the primary statute, continues with policy outputs (decisions) from implementing agencies, target group compliance with those decisions, the actual effects of agency decisions and concludes with substantial revisions (or attempts at revisions) to the primary statute (Mazmanian & Sabatier 1983). There are three theories regarding policy implementation: top-down, bottom-up and hybrid. This study examines theories related to existing cybersecurity management frameworks to develop cybersecurity management skills at public universities in Malaysia. As the most reliable predictor, the policy implementation hypothesis is strongly associated with the application of new government directives to public institutions in Malaysia. However, the hybrid strategy might result in a favourable adoption by a university and concerned personnel while conforming to Malaysian government standards.

METHODOLOGY

This study employed qualitative methodology to connect an understanding of social aspects of life. It primarily produces words, rather than numerical data, that researchers can use for further analysis (Bricki & Green 2007; Moriarty 2011; Dioubate et al. 2015). Qualitative analysts use discourse to gather information from participants, allowing them to respond as needed and comprehend the phenomena under investigation (Cronin 2014; Dasgupta 2015). Thematic exploration, data collection by observation, interview and other qualitative data collection techniques ware all part of the qualitative research analysis (Daud et al. 2016; Yin 2014). This study aims to explore the role of cybersecurity in the performance of Malaysian higher education institutions. Data were gathered through interviews with professionals in cybersecurity risk management. Participants were drawn from a group of personnel involved in cybersecurity risk management from twenty (20) public higher education institutions in Malaysia. Representatives from public universities who took part in this study were drawn from the university's cybersecurity risk management departments, particularly the strategic planning and risk management department. Data saturation, according to Kongnso (2015), is a point in qualitative research where information collection does not abdicate new data. Thus, no unused data in relation to the research subject emerged after interviewing representatives from a sample of ten Malaysian public universities. As a result, a sample of ten Malaysian higher education institutions was sufficient for this research.

Yin (2009) divided the case study's architecture into four distinct forms based on a 2 x 2 matrix, indicating a four-fold typology. First, the matrix demonstrates that any type of design would require the evaluation of contextual conditions in response to an event. The dotted lines indicate that the border between the case and the background is unlikely to be sharp. The four case study designs that resulted are as follows: (Type 1) single-case designs - holistic designs, (Type 2) single-case designs - embedded designs, (Type 3) multiple-case designs - holistic designs and (Type 4) multiple-case designs - embedded designs. Furthermore, Yin (2009) stated that case studies could be holistic or contain embedded analysis units. This research is the theoretical result of four distinct case study designs, which are depicted in Figure 1.

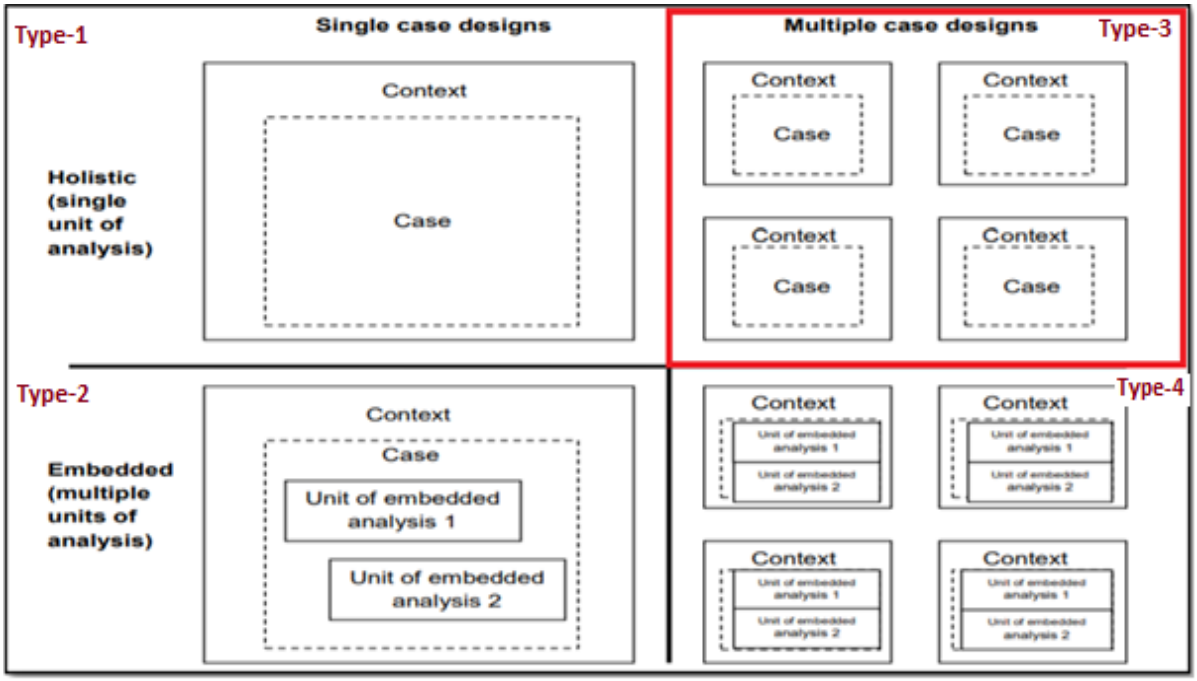

FIGURE 1. Basic designs for case studies

Source: (Yin 2009)

In this paper, a qualitative case study was used. The design chosen was the holistic (single unit of analysis) - multiple case design, as shown in the matrix's upper right quadrant. The researchers selected the holistic multiple case study designs because numerous data sources were used to investigate the accepted procedures. More than one case is included in the same study based on the matrix. Furthermore, each study in the 10 institutions was assigned one case study. Following Herriott and Firestone (1983), the current data revealed that multiple cases are perceived to be more stable. As a result, the researchers used purposive sampling to identify volunteers from the study population who had been educated on the subject. For a qualitative study, the sampling technique worked well, especially when selecting participants based on unique circumstances. Selecting cases is based on the expert's discretion or the researcher's case selection with a specific goal in mind (Ishak & Bakar 2014). To submit responses during the interview sessions, the selected participants must have a thorough understanding of cybersecurity risk management.

Doody and Noonan (2013) suggested using an interview guide before beginning data collection. In this study, one participant who was a cybersecurity risk management expert from a public institution examined the interview protocols, allowing for an assessment of the interview protocols as follows. The participant verified the permission form and the interview questions. The protocol's suggested interview questions were left open-ended, and participants' views and insights on cybersecurity management at their institutions were canvassed during the session. Following an analysis of the interview procedure, various protocol adjustments were made, and the researcher gathered data qualitatively using the validated interview questions.

The data collected, in the form of audio-recorded interviews, were transcribed verbatim and coded to identify the themes and subthemes. Then, the NVivo 12 coding software was used to facilitate data analysis (Laurence et al. 2010; Molok et al. 2013). This study used the interview responses to generate themes and subthemes before the transcription process. The themes and subthemes (nodes) were derived from the interview transcripts. However, the code was distributed sequentially to each participant, beginning with P (1) for the first participant and ending with P (10) for the last participant.

The second step was a thorough thematic analysis of the themes derived from the code. It allowed for the elimination and grouping of some themes to produce a final set of two themes. The references were broken down into five distinct nodes (Sub-themes). The discovered themes allowed us to achieve the purpose of this study, which is to explore the role of cybersecurity on the performance of Malaysian higher education institutions.

RESULTS

The findings are based on interviews with 10 participants who took part in-depth and face-to-face interviews with cybersecurity officers from 10 Malaysian public

universities. The first theme was the cybersecurity role in universities, which was divided into 3 sub-themes: process evaluation, university performance and university value. The second theme was the security of the university's information system, and was constituted by 2 sub-themes: physical and digital security and security of the procedure. This section summarises the interview outcomes from the samples shown in Table 1.

TABLE 1. Research question, themes, sub-themes, and summary of results

Research Question during the interview session	Themes	Sub-Themes	Summary of Results
What is the role of cybersecurity in promoting Malaysian higher education institutions' performance?	Cybersecurity role in universities	Process Evaluation	The framework was successfully implemented.
		University Performance	The framework's success is connected to knowledge development, operational strength and value increase, all of which safeguard the institution's reputation.
		University Value	The framework's effectiveness added value and credibility to the institution. Contributed to better security and decreased cyberattacks, which harmed institutions' reputations and economic profits.
	Security of Information system	Security of Physical and Digital Data	It was established to safeguard information and train technical personnel to protect digital, physical and sensitive data. The policy for accessing and controlling the data centre was created to protect essential information for the school's reputation. It ensures that the examination procedure and student and staff statistics directly contribute to the schools' commercial performance.
		Security of the Procedure	

CYBERSECURITY ROLE IN UNIVERSITIES

The function of cybersecurity at the institution was rigorously examined to establish the process contribution in terms of performance and value. In this part, we explored the following sub-themes: process evaluation, university performance and university value.

Process Evaluation: According to the participants, public universities in Malaysia employ cybersecurity as part of their Information Security Management System (ISMS) to simplify institutional tasks. Examining the existing cybersecurity system allowed us to determine the effects of the current frameworks on university performance. The following interview statements incorporate aspects of process evaluation:

"The cybersecurity framework's installation aided the ISMS. The university has advanced to the level of a developed institution, with success elements in the operational process." P (3)

"...Evaluation and measurement of their cybersecurity efficacy." Sometimes you look at things from both quantitative and qualitative perspectives. P (6)

"I identify or assess effectiveness by the number of phone calls I got requesting or seeking assistance in preparing the (Cybersecurity procedure) risk register. "I believe the framework's efficacy is increasing in tandem with the number of phone calls I receive." P (7)

The implementation of cybersecurity was a successful invention. It has helped to increase data security and reduce the number of cyberattacks that damage institutions' brands and profitability. According to Ismail et al. (2010), the university security process evaluation highlighted the company's successful cybersecurity management and assisted the organisation in meeting its objectives. The response from participants underlined the importance of establishing cybersecurity at the institution as proof of its effectiveness. This result has contributed to an increase in new international student enrolment, which has helped to alleviate the school's financial flow. Malaysia's public autonomous universities hope to positively impact cybersecurity practises by engaging in risk management activities such as strategy, cybersecurity management systems, resources and technology, and quality improvement (Shoki et al. 2014).

In general, research participants viewed the implementation of cybersecurity management was one of the most significant advances in Malaysian higher education institutions. They also requested a distinct section for physical security in cybersecurity to safeguard the institution's data centre and equipment.

University Performance: The framework supports the university's operational process regarding knowledge base generation, which improves academic achievement and profit. As a result, it enabled the institution to increase its performance, integrity and reputation. The following excerpt contains information on the university's performance:

"It will be better and so on...; therefore, this institution's business performance will be favourable." P (4)

"So, this is where a framework... may help raise information integrity and improve reputation. However, reputation is also important." P (9)

"So, for me, performing implies sustaining...not just in terms of performance, but also in terms of preserving greater value, because the university is not a production base." P (6)

In this scenario, cybersecurity management guarantees that institutions stay viable and reliable. It also improves the university's knowledge development, operational strength, value enhancement and institutional reputation protection. Consequently, the framework conforms to safety risk management in building a learning environment that recognises and analyses emerging security risks in the university's computer sector (Joshi & Singh 2017).

According to the study's participants, data security has been strengthened since implementing the ISO/IEC 27001 standard, as directed by the Malaysian Administrative Modernization and Management Planning Unit (MAMPU). It has contributed to a reduction in cyberattacks that used to destroy the university's reputation and profit. Furthermore, Ismail et al. (2010) discovered that good cybersecurity could boost organisational efficiency. It also contributes to the achievement of an organisation's goals. While organisations implementing comprehensive cybersecurity have shown to be successful, those not participating have needed to be more effective in obtaining the same benefits. As a result, cybersecurity management leads to verified goal attainment and performance improvement (MS ISO 31000:2020).

Nonetheless, the design of the interview questions employed in this study enabled us to comprehend the performance of Malaysian public institutions following the implementation of cybersecurity management.

University Value: The Malaysian government's cybersecurity management system helped increase the value of university operations and management systems to sustain the institutions' viability. The following citation has elements associated with university values:

"By using this procedure, we will be able to learn more about information system risk from experienced and qualified professionals in this field." P (4)

"We argue that our campus cybersecurity management is "in the same" area where we are rescued; that is the value for the university portion of the success aspect." P (3)

"I believe the key value is sustainability; as I previously stated, your risk does not have a supportive atmosphere. So everything comes down to sustainability." P (6)

"It provides good value for our institution since IT is heavy on data protection; consumers believe that they have safeguarded all of the information submitted to us. Its usefulness can boost people's faith in our organisation." P (7)

These studies demonstrated an increase in university effectiveness and trust. Thus, the deployment of the framework has aided the university's commercial process by boosting the number of students and overall income. However, because universities are educational institutions, one of the most crucial activities is exams, which need high levels of secrecy, honesty, and availability. Cybersecurity at the university safeguards the examination process and student and staff data, directly contributing to the institutions' financial performance. As a result, including the frameworks in the operating system affected the rise of new foreign student arrivals, eventually altering university ranking scores.

SECURITY OF INFORMATION SYSTEM

This theme evaluated the security of information systems in the university to discover the level of security of physical and digital data. The subsequent sub-themes, such as physical and digital security and security of the procedure, were debated in this section.

Security of Physical and Digital Data

Participants emphasised the need to integrate cybersecurity management into a secure information system. Because of this cybersecurity, the university could maintain its integrity and reputation. The university's business process requires protecting sensitive data regarding confidentiality, integrity, and availability. The following quotations discuss aspects of university cybersecurity:

"We need a larger example, such as physical security, because some of the risks are related to physical security... must ensure the physical security of all of these (digital and physical information), you know what we mean." P (3)\

"When we encounter problems such as fraud or (before) when they assault our server. Nonetheless, PPKT has done an excellent job in providing a very secure server to protect information." P (1)

"This is the most important reason we need to consider adopting cybersecurity because we want everybody, not only students but also employees, to have great trust in how we safeguard information." P (3)

"From the standpoint of cybersecurity defence, information integrity is vital in presenting the image and reputation of the organisation." P (9)

"Cybersecurity is highly technical knowledge, and finding the proper individual to look at this cybersecurity risk in institutions is critical." P (6)

Cybersecurity is more beneficial for higher education institutions particularly in relation to confidentiality, integrity and availability. Cybersecurity measures are implemented to safeguard digital, physical and paper-based data. As a result, information security components such as security policy, cybersecurity agency and asset management are included in international standards (ISO/IEC 27001). Participants demonstrated that the administration's approach to information protection boosted data security and contributed to the university's favourable standing.

SECURITY OF THE PROCEDURE

Implementing a cybersecurity system safeguards university data and personal information of students and employees from manufactured and natural catastrophes and breaches. Protecting higher education institutions' information has enabled universities to further trust in their operations management. The following statements quoted from the interviews provide information on the factors associated with the university data process:

"So, from data centre management, we analyse the present condition risk for our data centre. We perform the analysis. Then we compare the cybersecurity claims..." P (2)

"The first is university (A3) personnel; they must carry their staff ID... We have IT renderings prepared with configuration for outsiders because we have 200 data servers in the data centre." P (3)

"As a result, we must describe the confidentiality of the information, the availability of the data, and any assets that assist the protection... We limited the scope of one of the most important procedures in academic activity. Which were the high risks of information confidentiality, integrity, and availability, particularly regarding examinations and assessments, for example." P (9)

Cybersecurity at the university secures the examination process and student and staff data and directly contributes to the institution's performance. Furthermore, the respondents claimed that cybersecurity management ensures data security in terms of confidentiality, availability, and integrity. It also underscored the need for a well-prepared technical staff to protect digital and physical materials. Technical employees must be trained in cybersecurity to protect any data. Thus, some colleges create protocols for gaining access to the data centre, which is very important because it is difficult to repair once damaged.

DISCUSSION

Participants from all ten universities participating in this survey agreed that integrating cybersecurity was a successful innovation in Malaysian higher education institutions. Because universities are educational institutions, one of the most crucial activities is an examination, which necessitates high data security regarding confidentiality, integrity, and availability. Cybersecurity at the universities protects the examination process and student and staff data and contributes directly to the institution's business performance. Internal and external understandings caused differences in their perspectives of the institution's ideals and issues. It might provide new data that the management had not previously considered (Suray et al. 2019).

The participants demonstrated that safeguarding cybersecurity data through policy development led to the university's excellent standing. Securing the universities' operating procedure enhanced the entry of overseas students, increasing higher education institutions' income. Cybersecurity is projected to have a positive and critical impact on risk management methods in Malaysia's public universities (Shoki et al. 2014). It has also added value to the institution's performance, reputation, and business process. Joshi & Singh (2017) found that by using cybersecurity management, the most important exposures can be proactively targeted, and resources can be used effectively to achieve optimal results.

The outcome of the interviews showed that implementing cybersecurity in the university facilitated performance in terms of knowledge production, strength, values, and the protection of the institution's reputation. The performance and growth of cybersecurity in educational institutions depend directly on senior management (Khizhnyak 2017). However, participants in this study found that the performance of cybersecurity implementation was linked directly to the outcome of the university in terms of knowledge production. Thus, the participants demonstrated that cybersecurity safeguarded data and contributed to the university's good ranking. The cybersecurity policy defined data confidentiality, integrity, and availability safeguards.

THEORETICAL IMPLICATION

The participants agreed that handling cybersecurity in public colleges is a significant problem. The MAMPU directed the implementation of the ISO/IEC 27001 framework. Using the framework's norms and principles provided better knowledge of cybersecurity management. This research supports the use of policy implementation theory as the most consistent predictor for adopting the Malaysian government's new instructions offered to public universities.

The study produced significant theoretical contribution by employing public policy theory and its offspring, policy implementation theory. It also provided a fresh viewpoint by employing policy implementation theory, which positively influenced vital findings, such as academic performance, educational value, income, university reputation, and physical and digital data security. However, the study found that utilising a hybrid technique, policy implementation theory, matched the acceptance of MAMPU's instruction to apply ISO 27001 in higher education institutions. This hybrid policy might be adopted favourably by a university and related employees. Furthermore, higher education institutions have reaped benefits and controls in establishing a cybersecurity channel in the education sector.

PRACTICAL IMPLICATION

Cybersecurity was implemented by incorporating it into the universities' business strategy and decision-making processes. Cybersecurity reduced risk to acceptable levels and boosted the universities' ability to capitalise on opportunities. In the current security threat landscape, this study logically presented the current strategy used by higher education institutions to control cybersecurity risks and safeguard organisational information. The study revealed that using the universities' current framework to improve their commercial performance benefited the educational system by enhancing data security. The research linked the study's findings, establishing ties between the concepts and themes shown.

CONCLUSIONS AND FUTURE DIRECTION

The detection and prosecution of cyberattacks within the cyberspaces used by universities to carry out their statutory duties have become more complex. This complexity is accompanied by the increased cybersecurity challenges in academic institutions, emphasising the importance of implementing recommended cybersecurity management. One of the challenges for higher education institutions is the successful implementation of a cybersecurity strategy based on risk assessments while conforming to the company's demands. When security breaches or violations occur at universities, it has been observed that regulations are less likely to be followed because security policy papers need to be more robust and precise. Meanwhile, the university board directory wants more international students to attend the school to earn funds. It would only be possible if the institutions have a proven track record of data preservation in terms of confidentiality, integrity, and accessibility. Finally, this study aims to determine the role and impact of cybersecurity on the performance of Malaysian higher education institutions. As a result of implementing such programmes, the institutional practice of incorporating cybersecurity management into university culture and business operations increases. According to the participants, the Malaysian government, through the MAMPU, advocated incorporating cybersecurity management as part of ISMS in public universities, which can include the application of the ISO/IEC 27001 standard. According to the findings of this study, deploying cybersecurity has helped boost data security and lower cyberattacks that harm institutions' reputations and economic profits. The effectiveness of the existing processes adds quantitative and qualitative value and credibility to the university. Cybersecurity performance is connected to the university's physical and digital data security. Although Malaysian public universities implemented cybersecurity management, the findings indicated that top management should consciously address concerns connected to university performance by using internal and external assessment methodologies for cybersecurity. The conclusions of the study have theoretical and practical relevance.

This work added to the theory by employing the policy implementation theory derivative of public policy and yielded intriguing results. The study's findings will have a substantial effect on the university's operating process by revealing new views. The practical contribution of the results will serve as a tipping point for the administration of higher education institutions. It used the essential information for targeted strategies to improve Malaysian public universities' socioeconomic development and vitality. However, the research was limited to case studies of universities from public institutions. As a result, the study could not identify whether institutions not included in the study might obtain the same outcomes.

Furthermore, this study gathered information from university workers who may be on rotation. In the future, this research will consider the recommendations given by participants to establish an updated cybersecurity management approach. The quantitative research approach can also be used to analyse the extent of the outcomes from this study.

ACKNOWLEDGEMENTS

The authors would like to thank the Ministry of Education Malaysia for funding this research under the FRGS research grant. Furthermore, the authors would like to express their profound appreciation to the Centre for Research and Innovation Management (CRIM) UniSZA, which helped them in the research administration.

REFERENCES

Abdul Molok, N.N., Chang, S. & Ahmad, A. 2013. Disclosure of organizational information on social media: Perspectives from Security Managers. In *Pacific Asia Conference on Information Systems 2013*, 1-12.

Badamasi, B. & Utulu, S.C.A. 2021. Framework for managing cybercrime risks in Nigerian Universities. arXiv preprint arXiv:2108.09754.

Bandara, I., Ioras, F. & Maher, K. 2014. Cyber Security Concerns in E-Learning Education Proceedings of ICERI2014 Conference, (November), 728–734.

Boltz, J. 1999. *Informational Security Risk Assessment: Practices of Leading Organizations*. DIANE Publishing.

Boranbayev, A., Mazhitov, M., & Kakhanov, Z. 2015. Implementation of security systems for prevention of loss of information at organizations of higher education. *2015 12th International Conference on Information Technology - New Generations*, (It), 802–804.

Brikci, N. & Green, J. 2007. *A Guide to Using Qualitative Research Methodology.* London, Health Services Research Unit: London School of Hygiene and Tropical Medicine.

Chee, L.C. & Sin, T.S. 2020. The significance of personal value, risk attitude, and trust in life insurance ownership in the northern regions of Malaysia. *Jurnal Pengurusan* 58: 67–78.

Cheng, E.C. & Wang, T. 2022. Institutional strategies for cybersecurity in higher education institutions. *Information* 13(4): 192.

Clinch, J. 2009. *ITIL V3 and Information Security. Best Management Practice*.

Cronin, C. 2014. Using case study research as a rigorous form of inquiry. *Nurse Researcher* 21(5): 19-27.

Daud, W.N.B.W., Zainol, F.A., Salleh, F., Yazid, A.S. & Jamal, A.Z. 2016. Developing microtakaful flood model in Malaysia-its relevance and policy impacts. *International Journal of Business Continuity and Risk Management* 6(3): 197-208.

Dasgupta, M. 2015. Exploring the relevance of case study research. *Vision: The Journal of Business Perspective* 19: 147-160.

deLeon, P. & deLeon, L. 2002. Whatever happened to policy implementation: An alternative approach. *Journal of Public Administration Research and Theory* 12(4): 467-492.

Dioubate, B.M. & Daud, W.N. 2022. A Review of cybersecurity risk management framework in Malaysia Higher Education Institutions. *International Journal of Academic Research in Business and Social Sciences* 12(5): 1031–1093.

Doody, B.M., Molok, N.N.A., Talib, S. & Tap, AOM 2015. Risk assessment model for organisational information security. *ARPN Journal of Engineering and Applied Sciences* 10(23): 17607-17613.

Doody, O. & Noonan, M. 2013. Preparing and conducting interviews to collect data. *Nurse researcher* 20(5).

Ekpoh, U.I., Edet, A.O. & Ukpong, N.N. 2020. Security challenges in universities: Implications for safe school environment. *Journal of Educational and Social Research* 10(6): 112-112.

Fadzline, P. 2020. The challenges and solutions of cybersecurity in Malaysian Companies. In *Research Anthology on Business Aspects of Cybersec.* April.

Grajek, S. 2020. TOP 10 IT ISSUES 2020: The drive to digital transformation begins. *EDUCAUSE Review*, 4.

Hashim, R. & Razali, R. 2019. Contributing Factors for successful information security management implementation: A Conceptual Model. *International Journal of Innovative Technology and Exploring* 9(2): 4491-4499.

Herriott, R.E. & Firestone, W.A. 1983. Multisite qualitative policy research: Optimising description and generalizability. *Educational Researcher* 12(2): 14-19.

Ishak, N.M. & Bakar, A.Y.A. 2014. Developing sampling frame for case study: Challenges and conditions. *World Journal of Education* 4(3): 29-35.

Ismail, Z., Masrom, M., Sidek, Z. & Hamzah, D. 2010. Framework to manage information security for Malaysian academic environment. *Journal of Information Assurance & Cybersecurity* 2010: 1–16.

Standard, B. & Standard, N.Z. 2009. Risk management-principles and guidelines. BS ISO, 31000, 2009.

ISO/IEC. 2011. Information technology security techniques information security risk management. Retrieved from http://nsa.wkall.se/litteratur /iso_iec_27005-2011.pdf

Joshi, C. & Singh, U.K. 2017. Information security risks management framework – A step towards mitigating security risks in the university network. *Journal of Information Security and Applications* 35: 128–137.

Kang, C.M., Josephng, P.S. & Issa, K. 2015. A study on integrating penetration testing into the information security framework for Malaysian higher education institutions. *2015 International Symposium on Mathematical Sciences and Computing Research, ISMSC 2015*.

Khizhnyak, D.A., Shushpanova K.D. 2017. Organisation of the risk management system at the enterprise. *New Science: Financial and Economic Foundations* 1: 273–275.

Kongnso, F.J. 2015. Best practices to minimise data security breaches for increased business performance (Doctoral dissertation). Available from ProQuest Dissertations & Theses Global (UMI No. 3739769).

Lane, T. 2007. *Information Security Management in Australian Universities - An Exploratory Analysis*. (January), 269.

Laurence, C.O., Williamson, V., Sumner, K.E., Fleming, J. & others. 2010. Latte rural": The tangible and intangible factors important in recent GP graduates' choice of rural practice. *Rural Remote Health* 10(2): 1316.

Mazmanian, D.A. & Sabatier, P.A. 1983. *Implementation and Public Policy.* Glenville, IL: Scott Foresman.

Moriarty, J. 2011. *Qualitative Methods Overview. Methods review, 1*. London: NIHR School for Social Care Research.

MS ISO 31000:2010, Risk management – Principle and Guideline, Department of Standard Malaysia.

Purohit, D.P., Siddiqui, N., Nandan, A. & Yadav, B.P. 2018. Hazard identification and risk assessment in the construction industry. *International Journal of Applied Engineering Research* 13(10): 7639-7667.

R. Sheikhpour & N. Modiri, An approach to map COBIT processes to ISO/IEC 27001 information security management controls. *International Journal of Security and Its Application* 6(2): 13–28.

Roca, S.K.-L.-D.-V. 2019. Cybersecurity Current Challenges and Inria's researchdirections. Le Chesnay Cedex, France: Inria.

Shoki, M., Zakuan, N., Tajudin, M.N.M., Ahmad, A., Ishak, N. & Ismail, K. 2014. A framework for risk management practices and organisational performance in higher education. *Review of Integrative Business and Economics Research* 3(2): 422–432.

Suray, N., Karpenko, E., Dubovik, M., Shlyenov, Y. & Sterlikov, F. 2019. Risk management at educational institution. *Natal* 7(2): 1171–1184.

Talet, A.N., Mat-Zin, R. & Houari, M. 2014. Risk management and information technology projects. *International Journal of Digital Information and Wireless Communications* 4(1): 1–9.

Tixteco, L.P., Prudente, C., Pérez, G.S., Toscano, L.K., Jesús, J. De, Gómez, V., De, A. & Tellez, C. 2017. Recommendations for risk analysis in Higher Education Institutions. *The Eleventh International Conference on Emerging Security Information, Systems and Technologies Recommendations*, c, 125–130.

Taylor, H. 2006. Risk management and problem resolution strategies for IT projects: Prescription and practice. *Project Management Journal* 37(5): 49-63.

Taylor, L. 2017. What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society* 4(2).

Ulven, J.B. & Wangen, G. 2021. A systematic review of cybersecurity risks in higher education.

Universities UK 2013. Cyber security and universities: managing the risk. Retrieved December 31, 2017, from http://www.universitiesuk.ac.uk/policy-andanalysis/reports/Documents/2013/cyber-security-and-universities.pdf

Walker, A. 2020. UK' 95% sure' Russian hackers tried to steal coronavirus vaccine research. https://www.Theguardian.com/world/2020/jul/17/russian-hackers-steal-coronavirusvaccine-uk-minister-cyber-attack

Webb, J., Ahmad, A., Maynard, S.B. & Shanks, G. 2014. A situation awareness model for information security risk management. *Computers & Security* 44: 1–15.

Whitehead, G. 2020. Investigation of factors influencing cybersecurity decision-making in Irish SME's from a senior manager/owner perspective Dublin, National College of Ireland.

Yin, R. 2009. *Case study research: Design and* methods (4th ed.). Thousand Oaks, CA: Sage

Yin, R. K. 2013. Validity and generalisation in future case study evaluations. *Evaluation* 19: 321-332.

Balla Moussa Dioubate
Faculty of Business and Management
University Sultan Zainal Abidin
Kampus Gong Badak
21300 Kuala Nerus, Terengganu, MALAYSIA.
E-Mail: ballamoussa1508@gmail.com

Wan Norhayate Wan Daud
Faculty of Business and Management
University Sultan Zainal Abidin
Kampus Gong Badak
21300 Kuala Nerus, Terengganu, MALAYSIA.
E-Mail: wnhayate@unisza.edu.my

Fakhrul Anwar Zainol
Faculty of Business and Management
University Sultan Zainal Abidin
Kampus Gong Badak
21300 Kuala Nerus, Terengganu, MALAYSIA.
E-Mail: fakhrulanwar@unisza.edu.my

Fauzilah Salleh
Faculty of Business and Management
University Sultan Zainal Abidin
Kampus Gong Badak
21300 Kuala Nerus, Terengganu, MALAYSIA.
E-Mail: fauzilah@unisza.edu.my

Hilmi Mohd Faiz
Pusat Pengajian Pendidikan Jarak Jauh,
Universiti Sains Malaysia
11800 USM Penang, MALAYSIA.
E-Mail: faiz@usm.my

Lee Ooi Hai
Edustats Solutions, Suite 33-01,
33rd Floor Keck Seng Tower,
203 Jalan Bukit Bintang,
55100 Kuala Lumpur, MALAYSIA
E-Mail: harley@edustats.com.my