GLOBAL BUSINESS MANAGEMENT REVIEW
http://e-journal.uum.edu.my/index.php/gbmr

How to cite this article:
Othman, Z. (2023). Sustainability of higher education institutions: Case study on cyber attacks. *Global Business Management Review, 15*(1), 24-38. https://doi.org/10.32890/gbmr2023.15.1.2

SUSTAINABILITY OF HIGHER EDUCATION INSTITUTIONS: CASE STUDY ON CYBER ATTACKS

Zaleha Othman[1]

[1]*Othman Yeop Abdullah Graduate School of Business (OYAGSB), Universiti Utara Malaysia, Kuala Lumpur, Malaysia*

[2]*Corresponding author: zaleha@uum.edu.my*

Received: 20/09/2022 Revised: 19/07/2023 Accepted: 19/07/2023 Published: 30/07/2023

ABSTRACT

Institution (HEI). The study adopted a qualitative methodology, employing a single case study as approach. A single case study is a method established to provide insightful examination of inquiries based on an inductive process of data collection, which is appropriate for this study. The study used purposive sampling as technique in selecting the fourteen interviewees. In addition, relevant documents and observation were also conducted to confirm the validity of the data gathered. Using a thematic analysis of qualitative methodology, the findings revealed sustainability of HEI depends on how HEI counter cyber-attacks. Most important, the finding revealed eight themes of cyber-attacks, they are: Malware, Ransom attack, WannaCry, Defacement, Altered content, Denial of service, Dictionary attack and Users negligence. The findings would be useful for HEI in data protection. The empirical findings of this study reflects that HEI is vulnerable to cyber-attacks thus it is imperative for HEI management to govern and tighten their cybersecurity. The findings of this study suggest novel guidance to design security measures that could balance the open system and control security.

Keywords: Cyber-attacks; Higher Education Institution; Qualitative; Case Study

INTRODUCTION

Higher education institutions (HEI) have always been the target of cyber-attacks. As a matter of fact, hacking HEI is easy and has become a lucrative business for hacker (Forbes Technology Council, 2017). This is because HEIs have large amounts of useful data. Verizon (2017), disclosed that last year alone there were 455 cybersecurity incidents in the educational sector, and about 73 cases were related to data disclosure from malware or social engineering techniques in HEI applications.

One clear example of this is the case at Penn State University, United States, which faced a cyber disaster when it had to disconnect its network from the Internet. Clearly, the cause was a cyber-attack (Williamson, 2015). Alarmingly, the attack had been going on for two years and about 18,000 data (names and passwords) had been compromised. Although the FBI solved the case, it was a serious and terrifying episode for Penn State University, specifically, and higher education, in general. This is not an isolated case, as many other universities have faced a similar situation. Harvard and the University of Chicago were among the other United States universities that have suffered cyber threats (Carapezza, 2015), in which the personal information of staff and students was hacked. This phenomenon has a devastating effect on universities, as the event halts all academic activities. Malaysia also experiences similar cyber-attack. In Malaysia, the Schools Examination Analysis System, was recently shut down temporarily due to an alleged attack on the system. The suspension of system shocked Malaysia, as it was never expected that such a high-security and important website would be hacked. Known as ‘SQL Injection’, the attack implied that a cyber threat had penetrated the education system (Bedi, 2018). It was reported that ‘SQL Injection’ obtained about 4.9 million data from both primary and secondary school students. However, this was not the first incident of a hacking attack. There were many reported incidents, such as ‘WannaCry’, a virus that hacked the education system. The question has been asked frequently, how university deal with the cyber-attacks? Most important, what are the patterns of cyber-attacks that the higher institution deal with?

The disturbing part of it all is that HEI hold valuable data related to students’ and academic information, research information, policies, and strategies, which are vulnerable to cyber-attacks at any time. Hackers steal useful information from HEI, which is a 21st-century trade item. Loss of economic value, such as Intellectual property, research findings, personal data, and financial data, are the information stolen by hackers (Zalaznick, 2013).

So, can HEI sustain? This is the aim of the paper, to understand the patterns of cyber-attacks and to perhaps provide suggestion to avoid the economic loss facing HEI. Ramim and Levy (2006), stated that HEIs information systems provide economic value, that needs protection considering the vulnerability of the education system to cyber-attack. With everything from personal information to research information and other high-value information, it is imperative that HEIs understand the types of cyber-attacks in order to protect this economic value.

In this study, to find ways to sustain such protection, we conduct a qualitative methodology to explore the key elements contributing to sustainability of Higher Education Institutions. Our findings shows that the cyber security is important towards sustainability of Higher Education. In order to prevent the potential cyber security risks in the stuff using externally hosted web services and products as well as services depending on online services, it is therefore crucial for Higher Education Institutions to keep abreast with the knowledge on patterns of cyber-attacks.

The findings would be useful for HEI to protect their data. To the best of our knowledge, there is sparse research focusing on HEIs cyber-incidents, particularly in Malaysia. Even though the issue is topical and important, the types of cyber-attacks at HEI seem unknown. The novelty of this research is that the findings provide a rich understanding of the issue based on the socially constructed nature of the reality.

The findings are also useful for practitioners to reflect on the design of systems and management processes.

LITERATURE REVIEW

In recent years, an increasing number of studies have been conducted to examine cyber-related issues. This is probably due to the increase of concerns about the cybersecurity of information and the increase of cyber incidents. However, the number of empirical studies examining cyber-attacks at HEI is limited. Some consider that the scientific studies on security awareness in developing countries lack investigation (Marks, 2007). Most studies have focused on the technical aspect of data security. However, there is a lack of knowledge and understanding of cyber-attacks and their nature.

Although the technical aspect of data security is relevant, a greater understanding of the types of cyber-attacks affecting data security is also imperative. Rajab and Eydgahi (2019) made a similar assertion that there is a lack of findings relevant to support HEI awareness of information securities. They asserted that the compliance of universities to the proposed information securities policies is weak. They also found in many instances that faculty members and students neglect to comply with the rules of security, thereby putting their information at risk. Most shocking is that their study found that even the administrators and staff of universities have inadequate compliance. This is risky, as their ignorance of complying with best practices could put financial information of the universities at higher risk. Ismail et al. (2010) found that information security policy, risk management, access control, awareness programmes and training, and compliance are essential for HEI. These components are in line with the objective of developing the HEI cybersecurity framework, which was to apply and cover all hardware, software, data, information, networks, personal computing devices, support personnel, and users within HEI from intrusion, interception, interruption, and denial of services.

Previous studies also proved that there is a lack of attention to the issue of cyber security (Ramim & Levy, 2006). Ramim and Levy (2006) found that HEI had experienced cyber-attacks and that the nature of HEI (i.e., e-learning) opened them to cyber-attack. Rezgui and Marks (2008) found that conscientiousness, cultural assumptions and beliefs, social conditions, and university staff behaviour and attitudes towards work affect the information security awareness of staff. This finding is aligned with the findings of Rajab and Eydgahi (2019) that higher education employees’ intentions regarding information security policy compliance are influenced by information security risks, their ability to respond to information security incidents, their cost-effective evaluations of their ability and interventions’ choices in cases of information security breaches, and the probability of them being caught while violating information security policy compliance. In contrast, Belanger et al. (2017) found that sanctions do not fully influence information security policy compliance. Reading through previous studies, a gap is evident in the understanding of the types of cyber-attacks. The present study, therefore, focuses on exploring the types of cyber-attacks occurred at HEI.

METHODOLOGY: CASE STUDY

The objective of this study is to examine the patterns of cyber-attacks occurred at Higher Education Institutions in order to keep HEI sustainable. Like any other qualitative research question, this study depends on a well-specified research question, with inquiry-based understanding. Qualitative researchers (such as Creswell, 2013; Yin, 1994) prescribed that when one seeks understanding, a case study is appropriate. Further, sampling logic identified a single case study was adopted. Profile of the subject is deliberated below.

‘Case A’

To maintain the quality of the research, a single case study (i.e., case ‘A’) is employed. A single case study is a method established to provide insightful examination of inquiries based on an inductive process of data collection, which is appropriate for this study. A preliminary interview was conducted and found that there is an issue with cyber-attacks at case ‘A’, thus supporting the suitability of the case to be studied. Through the case study, we were able to gain in-depth understanding of the pattern of cyber-attacks.

Data Collection Method

Data collection is performed through participation involvement. In this study, the participants expressed themselves mainly through face-to-face interviews. However, in order to give strength to the data, triangulation of sources was gathered. Hence, relevant documents and observation were also conducted to confirm the validity of the data gathered.

- Interviews: A purposive sampling method was used to choose the participants. Purposive sampling was used in this study because it was essential to recognise the experts in order to purposively seek information relevant to answer the research questions. It is thus paramount to choose the right person to talk to, which became our fundamental criterion in selecting our samples. Following section deliberate on the participants profile of the study.
- Participants’ profile: To protect the confidentiality of the participants, each participant was identified by a code. Othman and Abdul Hamid (2018) asserted that confidentiality is essential in qualitative research. Confidentiality is part of the ethical consideration and research process and thus essential for any qualitative research. Purposive sampling was used to select the participants. Purposive sampling is a technique widely used in qualitative research for the identification and selection of information-rich cases for the most effective use of limited resources (Patton, 2002), which involves identifying and selecting individuals or groups of individuals that are especially knowledgeable about or experienced with a phenomenon of interest, in this case participants who had experience handling cyber-attacks at the case A’. All together fourteen participants were selected. Table 1 depicted the participant’s profile.

Table 1:

Participant profiles

No	Position	Affiliation	Gender
1	National Cyber Security Department Official	Government Sector	Male
2	Academician	Case ‘A’	Female
3	Academician	Case ‘A’	Male
4	Academician	Case ‘A’	Male
5	Academician	Public University	Male
6	Academician	Public University	Male
7	Academic Affairs Department	Case ‘A’	Female
8	Academic Affairs Department	Case ‘A’	Male
9	Students Affairs Department	Case ‘A’	Male
10	Director, Information Technology Department	Case ‘A’	Male

11	Information Technology staff	Case ‘A’	Male
12	Head of Department, IT Department,	Public University	Male
13	Hacker	Case ‘A’	Male
14	Student	Case ‘A’	Male

Source: research data

- Documents: Documents such as cybersecurity guidelines were used to support the data gathered from interviews. During the study, documents supported the research inquiries. The documents were given mainly by Information Technology (IT) department staffs, which helps to clarify certain aspects of cybersecurity. Documents such as surveillance audit reports provided information on the assessment of process and function as IT advocate. We also gained information about the network penetration testing report. The information prescribed the vulnerability areas of case ‘A’ (i.e., network and remedial) to overcome the weakness in the network. Other documents included articles gathered from the Internet.
- Observation: Apart from interviews, observation was also conducted to triangulate data from the interviews. Observation was conducted simultaneously with the interviews. Two of the researchers observed the controlled room at IT, accompanied by IT staff and the IT director. The observation took about 30 minutes. The aim of observation is to gain insight into the process of monitoring of cyber threats and cyber-attacks conducted by IT, which is the centre for cyber security at case ‘A’. Explanation was given as to how the IT could detect any attempt of cyber-attack via website.

Data Analysis

The researcher conducted a thematic analysis. The analysis consists of three steps, which were; first order level analysis, second order level analysis and aggregate dimension stage. First order level analysis involved labelling the raw data into categories. Secondly, the many categories were then further when through the process of level of abstraction, where from categories the researcher build themes. The last stage of the data analysis involved seeking patterns of meaning developed from the second-order level themes, which is known as the aggregate dimension stage. At this stage, the researcher builds meaning of the aggregate dimensions developed in the third stage of the analysis. This is the stage where the researcher developed pattern of cyber-attacks model. This is the stage where the researcher gives sensible meaning to the pattern emerged from the analysis. All themes were identified in the analysis section.

ANALYSIS

Several themes emerged from the aggregate dimension stage (see data analysis). Using thematic analysis of qualitative methodology, the findings implied the sustainability of HEI. Following are the themes that emerged to support the pattern of cyber-attack model at HEI.

Cyber-Attacks from The Perspective Of HEI

Our findings indicate that a cyber-attack is an offensive act of perpetrators on computer system infrastructures and networks. Congruent with previous studies (Ganesan, 2022), the advancement in internet technology leads to increased cyberattacks in Higher Education Institutions (HEIs). Incidents such as a break in the system to obtain information related to exams are common. Congruent with the argument given in the literature, HEI systems are vulnerable to perpetrators breaking in the system.

Our findings indicate HEI such as case 'A' are not safe from cyber-attacks. In fact, HEI are very cyberspace-friendly and susceptible to cyber-attacks. The data also revealed that threats come in different forms and with various purposes. In addition, the findings indicate there is also an association between cyber-attacks and individual motives. The level of technology has brought about unprecedented degrees of sophistication and impact of cyber-attacks. This threatens the smooth running of the system. Our findings revealed that cyber-attacks in HEI include virus attacks and hacking. Previous studies (Mezzour, Carley & Carley, 2014: Wang, Tse, Cui & Jiang, 2022) found similar activities: exploits, web attacks, and fake applications.

Types Of Cyber-Attacks

The findings implied that cyber-attacks is most vulnerable to open system. This finding is congruent with the previous studies that education institutions such as universities are easy targets for cyber attackers because of their culture of open communication and collaboration with stakeholders (Roman, 2014). Coleman and Purcell (2015) claimed that educational institutions have a high volume of network users and mobile users with an open networking culture, and this open access attracts hackers. Table 2 depicts various cyber threats, cyber-attacks, and motives.

Table 2:

Cyber threats and motives

Cyber-attack	Cyber threats	Motive
Virus attack	Malware	• Self-challenge • Interest to hack a certain system
	Ransom attack	• Challenge by peers to hack system • Excitement and challenge
	WannaCry	• Self-motivated
Hacking	• Defacement • Altered content • Denial of service • Dictionary attack • Through users such as password, spam, phishing	• To practice skills • Enjoyment and fun • Bridge with purpose – self-interest • Info seeking • Hackers interested in exam-related issues, such as questions, results, and grades. Some students seek information about their lecturers for personal matters. Hence, teachers' personal laptops may be targeted. • Vulnerability area • Loophole in the system • Thrill seeking

Source: from research data

Technical Aspect

Our results showed that case 'A' also encountered attempts from the three patterns (phishing, ransomware, and insider threats) of cyber-attacks. Interestingly, data implied that most cases were unsuccessful. Attempts were made, but case 'A', managed to prevent the hackers from breaking into the system (i.e., gain entrance to the server). However, there is a differing view, as our data also showed several cases of insiders who had successfully broken the system. Based on our conversation with the hacker, he confessed that he managed to gain entrance to the server using a ‘trial and error’ technique (i.e., using Internet protocol). In interviews with other respondents, they also claimed insiders were the culprit. Our respondent, the hacker, confessed that it is easier to penetrate the server as an insider than from the outside.

Case 1: Virus Attack

Data revealed that virus attacks are common at universities, including case ‘A’. Our findings showed that there are various techniques used to conduct cyber-attacks, such as viruses, worms, Trojan horses, and social engineering. Phishing, spear phishing, malware, and ransomware are frequent cyber threats challenging the server system. The motive of malware is to cause a system crash. When one thinks of malware, one thinks of ransomware, viruses, worms, etc. These malware threats are often used as a means to breach data or steal information. The motive is to gain personal information. Interestingly, there were cases in which the hackers just wanted to test their ability. Our respondent, the hacker, claimed that the thrill of hacking was his motive.

However, our findings revealed that case ‘A’ has a strong firewall that prevents these attacks. Triangulation of data (interviews with stakeholders and research respondents) indicated that case ‘A’ has sophisticated cyber security. Nonetheless, there was an incident a few years ago in which the perpetrator managed to access the system. Since then, IT department at case ‘A’, claimed they are careful and constantly upgrade the monitoring of the system in order to prevent other such cyber incidents.

Case 2: Hacking

Hacking occurs at HEI, including case ‘A’. Our findings indicate that hacking occurred at case ‘A’ in several instances. Our interview with the hacker is strong evidence that hacking happened at case ‘A’. The hacker shared his story of how he hacked the system. The story is presented below. There is triangulation of data, evidenced in respect to incidents of hacking. An officer (case ‘A’ staff) informed that there were instances of hacking in the system. She shared her story:

Every semester there will be a case of ‘hacking’ in the system. But we do not know how they do it (case ‘A’ staff). We do not know how the system was hacked. The student tried to change his CGPA to 3.67 because he wanted to apply for a grant. He also wanted to change from failed to passed (case ‘A’, admin staff).

One of the ways to hack is through passwords. The hacker develops a system using dictionary words. Normally, hackers use super-users’ or credential users’ names and passwords in accessing multiple information systems.

Our interview with the hacker revealed that there is a window for hackers to break systems. In fact, our findings revealed that hackers penetrate systems through several means. A popular means is ‘trial and error’. The hacker explained that he was able to penetrate a server using trial and error. An example of excerpt that support this statement is as follows:

Normally, attackers attack the data of end users (not clear). For example, they use phishing email and spam emails. So sometimes users do not know that that one is a bad email. They just click. In this way, hackers get your path. For example, the bad code will be downloaded onto their PC. And then their account is hacked.

Case 3: Unsecured Personal Devices

A bring-your-own-everything (BYOE) environment has its drawback. It allows students, faculty, staff, and visitors to bring everything from smartphones and tablets to laptops, desktops, and processing systems. A BYOE environment permits more individuals to gain access to the wireless network, and some of their devices may not be secure, thereby making the HEI network vulnerable.

It is a Trojan, malicious code, malware kind of thing. Normally they use email, and with social media right now, Facebook and all those things. It's quite dangerous. What we need to do is to educate users to protect their machines. At least they have their own anti-virus (IT staff).

Beudin (2015) claimed that 36% of breaches in the higher education context are attributable to hackers and malware. The author further stated that hackers use an advanced persistent threat, which means the hackers obtained access to the computer system undetected because of software vulnerabilities, leading to the eventual theft of large amounts of data.

Another means of hacking is through a malicious insider, whereby an employee, contractor, or other person with authorised access to an organisation's network, system, or data intentionally exceeds or misuses that access in a manner that negatively affects the confidentiality, integrity, or availability of the organisation's information or information systems. Malicious insiders have become increasingly prevalent on campuses, as students use keystroke loggers to capture professors' passwords and then use this information to change grades. According to Beudin (2015), about 10% of all data breaches occur at the hands of a malicious insider. A malicious insider is defined as 'a current or former employee'.

DISCUSSION

Vulnerability of HEI that affect its sustainability

Data revealed many types of cyber threats. Threats depend on the vulnerability of the system, which leads to cyber-attacks. Our findings revealed that the open-door system has its drawback. With this system, hackers can penetrate the system, and defacement is a common cyber-attack occurring due to an open system. Defacement means the perpetrators cause damage by putting up some pictures on the website. It happens when there is vulnerability in the system.

Our findings also indicate that there are many tools available online that perpetrators can use for defacement. In fact, our respondent said that tools can be obtained freely on the Internet. One disadvantage at case 'A' is that the open source for its website creates vulnerability. Our findings revealed that although the open source has some disadvantages, case 'A' is prepared to balance the open source with preventive measures. According to the respondent, hacking happened due to weakness in the open-source system. However, case 'A' balanced the open-source system with two layers of protection.

Abdulghafour Mohammad and Sergio Vargas (2022) in their study found that despite the positive impact of blockchain technology in higher education, the adoption of blockchain technology as preventive measures towards cyber attacks are not widely adopted due to three main barriers, which are technology barriers (Integration complexity, Security, Privacy, Immutability and lack of flexibility, Data unavailability), environmental barriers (legal issues, lack of regulatory compliance, the market and ecosystem readiness, sustainability concerns), and organizational barriers (lack of adequate skills, Financial barriers, Lack of management commitment and support).

Congruent with our findings, regardless of the two-layer protections, users need to be educated, as there are preventive mechanisms from the users' side, namely anti-virus software. Moreover, an alert culture has been adopted by some HEI, including case 'A'. We also found that there is an initial barrier where any identified spam will be blocked at the onset. This is not strange, as there is empirical evidence of a similar outcome (i.e., HEI are easy targets). Roman (2014) concurred that HEI are indeed easy targets for cyber-attacks. Roman claimed that the open communication and collaboration among stakeholders make educational institutions susceptible to attackers. As revealed by our respondent (hacker), open communication allows attackers access to the server. The network users are mobile and accessible. The use of various kinds of devices (e.g., mobile phone, computer) also provides a gateway for attackers. Roman (2014) supports the evidence of educational institutions as easy targets due to the culture of open access, and our findings are in agreement. The academic culture of openness and unfettered access to content and data makes educational institutions vulnerable to attackers. In addition to human factor, even sophisticated security systems with countermeasures to combat cyber-attacks, HEIs are vulnerable. According to Sulaiman et al., (2022), humans are regarded as the weakest link in cybersecurity systems as development in digital technology advances, which put the HEI sustainability even vulnerable.

Triangulation of interviews conducted with several academicians who are experts in cybersecurity affirmed that the open-access culture exposes universities to attackers. The respondent from Cyber Security Malaysia also confirmed that the culture of higher education operations makes it easy for attackers. The use of open-access networks and the freedom of obtaining access to the system make it even tougher for universities to secure against cyber-attacks. Straumshein (2015) asserts that the myriad of devices used on campuses in regards to the accessibility of data poses a risk to securing information/data. Greenberg (2014) states that the population of universities (staff, students, and other stakeholders) makes them 'an attractive target'. The abundance of personal information is valuable for attackers.

In 2014 Joanna Gamma conducted a study on data breaches in higher learning, where she investigated the data breach attributes. She noted that data breaches have been increasing over the years. Gamma stressed that the data breaches recorded are expected to be less than the actual figure. She found that education has a larger number of reported breaches but fewer records exposed. This is similar with our findings, where we found that the reported cases did not include any hacking, whereas during our interviews there were several cases of hacking that occurred at case 'A'. When asked (referring to authority relevant to data security), none admitted there were breaches. Interestingly, Gamma (2014) found doctoral (DR) programme have the majority of reported breaches, followed by master's (MA) institutions and bachelor's (BA) institutions, which had fewer reported data breaches. Interestingly, data informed (by the hacker) that the breaches are due to two reasons: testing their skills and for fun. Based on Gamma's empirical evidence, unintended disclosures and hacking/malware are the most common breaches in higher education. Gamma classified breaches into eight categories:

- Payment card fraud (CARD): Fraud involving debit and credit cards that is not accomplished via hacking.
- Unintended disclosure (DISC): Sensitive information posted publicly on a website, mishandled, or sent to the wrong party via e-mail, fax, or mail.
- Hacking or malware (HACK): Electronic entry by an outside party; data loss via malware and spyware.
- Insider (INSD): Intentional breach of information by someone with legitimate access (e.g., an employee or contractor).
- Physical loss (PHYS): Lost, discarded, or stolen non-electronic records, such as paper documents.
- Portable device (PORT): Lost, discarded, or stolen portable devices (e.g., laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape).

• Stationary device (STAT): Lost, discarded, or stolen stationary electronic device such as a computer or server not designed for mobility.
• Unknown or other (UNKN): Breaches that do not fit into the above categories or where a root cause has not been determined.

Mateski et al. (2012) examined the relationship between incident characteristics and cyber-threat attributes. They depicted the categories of incident information that may be used to assess and measure the attributes of a threat.

Table 3:

Categories of incidents

	Incident details related to classification	**Expected relation to threat attributes**
- Incident characteristics	• What type of incident occurred (e.g., website defacement, denial of service, unauthorised access, reconnaissance/probing)? • If malicious software (e.g., a virus or Trojan) was involved in the incident, was its purpose: • Command and control (C&C)? • Remote access? • Data exfiltration? • Data manipulation? • Activity monitoring?	- Technical personnel - Cyber knowledge
- Target system characteristics	- • Was the level of security protection on the target system • high—fully protected using access control, file monitoring, up-to-date patches, etc.? • Moderate—some protections implemented? • Low—very limited protections implemented?	- Technical personnel - Cyber knowledge - Access

- Timeline	- • What is the date of initial activity related to incident? • What is the most recent date of activity related to incident? • On what date was the incident detected?	- Intensity - Stealth - Time
- Covert activity	- • Was activity related to the incident identified by: • Network monitoring? • A monitoring application (e.g., intrusion detection system or anti-virus software)? • A system administrator? • A system user? • Were identified activities immediately associated with the incident? Or were identified activities originally dismissed as false alarms? • Were event logs or timestamps modified or deleted to obfuscate activity associated with the incident? • Were file/disk deletion tools involved in the incident? • Were incident activities related to reconnaissance, probing, execution, or exploitation stages of attack?	- Stealth - Cyber knowledge - Access
- Attack vector	- • Was the incident facilitated by: • Phishing?	- Stealth - Time - Cyber knowledge - Access

	• Social engineering (other than phishing)? • Remote access (e.g., VPN or modem)? • Inside access? • If the attack was facilitated by any type of social engineering, including phishing, was it a targeted, individual approach or a broad blanketing approach?	
- Attack sophistication	- • Was more than one computer system affected by this incident? • Was the internal network accessed on multiple occasions during this incident? • Were activities associated with the incident novel in any way (i.e., a zero-day attack) or common (i.e., easily acquired toolsets)?	- Stealth - Time - Cyber knowledge - Access
- Anti-virus signature	- • Does an anti-virus signature (from any vendor) exist for any malicious software involved in the incident? • If so, did the signature exist and was it widely available on the date of initial activity?	- Technical personnel - Cyber knowledge
- Physical interaction	- • Was the system physically accessed as part of the incident? • Was the incident facilitated via the introduction of a	- Technical personnel - Kinetic knowledge - Access

	physical medium (e.g., USB drive, CD, hardware)? • Did the incident result in any physical, real-world effects?	
- Obfuscation	- • Was any involved malicious software encrypted or packed? • Was any activity, function, or script injected into another for malicious purposes?	- Stealth - Technical personnel - Cyber knowledge

Source: Mateski M, Trevino MC, Veitch KC, Michalski JJ, Mark Harris J, Maruoka S, Frye J, Sandia National Laboratories. Cyber threat metrics. SANDIA REPORT SAND 2012-2427. Sandia National Laboratories: USA, pg. 9.

Observing the incidents and threats, there are some similarities and differences between our findings and the findings of Mateski et al. (2012), implying the mechanism of cyber-attacks is generally similar between countries.

CONCLUSION

The empirical findings of this research reflects that in HEI is vulnerable to cyber-attacks thus it is imperative for HEI management to govern and tighten their cybersecurity. The findings of this study suggests novel guidance to design security measures that could balance the open system and control security. In addition, the findings are relevant to the academic field by advancing the understanding of cyber-attacks in HEI. Moreover, these findings are especially useful for educational institutions that are considering or currently lack cybersecurity measures.

Implication to field of study

Cyber security protection has become main-stream concern, not only for business but at higher education. Besides, cyber related attack such as virus and hacker technology are multiplying and this impacted data security issues. Mitigation is crucial however, to mitigate one needs to know the type of cyber attacks often occurred at higher education institutions. The findings is useful as it advance the understanding of HEI. The findings could also guide HEI to develop cybersecurity risk assessment model for HEIs by modeling the patterns of cyber attacks found in this study.

Implication to practice

As this research suggests that HEI should be prepared for cyber-attacks. The open access nature of HEI is seen as high risk thus presumption of possible cyberthreats is important. The findings could guide HEI towards responding to the cybersecurity vulnerabilities among higher education institutions. We believe that cybersecurity of HEI could be safeguarded if they know the patterns of cyber-attack when these strategies are considered thoroughly and with the concerted effort of relevant HEI stakeholders.

Limitation and Future Research

It is important to mention that this study has a limitation in respect to the sample selection. In order to gain detailed information on the types of cyber-attacks in the Malaysian context, the researchers failed to get hackers to participate. There were a few hackers who were willing to contribute at the beginning of the study but changed their mind. However, those that participate provide insightful information to support the research question, thus compensate for the insightful understanding of the phenomenon. For future research, it is suggesting that causal effect study should be conducted to gain general view of the topic. Future research may examine the effectiveness of strategies for HEI.

ACKNOWLEDGMENT

The research has been carried out under the Fundamental Research Grant Scheme 13807 (FRGS/1/2017/SS01/UUM/02/27) provided by the Ministry of Higher Education (MOHE).

REFERENCE

Beaudin, K. (2015). College And University Data Breaches: Regulating Higher Education Cybersecurity Under State And Federal Law. *Journal Of College And University Law* 41(3), 657-694.

Bedi, R. (2018, June 10). Education minister confirms exam analysis system suspended. The *Star Online*. Retrieved from https://www.thestar.com.my/news/nation/2018/06/10/online-school-exam-analysis-system-suspended-says-education-ministry/

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information. & Management Advanced* Retrieved from online Publication. doi:10.1016/j.im.2017.01.003.

Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing among five approaches* (3rd ed.). Thousand Oaks, CA: Sage Publications.

Carapezza, K. (2015). Cyber Ed: How higher education is re-evaluating a growing Threat. Retrieved from http://www.Pri.Org/Stories/2015-08-06/Cyber-Ed-How-Higher-Education-Re-Evaluating-Growing-Threat.

Coleman, L., & Purcell, B. (2015). Data breaches in higher education. *Journal of Business Cases and Application*. 15, 1-7.

Forbes Technology Council. (2017). What Cyberthreats Do Higher Education Institutions Face? Retrieved from https://www.forbes.com/sites/forbestechcouncil/2017/08/21/what-cyberthreats-do-higher-education-institutions-face/#3cd88eab640d.

Gamma, J. (2014). Just in time research; Data breaches in higher education. *EDUCAUSE*. Retrieved from https://net.educause.edu/ir/library/pdf/ECP1402.pdf.

Greenberg, A. (2014). North Dakota University System hacked, roughly 300K impacted. from SCmagazine.com. Retrieved from http://www.scmagazine.com/north-dakota-universitysystem-hacked-roughly-300k-impacted/article/337181/.

Ismail, Z., Masroon, M., Mohamad Sidek, Z. & Hamzah, D.S. (2010). Framework to manage Information Security for Malaysian Academics Environment. *Journal of Info. Assurance & Cybersecurity*. Retrieved from http://www.ibimapublishing.com/journals/JIACS/jiacs.html.

Marks, A. (2007). Exploring universities' information systems security awareness in a changing higher education environment: a comparative case study research. Unpublished PhD thesis, University of Salford, Cardiff, United Kingdom.

Mezzour, G., Carley, L., & Carley, M.K. (2014). Global Mapping of Cyber Attacks. Retrieved from https://ssrn.com/abstract=2729302 or http://dx.doi.org/10.2139/ssrn.2729302.

Mateski, M., Trevino, M.C., Veitch, K.C., Michalski, J.J., Mark Harris, J., Maruoka, S., … Sandia National Laboratories. (2012). *Cyber Threat Metrics.* SANDIA REPORT SAND2012-2427. Sandia National Laboratories, USA.

Othman Z, & Hamid, FZA (2018). Dealing with un(expected) ethical dilemma: Experience from the field. *The Qualitative Report*, 23(4), 733-741.

Patton, M.Q. (2002). *Qualitative Research & Evaluation Methods.* (3rd ed). Thousand Oak: Sage Publications, Inc.

Rajab, M., & Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computer & Security*, 80, 211-223.

Ramim, M., & Levy, Y. (2006). Securing E-Learning Systems: A Case of Insider Cyber Attacks and Novice IT Management in a Small University. *Journal of Cases on Information Tech*ology. 8 (4), 24-34.

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computer. & Security*, 27, 241-253.

Roman, J. (2014). Latest incident highlights breach vulnerabilities in academia. Retrieved from http://www.databreachtoday.com/add-butler-university-to-breach-list-a-7007.

Straumshein, C. (2015). A Playground for Hackers. from Inside Higher Ed. Retrieved from https://www.insidehighered.com/news/2015/07/06/pennsylvania-state-u-cyberattackspossibly-part-larger-trend-experts-say.

Verizon (2017). *2017 Data Breach Investigation Report* (10th ed). Retrieved from https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf.

Williamson, W. (2015). Higher Education Crams for Cyber Security. Security Week Internet and Enterprise Security News, Insights and Analysis. Retrieved from https://www.securityweek.com/higher-education-crams-cyber-security.

Yin, R. K. (2003). Case Study Research: Design and Methods. Thousand Oaks, California: Sage Publications.

Zalaznick, M. (2013). Cyberattacks on the rise in higher education Foreign governments and organized crime targeting institutions' most sensitive information. Retrieved from www.universitybusiness.com/article/cyberattacks-rise-higher-education.