Impact of Cybersecurity Risk Management Frameworks on Malaysian Public Universities Business Performance

By Dioubate, Balla Moussa & Wan Daud, Wan Norhayate

Universiti Sultan Zainal Abidin

Abstract- The existence of many risk management procedures helps institutions to cope with challenges and select acceptable risk management techniques. Cybersecurity risk management is one of the requirements of security management and it is significantly important in understanding the entire security profile of the institution. The aims of this study is to evaluate the impact of the cybersecurity risk management process applied in Malaysian higher education institutions. It will assess the effectiveness of existing cybersecurity risk management frameworks in Malaysian higher education institutions to monitor cybersecurity risk. The method of data collection utilised in this study is a semi-structured qualitative interview. Therefore, the sampling of 10 public universities and 12 cybersecurity risk management officers from the departments in charge of information security risk management contributed to this study and the data provided were enough to reach data saturation.

Keywords: cybersecurity, cybersecurity risk management; risk management frameworks.

GJMBR-A Classification: DDC Code: 332 LCC Code: HG106
Impact of Cybersecurity Risk Management Frameworks on Malaysian Public Universities Business Performance

Dioubate, Balla Moussa & Wan Daud, Wan Norhayate

Abstract: The existence of many risk management procedures helps institutions to cope with challenges and select acceptable risk management techniques. Cybersecurity risk management is one of the requirements of security management and it is significantly important in understanding the entire security profile of the institution. The aim of this study is to evaluate the impact of the cybersecurity risk management process applied in Malaysian higher education institutions. It will assess the effectiveness of existing cybersecurity risk management frameworks in Malaysian higher education institutions to monitor cybersecurity risk. The method of data collection utilised in this study is a semi-structured qualitative interview. Therefore, the sampling of 10 public universities and 12 cybersecurity risk management officers from the departments in charge of information security risk management contributed to this study and the data provided were enough to reach data saturation. The information gathered from respondents is transcribed and coded word by word to identify themes and sub-themes. As a result, a thematic analysis of the data is performed based on the information collected from participants. It expects to discover the strengths and deficiencies of the present frameworks used in higher education institutions. However, the participants from all the universities visited for this study deliberated that the cybersecurity risk management frameworks were considered as one of the most successful innovations in the area of higher education institutions in Malaysia. It is believed that this study would contribute significantly to understanding the performance and usefulness of cybersecurity risk management frameworks in Malaysian public universities.

Keywords: cybersecurity, cybersecurity risk management; risk management frameworks.

1. Introduction

According to Bandara (2014), universities in the United Kingdom (UK) hold crucial intellectual property across the study and supplementary academic materials that might be tempting targets for criminals. The universities face a collection of cybersecurity threats. These disrupt the running of a university web, and a targeted attempt to attain valuable information from webs and their users. Universities are also facing an increasing threat from persistent sources of menaces, attacking the sector’s economic development in the UK and abroad. Institutions should effectively manage the cybersecurity risks to the success of higher education, and other industries (Universities UK, 2013).

Lane (2007) mentioned that the context of cybersecurity in Australian universities is convoluted and prone to obscurity therefore, a solid foundation is required for the successful implementation of cybersecurity habits in the institutions. The fact that the relevance of cybersecurity is not crucially incorporated and the protection arrangement in the context of both the corporation and the intellectual setting is a difficult balancing act. However, several Australian institutions are waiting to speak with one another about creating competent control over data security.

Kang et al. (2015), the majority of Malaysian higher education institutions (HEIs) do not include ethical hacking in their security development life cycles (SecSDLC). Despite the fact that it has shown its usefulness, these institutions do not trust it. With the fast growth of information technology, hackers are given sophisticated tools, and as a result, preserving information security is becoming a difficult challenge. Using ethical hacking techniques and processes can assist to decrease security concerns. Due to a lack of penetration assessment skills, managers are hesitant to assign this arm to defend their information from opposing hackers. Consequently, it is essential to include the risk management channel retaining knowledgeable and individual assets. Because of that, there is a need for higher education institutions to imbibe a corporate approach to the management of their security information as a component of the current governance structure (Grajek, 2017).

© 2022 Global Journals
II. Literature Review

Risk attitudes in the context of cybersecurity, are linked to the opportunity for threats to exploit the vulnerabilities of an organization's assets or group of information assets (ISO/IEC, 2011; Chee & Sin, 2020). Because of the interconnectivity of computers and the ease with which many individuals may access information systems in recent years, information systems have been put at danger from accidental operator mistakes as well as natural and man-made calamities (Boltz, 1999; Talet et al., 2014). Risk management is commonly seen as a means of reducing uncertainty and its repercussions, therefore increasing the likelihood of organizational success (Talet et al., 2014). Risk management, according to the Standards Association of Australia and Standards New Zealand, defines the architecture (principles, structure, and method) of successfully managing risks (ISO/IEC, 2009). Risk management is a managerial need as well as an important component of organizational systems, comprising critical checking and management procedures. Furthermore, according to the international standards office ISO/IEC (2011), risk management coordinated actions to reduce and control risks in the company.

Cybersecurity is becoming a big concern for all individuals, including professionals, legislators, and, more broadly, all decision-makers. It has also become a serious challenge for societies that must defend against cybersecurity attacks with both preventative and reactive measures, which need intensive monitoring while still protecting freedom and avoiding mass surveillance (Fadzline, 2020). Computer security, sometimes known as cyber security or IT security, is the protection of computer systems against damage to their hardware, software, or information, as well as disruption or misdirection of the services they provide (Roca et al., 2019). To maintain company continuity, cybersecurity improves the return on investment and business prospects while reducing business risks and knowledge security from diverse threats (Sheikhpour & Modiri, 2011; Dioubate et al., 2015). Qualitative analysts use discourse to acquire information from participants, allowing them to ask how many questions are needed to grasp the phenomena the study addresses rather than how many questions are necessary to understand the phenomenon the research addresses (Cronin, 2014; Dasgupta, 2015). As a result, the focus of this research is to look at the influence of cybersecurity risk management practices on Malaysian higher education institutions.

This study’s data was gathered through interviews with cybersecurity risk management professionals. Regarding the nature of this study, the researcher used a qualitative case study approach to address the study's aim. The participants in this study were representatives of Malaysia’s twenty (20) public institutions. Based on the criteria, the representatives from a sample of 10 public universities have participated in this study. The participants were designated from the department in charge of cybersecurity risk management in the university. The department in charge of strategic planning and risk management in most universities is to manage cybersecurity risks. The executive members of the department represented the university as a unit of the study.

The case study attempts to address how and why the questions are asked, using the participants’ reference points instead of the predetermined answers imposed by the researcher (Haworth & Ali, 2001). These include exploratory, explanatory, and descriptive case studies. Before determining the research problem, exploratory case studies, fieldwork, and data collecting might be undertaken. Case studies were classified into single or multiple holistic studies by Yin (2003). Yin (2009) divided the case study's architecture into four...
unique forms based on a 2 x 2 grid. Yin used to represent a four-fold typology.

First and foremost, the matrix demonstrates that every type of design seeks to analyze contextual factors in reaction to an event. The dotted lines indicate that the border between the case and the backdrop is not sharp. The four case study design types that resulted are (Type 1) single-case – holistic designs, (Type 2) single-case designs, (Type 3) multiple-case designs – holistic designs, and (Type 4) multiple-case designs – embedded designs. Furthermore, Yin (2009) indicated that case studies might be holistic or have embedded analysis units. This is theoretically the product of four separate case study designs. These are shown in the figure below (Figure 1).

![Figure 1: Basic designs for case studies](image)

In summary, the case study's nature was based on holistic multiple cases with a single unit of analysis, i.e. in the upper right quadrant of the matrix. This is where more than one case is included in the same analysis. According to Henriott and Firestone (1983), evidence indicates that multiple cases are perceived to be more stable. The researcher used purposive sampling to ease the selection of participants from the study population with a good understanding of the subject matter. Purposive sampling is a more appropriate technique for a qualitative study, particularly when selecting a participant for specific circumstances. This sampling technique is based on the expert's judgment when choosing cases, or the researcher selects cases with a particular intent in mind (Ishak & Bakar, 2014).

The selected participants have significant knowledge in cybersecurity risk management to answer the interview questions. Doody and Noonan (2013) suggested the use of an interview guide before starting data collection. The researcher utilized the interview method with participants to collect the data. The interviews with participants from the department in charge of cybersecurity risk management in Malaysian higher education institutions were recorded and transcribed word-to-word. The researcher transcribed the audio-recorded interviews and coded the data sentence by sentence to identify the themes and subthemes (Laurence et al., 2010; Molok et al., 2013). However, in this research, the code was successively given to each participant, starting with the code number P (1) for the first participant until the code number P (10) for the last participant.

The researcher used NVivo 12 software for coding based on the transcripts made from the interview record, documents, and observations to identify the words used by respondents during the interview. The researcher applied the auto coding method to categorize research questions by source types, such as research questions and emerging themes. The evolving themes allowed us to reach the objective of this study which is to examine the impact of the existing cybersecurity risk management frameworks on the business performance of the higher education institutions in Malaysia.

IV. Findings

The investigation's findings are based on interviews with 12 participants who participated in in-
depth, face-to-face interviews with cybersecurity risk management officials from Malaysia’s ten public institutions. This section summarizes the interview outcomes from the ten university samples shown in Table 1.

Table 1: Research Question, Themes, Sub-Themes, Sources, and References exported from NVivo 12 software

<table>
<thead>
<tr>
<th>Research Question</th>
<th>Themes</th>
<th>Sub-Themes</th>
<th>Sources</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>How is the impact of the cybersecurity risk management frameworks on the business performance of the higher education institutions in Malaysia?</td>
<td>Risk Management Framework and Universities Performances</td>
<td>Framework Evaluation for University</td>
<td>6</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Performance</td>
<td>10</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Value</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Security of Information and Data</td>
<td>Information Security</td>
<td>10</td>
<td>53</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information Data</td>
<td>5</td>
<td>22</td>
</tr>
</tbody>
</table>

a) Themes 1: Risk Management Framework and Universities Performances

This theme analyzed systematically the cybersecurity risk management process to find out the contribution by evaluating the frameworks in terms of performance and value. The following sub-themes framework evaluation, the Performance of the framework on the university, and the value were discussed in this section.

Sub-theme 1a: Framework Evaluation for University

Public Universities in Malaysia are using cybersecurity risk management frameworks to facilitate the functioning, the assessment of the current frameworks permitted to know how they influence the risk management process as stated by these participants.

"I think ISMS implementation in the university has become one of the university development success factors…. Because the university has grown but one of the success factors is (P3)."

"Evaluation measurement of their effectiveness for risk management sometimes, you can look from one quantitative perspective you can look from the qualitative perspective (P6)."

"I just identify or measures the effectiveness through how many phones I received asking or seeking help to prepare the ISMS risk register. I consider the level of effectiveness of the framework to increase parallel with the number of phone calls I received (P7 and P8)."

The implementation of cybersecurity risk management frameworks was a successful innovation. It has contributed to increase security and reduce the cyberattack that destroys the reputation and economic profit of the universities.

Sub-theme 1b Performance

The framework is supporting the performance of the university regarding the knowledge base production but mainly the money as profit, which revealed that the strength was improved, the integrity and the reputation of the school were saved after the implementation of the framework.

"It will be better and so on …, so business-wise business performance for this institution will be positive (P 4 and P 5)."

"So this is where a framework … can help strengthen the integrity of information can indirectly also improve the reputation. But reputation is also important (P 9)."

"So, performance for me is sustaining the performance and also can get more value to keep more value but in terms of money, I'm not sure that because the university is not a production base (P 6)."

"The performance of the frameworks is linked to the knowledge production, the strength, values increased, and the protection of the institution's reputation. It maintains the sustainability and trustworthy of the universities.

Sub-theme 1c Value

The process of framework implementation instructed by the Malaysian government contributed to add values to the university operation and management and to maintain the sustainability of the institutions.

"The implementation of this framework allows us to learn more about risk related to information systems from experienced and knowledgeable people in this area (P 4 and P 5)."

"we say that our information security management in the campus is "in the same" place we are save that is the value for the university part of the university success factor (P 3)."

"I think the main value is sustainability, as I mentioned to your risk is about having a very conducive environment. So, it's about sustainability (P 6)."

"It gives us positive value, positive value for our institution because IT is quite heavy data protection, people feel that they have secured all the information..."
supply to us has been secured. The value it can bring is to increase the level of people's trust in our organization (P 7 and P 8).

The effectiveness is shown quantitatively and qualitatively this has improved and brought value and trust to the university. The framework implementation has given a positive value to the university. Therefore, the number of students and income of the university have increased.

b) Themes 2: Security of information and Data

This theme was related to the digital information and data used as a source of communication inside the university. The security of information is very important for the reputation of the university. The safeguard of information should be practical in terms of confidentiality, integrity, and availability (CIA). There is a necessity to protect physical and digital data in the university management system, especially for the examination process. The sub-themes are information security and information data.

Sub-theme 2a Information security

This participant pointed out the importance of having a good cybersecurity system in the university to preserve the integrity of the school and maintain its reputation. The safeguard of sensitive data in terms of confidentiality, integrity, and availability is necessary particularly in the examination process of the university.

We need a bigger example like physical security for example because some of the threats come from physical security… to make sure to secure all of these you know what we call it all physical (P 3).

When we have issues like fraud or previously we have the issue when they attacked our server. But PPKT has done a good job where we have a very secure server (P 1).

We implemented the framework ok. We have to secure the data center. The secure data center that's means we are safe. We are safe in terms of the threats from the internet from outside (P 3)

This is the most factor why do we need to consider implementing this information risk management because we want people not only the student but also the staff to have a high trust, high trust in how we protect the information (P 3).

From the cybersecurity protection perspective, the integrity of information is very crucial and critical in projecting the image and the reputation of the institution (P 9).

Cybersecurity is very technical knowledge and the appropriate right person is very important to look at this information security risk in the institutions (P 6).

The security of information in terms of confidentiality, integrity, and availability are the most part for students and staff. The framework is implemented to secure information and prepare well technical staff to protected digital, physical, and sensitive data.

Sub-theme 2b Information Data

Implementing a cybersecurity system protects data in the university and preserves sensitive data of students and staff against natural disasters and breaching. It has given confidence to universities for their operation.

So from the data center management, we analyze what's the current situation risk for our data center, we do the analysis. Then we compare with the statements what we call the ISMS (P 2).

First is university (A3) staff, they must wear their staff ID… For the outsider, we have the IT renders make with something configuration because we have 200 data servers in the data center (P 3).

So we have to define the confidentiality of the information, the availability of the data, and all assets that support the protection… So what we did was limited the scope for one of the most important processes in the academic activities were this high risk of information confidentiality, integrity, and availability especially related to exams and evaluation for example (P 9).

A cybersecurity risk management in the university secures the examination process, students, and staff data which contributed directly to the business performance of the institutions. However, the practice of policy to access and control Datacenter was implemented is to secure vital information for the reputation of the school.

V. Results and Discussion

a) Discussion on Risk Management and Universities Performances

According to Ismail et al. (2010), Framework Evaluation for University will improve the company's efficiency of having successful cybersecurity risk management. Around the same time, it also helps to accomplish the goals of the organizations. The feedback from participants displayed that the affluence of the use of the framework in the University as proof of the success of the implementation. This has contributed to an increase in new international students' arrival, which has affected the school's income. All of Malaysia's public autonomous universities' risk management activities, including strategy, risk management systems, resources and technology, and quality improvement, are intended to have a positive and important influence on risk management practices (Shoki et al., 2014). Participants in this survey agreed that implementing information security risk management frameworks was one of the most effective innovations in Malaysian higher education institutions. This framework is the safety risk management to ensure an educational environment that recognizes and assesses security risks emerging in the University's computing environment (Joshi & Singh, 2017).
The interviews of the participants in this study showed that in Malaysian higher education institutions, the use of the cybersecurity risk management framework has contributed to increase the security and reduce the cyberattack that destroys the reputation and economic profit of the universities. Another study from Ismail et al. (2010) found that having successful risk management can improve the efficiency of organizations. Around the same time, it also helps to accomplish the goals of the organizations.

According to Shoki et al. (2014), the Enterprise Risk Management Framework (ERM) is a university-wide risk management process applied in a strategic setting across the University, designed to identify potential events that may have a positive or negative impact on the University and designed to manage risks so that they are within the risk appetite (Shoki et al., 2014). Furthermore, additional research has discovered that introducing ERM or successfully executing risk management techniques has an impact on organizational efficiency (COSO, 2004 & Gordon et al., 2009).

Organizations that adopt good risk management have been successful, but those who do not participate in this practice have been ineffective (Salman and Zain UI-Abdeen, 2010). Risk management leads to the verifiable achievement of goals and the improvement of performance (MS ISO 31000:2010). As a result, it is reasonable to expect that good risk management techniques would contribute to organizational performance at Malaysia's public autonomous institutions.

Universities are education-based institutions. Therefore, one of the most critical processes is the examination which required a high level of security in terms of confidentiality, integrity, and availability. A cybersecurity risk management in the University secures the examination process, students, and staff data, which contributed directly to the business performance of the institutions. Therefore, the implementation of the frameworks is directly linked to the outcome of the University in terms of knowledge production, the strength and values increased, and the protection of the institution's reputation. The framework's effectiveness is shown quantitatively and qualitatively, and it brought value and trust to the University. It should contribute to the growth of the new students' arrival, which has increased the income and rank of the University.

b) Discussion on Risk Management and Education Institutions

ISO/IEC 27001 includes components such as security policy, cybersecurity agency, asset management, and so on. Human capital, physical and environmental protection, connection and operational management, access control, information system procurement, installation, and maintenance, cybersecurity incident management, business continuity management, and enforcement (Ismail et al., 2010).

The interviewees informed that cybersecurity gave the importance of implementing the framework to secure information in terms of confidentiality, availability, and integrity. They also mentioned the importance of having a while prepared technical staff secure digital and physical data to preserve the university's reputation. This showed the importance of implementing a safe framework to protect information and have trained technical staff to secure digital and physical data and preserve sensitive data. This study deliberated the protection of information data in terms of confidentiality, integrity, and availability. Therefore, in some universities, there was a policy to access the Datacenter implemented by the management to secure vital information stored inside. This was done to increase the university's reputation, which is very important because it is tough to repair once it is damaged.

The dissemination of information to external stakeholders will result in conclusions regarding their perception of this danger. The point of view of the company's principles and challenges differs from the point of view of internal understanding. This might offer management with new information that they had not previously suspected (Suray et al., 2019). Thus, the participants showed that the precautions practiced by managing to secure data by making policies contributed to maintaining the status of the university high. The cybersecurity policy outlined the safeguards for information data in terms of confidentiality, integrity, and availability.

VI. Conclusion

The purpose of this research is to evaluate the impact of the cybersecurity risk management approach utilized in Malaysian institutions. The study's goal was to assess the efficiency of Malaysian higher education institutions' existing cybersecurity risk management systems. As a result, once such programs are implemented, the institutional practice of integrating risk management into university culture and business operations is improved. Another piece of evidence provided by participants indicated that cybersecurity risk management frameworks had a beneficial influence on institutions. Advises that higher education institutions improve their cybersecurity risk management practices (Higher education institutions). Although some higher education institutions may adopt a risk management framework simply because the government requires it, evidence from the findings show that institutions that adopt the framework primarily to control cybersecurity risk end up with programs that rely heavily on management strategies. Therefore, the issues of universities' performances can be solved by adopting a framework to improve the risk management practices,
decision-making processes, and crisis planning. In the future, this study will consider the recommendation made by a participant to develop an updated cybersecurity risk management framework.

**REFERENCES**

29. R. Sheikhpour and N. Modiri, “An approach to map COBIT processes to ISO/IEC 27001 information
32. Sum RM and Saad ZM (2017) 3rd Int. Conf. on Qalb-Guided Leadership in Higher Education Institutions 28-42.