The Human Dimension as the Core Factor in Dealing with Cyberattacks in Higher Education

Zaleha Othman[a*], Nazahah Rahim[b], Muhammad Sadiq[c], [a,b]Othman Yeop Abdullah Graduate School of Business, Universiti Utara Malaysia 06010 UUM Sintok, Kedah, Malaysia, [c]Taylor's University, Subang Jaya, Selangor,47500, Malaysia Email: [a*]zaleha@uum.edu.my

Higher education institutions deal with an enormous amount of personal and critical data. Thus, they have a great responsibility for data protection. In recent years, higher education institutions have faced cyberattack challenges, and thus their need for data protection is obvious. As academics, we are motivated and concerned about how higher education deals with this challenging issue, and for this reason, we have conducted a study to examine the core factors in how higher education deals with cyberattacks. Using a qualitative methodology, specifically a case study method, with triangulation of data gathered from fourteen interviews, document analysis and observation, the study has several interesting findings. It demonstrates that the human dimension is at the core and that t wo key matters are contextually related to human action: 1) the decision to have an open network and 2) humans as a means and an end of cyberattacks. Specifically, the liberalisation of social networks has meant that there is a human dimension in cyberattacks. As has been found in previous studies, the human factor is one of the main concerns related to cyberattacks. This study provides several useful suggestions for preparing higher education institutions to tackle cyberattacks. Our findings are useful in practice because understanding the issue, and the process whereby hackers penetrate a system is essential in order to prevent cyberattacks.

Key words: *Cyberattack, higher education, qualitative, human, factor.*

Introduction

The higher education sector deals with an enormous amount of data, mostly personal and critical information. However, dealing with this enormous amount of data can be challenging. One of the many challenges currently faced by higher education institutions is the threat of cyberattack. There are many reported cases of cyberattacks, implying that higher education institutions have become targets. The nature of handling enormous amounts of data has made higher education a target for espionage. Penn State University in the United States, for example, faced a cyber disaster when it had to disconnect its network from the internet (Williamson 2015). Ironically, the attack originated from China and, alarmingly, it had been going on for two years; about 18,000 pieces of data (names and passwords) had been compromised. Although the Federal Bureau of Investigation solved the case, it was a serious and terrifying episode for Penn State University, specifically, and higher education, at large. This is not a single case, as many other universities have faced similar issues: Yale, the University of Hawaii, are on the long list of higher education institutions that have faced this notorious challenge.

The rising number of cyberattacks on higher education institutions is a concern. This phenomenon does not only have financial implications for higher education institutions but also has an impact on the reputation of higher education. Although higher education institutions have taken proactive measures in which they have invested heavily in infrastructure to ensure data protection through cybersecurity, they continue to make headlines. The question is what causes this.

Studies have been conducted on this issue, and there is a view that the human factor is to be blamed for the incidence of cyberattacks. According to Rajab and Eydgahi (2019), human error contributes to the lack of data protection in higher education institutions. They also found that human negligence and lack of awareness contributes to cyber-attacks at higher education institutions. Also, almost a third of those in the higher education systems in the United States have opened emails containing malicious attachments (Brumfield, 2016). A similar finding was made in a PWC (2017) report, which stated that 95% of data breaches are due to human error. The PWC (2017) report also found that 29% of cyberattacks manipulate or destroy data without the knowledge of the data owner.

BitSight Insights conducted a scientific study in which it examined the cybersecurity performance of nearly 20,000 companies against the growing threat of ransomware and reported that the education sector has the highest rate of ransomware attacks across all industries: three times more than healthcare and ten times more than finance (BitSight Insight Report 2006). Worse still, the survey revealed that academic institutions show low-security ratings, with 58 per cent of organisations in the education sector having some type of file sharing on their network. As mentioned earlier, the enormous amount of data in the education sector, including access to social security numbers, medical records, intellectual property, research, and financial data of faculty, staff and students, means that higher education institutions are a prime target for cyberattacks. Moody Investor Service (Moody Investor Service 2019) reported that, although the risk of cyberattacks in higher education is rated at medium, the trend is for the number of cyberattacks to increase, implying that the risk is escalating. Moody Investor Service claimed that higher education is at a higher risk if there is a lack of investment in cybersecurity (Moody Investor Service 2019).

Considering the breadth of operations, the expansive online networks and the innumerable access points of higher education institutions, cyberattacks must be expected. There is a view that there is a lack of preparedness within higher education institutions in dealing with cyberattacks, and thus that higher education institutions are a target for attacks. Camilla Turner, education editor of *The Telegraph* newspaper in the United Kingdom, stated on 14 April 2019 that 'universities are failing to protect themselves from cyberattacks' (Turner 2019). She reported that elite British institutions such as Oxford and Cambridge universities have been infiltrated and that millions of dollars' worth of research documents, including research on nuclear power plants, has been stolen by hackers (Turner, 2019). This is indeed, alarming.

As cyberattacks have become the new normal, it is imperative for higher education institutions to be prepared with resilient measures, to strengthen their vigilance and to be diligent in preventing data breaches. Thus, it is the intention of this paper to examine the issue further and to seek insights into the measures that can be taken by higher education institutions to cope with cyberattacks.

Cyberattacks in Higher Education Institutions

The disturbing part is the knowledge that universities hold particularly valuable personal information related to students and lecturers, research information, policies, and strategies, and this information is vulnerable to a cyberattack at any point in time. Intellectual property, research findings, are personal data, are the type of information sought by hackers (Zalaznick 2013). Universities are therefore currently susceptible to cyber incidents and cyber threats. Some observers even think that universities are particularly vulnerable because most of them practise open access and the sharing of information. According to Carapezza (2015), universities are in a dilemma, as they must find a balance between a highly secure network and a system of open access and information sharing.

Essentially, this cyberattack dilemma needs to be taken seriously. Scholars have made this claim for many years (Ramim and Levy 2006). Ramim and Levy (2006), for example, pointed out that a university information system, particularly one related to e-learning, is an area that is vulnerable to cyberattack. Their findings for the particular case that they studied indicated that a lack of security (in IT policies and procedures) was the cause, and they showed that this had resulted in multiple instances of damage to the university information system.

With everything from personal information to research and other high-value information at risk, Malaysian universities must develop both mitigating measures relevant to the Malaysian culture, and the infrastructure to curb cyber incidents and cyber threats. It is, therefore, the aim of this paper to examine the issue further and to investigate the factors contributing to cyberattacks at higher education institutions. It is anticipated that the results will be useful for universities in Malaysia, as our exploration of the issue will provide an understanding of cyberattacks at Malaysian universities. To the best of our knowledge, there has been little study of Malaysian higher education institutions, specifically and globally, even though the issue is topical and important. Those studies that have been done have neglected the socially constructed nature of the matter when investigating the issue. Gaining a rich and complex understanding of the issue is essential to produce practical and relevant results. It is expected that the end results will offer solutions for data protection for universities in Malaysia.

In summary, given the importance of the issue and the escalating risk of cyberattack, which could have wide and expensive implications for higher education institutions, it is imperative to examine the issue further. Therefore, in this article, we provide insights into how human factors affect the measures that can be taken in higher education to mitigate the risk of cyberattacks. Past studies commonly took a traditional approach, and in the advancement of knowledge concentrated on the pedagogical aspects of higher education.

This paper contributes by giving new knowledge on how higher education institutions could prepare themselves to face the challenges of the twenty-first century. We adopted a qualitative approach and interviewed fourteen participants, including information technology experts, academics, a hacker, and an administrator. The participants all had direct experience with cyberattacks, and some had direct involvement in matters related and relevant to cyberattacks at higher education institutions. This study marks one of the initial empirical attempts to examine the topic using an interpretive paradigm.

Literature Review on Cybersecurity in Higher Education Institutions

This section provides an overview of the major trends in cybersecurity and how cyberattacks are dealt with in higher education institutions. The literature reveals that nowadays, cybersecurity is the main concern for organisations wishing to keep their digital information and data secure (Sigholm, Falco, and Viswanathan 2019). Hence, in the cyber world, an organization must be proactive in order to prevent cyberattacks. Previous studies by Adams and Makramalla (2015) and Young-McLear, Wyman, Benin, and Young-McLear (2016) say that there are eight types of cyberattackers, as follows:

1.	Script Kiddies	these are immature attackers who depend on existing tools; they exploit scripts and programs and are not interested in learning how these tools work. Their basic aim is to get attention and create mischief.
2.	Cyber-Punks	these are attackers who exploit programs through writing viruses. Their basic aim is to gain fame and create trouble.
3.	Insiders	these are attackers who have internal access to an organization.
4.	Petty Thieves	these are people who hijack systems and commit online fraud such as the theft of identities and personal data.
5.	Grey Hats	these are attackers belonging to the categories of black hats (illegal hackers) and white hackers (who work to improve cybersecurity). Their aim is to attack systems to prove their ability or to find gaps in security systems.
6.	Professional Criminals	these are people who are specifically hired to attack and infiltrate systems; they are also known as cyber mercenaries.
7.	Hactivists	these are attackers who are inspired by a specific ideology, and may belong to a terrorist group.
8.	Nation States	these are attackers who are working on behalf of their governments or a group of governments.

Moreover, the prior literature shows that insiders perpetrate most cyberattacks and that the damage caused to their organisations is much greater than the damage caused by a hacker on the other side of the world (Luker and Petersen 2003). According to Payne (2003), the main reasons behind cyberattacks by insiders are these:

a. Lack of awareness related to security threats.
b. Reliance on others to deal with cybersecurity issues.
c. Lack of sufficiently skilled to address cybersecurity issues.
d. Priority is given to other matters and less on cybersecurity.

Payne also mentions that attackers are well aware of these human vulnerabilities and try to get huge benefits from these weaknesses and the lack of awareness. In his study, Payne (2003) considers cybersecurity to be an issue of great significance for higher education institutions. However, it is very difficult to market this issue of cybersecurity at the university level and, specifically, at the level of students, parents, campus administrators and faculty members. The awareness of cybersecurity and its importance varies from audience to audience.

The target audience within an institution includes the administrators, who are the most important because the administrative directors are responsible for all the decisions and policy settings for cybersecurity on the campus. Furthermore, the work of faculty members and researchers is at stake when there is a cyberattack. There is a risk of the loss of research data, information and personal data. For this reason, higher education institutions need to create an awareness of cybersecurity issues (Payne 2003). According to Caldwell (2013), cybersecurity is an issue of great concern for knowledge-centred organisations in the current era of technology. However, a greater risk for these organisations is the lack of skilled professionals. Studies have mentioned that there is a huge skills gap and shortage in the cybersecurity market and that there is a great need for organisations wishing to survive in the modern technological era to have professionals with an excellent level of cybersecurity skills to protect their valuable information (Li et al. 2019; Peacock and Irons 2017).

Cybersecurity is not a new area for research, but it has become a major national issue over the last two decades and has gained the most attention from researchers in last ten years (Bordoff, Chen, and Yan 2017). As the use of internet technologies increases, the cybersecurity risks and the threat of cyberattacks also increase. Cyberattacks are attempts to hack computers or destroy systems. Cyberattacks range from downloading a virus from the internet or something as major as hacking an entire multinational organisation in order to gain insider knowledge and to steal information (including personal and financial information).

Contributing Factors

Nevertheless, there is little information and knowledge available about how cyber attacks affect individuals in the long term. For instance, are there any psychological effects of being a victim of a cyberattack? Do people approach cybersecurity differently after they have fallen victim to an attack? How long does it take the average internet user even to notice that they have fallen victim to a cyberattack? These are all avenues that have not been explored in the current literature. Moreover, the literature has mentioned that several factors contribute to the occurrence of cyber-attacks:

a. Human Factors: there are four main factors related to individual cybersecurity behaviour: (1) experience and knowledge in cybersecurity, (2) trust or optimism in the cyber world, (3) gender differences, and (4) beliefs and perceptions about cybersecurity (Bordoff et al. 2017).
b. Business Factors: another emerging field of research concerns the factors affecting business cybersecurity practices and behaviour (Bordoff et al. 2017). The literature shows

that there are two main components in how a business deals with issues of cybersecurity. First, how it deals with its employees concerning cybersecurity, and, second, the costs it incurs in both implementing and continuously improving its cybersecurity strategies to minimise the risk of a cyberattack.

Strategies for Tackling Cybersecurity

Most of the literature on cybersecurity concerns the strategies for developing strong technology and improving the cybersecurity behaviour of employees in businesses. More than 75% of the articles found were related to these issues. However, the main strategies mentioned in the literature are:

1. **Personal strategies**: these strategies are used to enhance and improve the cybersecurity skills and behaviour of employees. They include training programmes, lectures, games, seminars, and simulations.
2. **Business strategies**: in the literature, the most extensively discussed strategy for improving cybersecurity on a business level is the sharing of information with other businesses to increase business cybersecurity.
3. **Government strategies:** there is a recently emerging consensus in the literature that governments also need to play a part, by making policies to stop cyberattacks and helping education institutions to train cybersecurity professionals.

Methodology

We collected qualitative data. We opted for a qualitative paradigm because the study aimed to gain an understanding into how higher education institutions deal with cyberattacks. The qualitative paradigm helped us to gain insightful information in the field. Apart from this, it allowed us to gain first-hand and original information, through interviews and observation, on how higher education institutions deal with the issue at hand.

Case Study Method

A single case study of Universiti Utara Malaysia (UUM), a management university in Malaysia, was used for this study. We employed the case study design since a case study fits best when one is examining a context-bound situation. In addition, a case study is a method used to provide insightful examination through inquiries, based on inductive processing of the data gathered, and this reflects the intention of the present study. An initial interview was conducted, and it was found that there is an issue with cyberattacks at UUM, thus supporting the suitability of UUM as a case. Through the case study, we were able to gain an in-depth understanding of the cyber threats and to suggest measures through which the threats could be avoided. The following section describes the background of the chosen case.

Case Profile – Universiti Utara Malaysia

UUM is a public university providing undergraduate and postgraduate academic courses in management. There are about 20,000 students, with most students attending full-time courses. UUM has about 12 departments (including centres and units). All the departments have adopted an online service. UUM has five major online applications: UUM e-com (payment gateway), UUM Portal, an application system, an admissions system, and UUM Online Learning, all of which come under UUM IT department.

On 8 August 2016, UUM established a strategic partnership with CyberSecurity Malaysia as a step towards ensuring the security of its cyberspace (http://www.uum.edu.my/en/uum-news/3301-uum-cybersecurity-malaysia-pact-to-strengthen-national-cyber-defence). UUM realised that cyber threats and attacks are not limited to viruses and malware attacks, but go beyond this. Although UUM has an advanced ICT system (including Internet of Things security and cloud security to prevent cyber espionage and warfare), it needs to keep ahead of the perpetrators. UUM has taken many proactive and innovative measures to pursue its cyber defence preparedness in line with the current cyber threat scenarios.

UUM Information Technology (UUM IT)

UUM IT is at the core of information technology at UUM. Its goal is to spearhead innovation in IT to enable seamless communication within the UUM community. It has four listed objectives: Technology Infrastructure, Information Systems, Customer Services, and Innovation. With the vision of creating a digital campus, UUM IT envisaged that UUM would stand connected and that communication would be seamless. UUM IT supports two major areas: the academic area and the administrative area. The academic function involves three focus areas (IT, online learning, and evaluation), while the administrative support involves IFAS, an integrated financial and accounting system, a personal information system and a student affairs department.

Although UUM has cybersecurity measures in place, a cyber incident still occurred. Around 2010, UUM experienced a cyberattack on its system that resulted in the server that hosted the UUM system application shutting down, putting a halt to students' and faculty members' academic work. In order to assist in understanding the issues addressed in this case, the following section will describe the relevant inquiries we made to instigate an understanding of the issue and to contribute to practice and knowledge.

Interviews

We designed our interviews to gain a wide range of views about the cyberattack challenges faced by higher education institutions. We interviewed fourteen participants who were able to give good insights into the topic. We selected participants who would share their experience, knowledge and skill on the topic under study. Table 1 depicts the profile of the participants in this study.

Table 1: Participants' Profiles

No	Position	Gender	Age
1	Cyber security Agency officer	Male	30-40
2	Academic staff (UUM)	Male	50-60
3	Academic staff (UUM)	Male	30-40
4	Academic staff (UUM)	Female	30-40
5	Academic staff (Public University)	Male	30-40
6	Academic staff (Public University)	Male	30-40
7	Academic Affairs Department officer	Female	40-45
8	Academic Affairs Department officer	Male	30-40
9	Student Affairs Department staff	Male	20-30
10	UUM IT officer	Male	30-40
11	UUM IT officer	Male	40-50
12	IT Department, Universiti Sains Malaysia officer (Public University)	Male	40-50
13	Hacker	Male	20-25
14	Student	Male	20-30

Our participants were, on average, aged between 30 and 40 years, and all of them had a direct connection to dealing with cyberattacks. They were a hacker, several administrators and several educators. The interviews were conducted face to face with the participants. Because of the nature of the research, which requires inductive and purposive sampling, the participants were selected on the basis of their ability to have an in-depth understanding of the research question. All of the participants gave consent to their interviews being tape-recorded, and all the interviews were later transcribed. Each interview lasted 60 to 90 minutes and covered the question of how to deal with cyberattacks.

Observation

We also conducted an observation. The observation aimed to triangulate the interview data. We contacted the IT administrator, seeking permission to observe the control room, which was on the premises where the university conducted its surveillance. Our observation lasted for about 30 minutes and focused on the people managing the process. Two of the researchers carried out the observation and were accompanied by UUMIT staff. The observation aimed to gain insight into the process of monitoring for cyber threats and cyberattack conducted by UUMIT, which is the centre for cybersecurity at UUM. An explanation was given on how UUMIT detects attempts at attack or actual attacks.

Documents

Documents such as cybersecurity guidelines were used to support the data gathered from the interviews and the observation. The documents were given to the researchers by UUMIT and helped to clarify a certain aspect of the mitigating measures. Documents such as surveillance audit reports provided information on the assessment of the process and functions of UUMIT. We also gained information about a network penetration testing report from UUMIT. The information described the vulnerable areas in UUM, such as the network, and the remedies used to overcome the weaknesses in the network. Other documents reviewed included articles gathered from the internet.

Data analysis

We designed the interviews to address the process of dealing with cyberattacks. We adopted a thematic analysis technique for analysing the data. We focused on coding for occurrences and connections between the codes. We conducted an audit trail and a peer review to reduce bias. A pattern, the human factor, emerged as to the means of mitigating cyberattacks at higher education institutions. The pattern emerged through a process of analysis, which involved three steps: 1st order concept, 2nd order theme, and aggregate dimension. The three-step analysis of Gioia, Corley and Hamilton (2012) was followed.

Findings and Discussion

The purpose of this study was to identify the factors associated with cyberattacks at higher education institutions. Based on the thematic analysis conducted, the keystone finding was that the human factor is associated with cyberattacks at higher education institutions. Our finding also demonstrated two key matters that are contextually related to the human factor: 1) the manifestation of the openness of the network, and 2) humans as a means and an end of cyberattacks.

First Key Matter: Open Networks

Based on the thematic analysis, open networks, that is, the practice of having an open system at higher education institutions contributed to the human factor as the keystone of cyberattacks. The openness of the network is an integral component of the operations of a higher education institution. The data implied that the decision to have an open system was a management decision, and thus was the result of human intervention. Our findings placed individuals as the decision-makers in relation to the open nature of the network. Expanding our analysis, the thematic analysis implied that the greater the freedom advocated by the management concerning the openness of the network, the higher the risk of cyberattacks, unless this is matched by higher investment in cybersecurity. This is congruent with past findings, such as those of Straumshein (2015), who claimed that the nature of universities is such that they are exposed to threats because of their collaborative network culture (i.e., open access and freedom of access to the network). The myriad devices contribute to the freedom to access the network. Our thematic analysis results showed that the myriad devices used by the stakeholders add to the difficulty of controlling access to the network; this is different from other organisations where access to the corporate network is easier to manage and control. There are external devices that contribute to the stakeholders' ability to access the server. Also, the findings revealed that data breaches such as hacking and unintended disclosure are some of the more common attacks at higher education institutions. This is consistent with previous studies that found that data breaches in higher education are hacking or malware, unintended disclosure, and portable device breaches (Coleman and Purcell 2015).

However, the thematic analysis revealed that UUM had, so far, managed the cyberattacks, or breaches of the system, efficiently. This is clear from the following excerpt: *"So far we don't have extreme cases. Before we used to encounter one case … where there was a memo from the hacker 'YOU HAVE BEEN HACKED'. (UUMIT officer). The case was detected. It was from Egypt. Cannot do anything. But after that UUMIT checked the error how the hacker break through the server" (UUMIT officer). '*

Linking the above to human factors, stringent and diligent cybersecurity is called for. The thematic analysis indicated that UUM management should not rest content, as the digital era could create a higher risk for higher education institutions dealing with cyberattacks in the future. This is because *"there are many ways to hack the system, through system loophole, the weakness point"*. Interestingly, the dataset of our study indicates that the multiple roles played by higher education institutions contribute to their vulnerability to cyberattacks.

The Multiple Roles of Higher Education Institutions

Our data revealed that, because of the nature of a higher education institution (and considering here the structure of universities), the multiple roles it plays (three functional roles: an administrative role, an academic role and a research role) make it easier for cyber attackers to penetrate the system. All these functions are inter-related, but at the same time, they are relied on independently. Each has its network security requirements and serves a different purpose. As mentioned, the multiple roles mean that it is even easier for hackers to penetrate the system. In addition, our participants asserted that a controlling centre such as UUMIT has too great a responsibility, as it covers all the functions of UUM. *"UUM System is huge and only UUMIT alone handling the system" (UUMIT officer).* The lack of expertise and the lack of human resources to deal with such huge responsibilities add to the potential for cyberattacks.

Second Key Matter: The Human Factor as a Means and an End of Cyberattacks

Our findings revealed that humans are a factor in mitigating cyberattacks. Nonetheless, they also revealed that humans are the leading factor in causing cyberattacks. Specifically, the liberalisation of social networks means there is a human dimension to the causes of cyberattacks. Previous studies have also revealed similar findings that the human dimension is one of the main contributors to the poor state of cybersecurity in Malaysia (Muniandy and Muniandy 2012). Analysing the data, we found that humans' lack of awareness and carelessness in managing passwords is common, contributing to a higher education institution such as UUM becoming a target for cyberattacks. This is not surprising, as the past literature also found that 70% of users use the same password for each website login, 67% do not like to be forced to change their password, 65% of employees either use the same password for different applications or write the password down, 50% of users never change their online passwords, and 28% of online banking users use their passwords on other internet sites (Ciampa 2010). The ignorance of users makes passwords a frequent focus of attacks. This explains the risk of cyberattacks. Our findings revealed that UUM had encountered several attempts at cyberattacks: phishing, ransomware and insider threats. Interestingly, the data implied that the cases were mostly unsuccessful. Attempts were made, but we found that UUM had managed to prevent the hackers or perpetrators from breaching the system (gaining entrance to the server). Our data also showed that there were several cases of insiders who had successfully breached the system. In our conversation with a hacker, he confessed that he had managed to gain entrance to the server using a 'trial and error' technique, that is, by using IP. In other interviews with other respondents, the claim was made that an insider was the culprit. Our respondent, the hacker, confessed that it is easier to penetrate a server as an insider than it is from outside.

From the explanation shared by the respondent, the hacking happened because of a weakness in the open-source system. However, UUM balanced the open-source system with two layers of protection. Most importantly, the finding revealed that, regardless of the two-layer protection, users need to be educated, as there are preventive mechanisms available on the users' side, like anti-virus software. There is also an alert culture adopted by UUM. The following excerpt proves that actions are taken to compensate for the open-source system:

"If there is a spam email, normally we will email, that is our practice. Because there are a lot of spam emails. And sometimes we cannot, even machine cannot categorize that this is spam. Because we look at the image very --- aww – it's normal, normal (laughs). When we go deep into this, this is spam email" (Respondent/ UUMIT).
We also found that there is a first barrier, where any identified spam will be blocked from the outset. *"If that one is well-known spam, then the system will block. If there is an attempt, that will be blocked" (UUMIT officer).*

This is not strange, as there is empirical evidence of similar outcomes, namely that higher education institutions are easy targets. Roman (2014) confirmed that higher education institutions are indeed easy targets for a cyberattack. Roman associated the culture of open communication and collaboration among stakeholders with the susceptibility of educational institutions to attack. As revealed by our respondent, the hacker, the open communication eases attackers into the server. The network users are mobile and accessible. The use of various kinds of devices like mobile phones and computers creates a gateway for attackers. Roman (2014) supports the evidence that educational institutions are easy targets because of the culture of open access. Our findings indicate that this is accurate. The academic culture of openness and the unfettered access to content and data makes educational institutions vulnerable to attack.

The triangulation of the interviews conducted with several academics who are experts in cybersecurity mentioned, similarly, that the open-access culture exposes universities to attack. One of the respondents confirmed the findings that the culture of higher education and the nature of universities' operational activities make things easy for attackers. The demand for an open-access network and the freedom of accessibility to the system make it even tougher for universities to protect themselves against cyberattacks. Straumshein (2015) asserts that the myriad of devices used on campuses to access data poses a risk to the security of information and data. Greenberg (2014) asserts that the population of university residents (staff, students and other stakeholders) makes universities 'an attractive target'. The abundance of personal information is valuable for attackers. Chow (2015) claimed that the cutting edge research conducted at universities is also a rich target for hackers. However, UUM has not yet reached this level. In our findings, there is no issue in respect of cutting edge research being the target of cyberattackers, but there is concern about personal data. This is probably because the research at UUM is in the social sciences, and hence there is limited availability of sensitive and secret information.

In regards to the damage, here is what one respondent said:

"It depends --- if it is targeted to the system admin for example, or the administrator and they open it on the server, maybe the damage is quite big enough. But if you target the user, then the impact will be under user" (UUMIT officer).

On the other hand, human action is also an important mitigating measure to curb cyberattacks at UUM:

"If there is some hacking activity, we block. But if they are trying to do some hacking, I mean the normal one. The activity is already in our database and the system will block.

"If the system looks at the pattern, say this is the bad one, the system will block" (UUMIT officer).

Through our observation, we noticed the constant control performed by UUMIT. During our observation in the control room, we were shown how the staff in charge monitored the pattern of traffic and the irregularities in the traffic in order to detect any attempt to break into the system. This suggests that humans play a crucial role in managing cyberattacks. The role of a security analyst, for example, is key in protecting the infrastructure of a corporate network from organised cyberattacks or random cyberattacks. Jajodia, Liu, Swarup and Wang (2010) found that the human role is significant in managing cyberattacks and that the security analyst, called a 'defender', who oversees the infrastructure of a network has a very important role. The 'defender' is the key to identifying a cyberattack.

Conclusion

Institutions of higher education, such as UUM face a constant deluge of cyberattacks. Thus, it is imperative that UUM studies and focuses on human measures to face the challenges created by cyber threats, although this study also found that humans are the means of cyberattacks. Our analysis revealed that higher education institutions are not well prepared for cyberattacks. Although the government, in general, has measures to cope with cyberattacks, there is limited cyber protection in respect to security in cyberspace for higher education institutions including UUM. The participants stated that higher education institutions such as UUM should factor in the human dimension, as this is core in mitigating cyberattacks. An explanation of how human beings can lead the way as both the means and the end.

First, talent development. Digital forensic experts are required in UUM. It is recommended that UUM, or any other higher education institution for that matter, develop talent or hires talented human capital, as one of the essential components of its preventive measures. As UUM houses a huge volume of sensitive data and any cyber attack may cause significant damage far beyond the walls of the academy, UUM must have experts. Experts such as digital forensic experts are needed to meet the cybersecurity challenges. The development of cybersecurity expertise for UUM is essential, and similarly, other colleges and universities can be better equipped to address cyber threats.

Second, the open system concept. Checks and balances are a priority. UUM should have checks and balances of its open system. Although it is important for UUM, or any other higher education institution, to adopt an open and transparent mode of consecutiveness, the higher education institution needs to have some control and some degree of balance between its open system and data protection.

Third, education. It is also recommended that UUM, and any other higher education institution, educates its staff and students in how to understand cyberattacks and the preventive measures against cyberattacks. Awareness programmes should be initiated and continuously organised to educate people on this subject. Higher education institutions are exposed to cyberattacks because of the vulnerability of their open systems, which could be broken into using SQL injections. Awareness of this should be taken into consideration when the institutions create their education awareness programmes.

Fourth, the behaviour of employees. This is one other factor that needs attention. The attitude among the employees at UUM and other higher education institutions needs serious attention. According to Adnan Rizal, Suhaimi Sarijan and Norhayati Husin (2017), although Malaysians are aware of the risk of cyberattacks, their lackadaisical attitude towards them makes them vulnerable to hackers. Complacency is another attitude that means that Malaysians are susceptible to cyberattacks.

Implications for Practice

Our findings are particularly useful for UUMIT. Understanding the issues and the process by which hackers penetrate the system is essential to prevent cyberattacks. This study gives just that understanding, providing insights into the process of cyberattacks and cyber threats, particularly for UUMIT. This information will be useful to enable UUMIT to prepare and develop measures against future threats. Securing data is crucial for UUM, and through our findings, UUMIT could be one step ahead of the hackers. The importance of keeping information safe is a priority for UUM. The open system provides transparency, but at the same time, it exposes UUM to hacking; thus, acting as a steward of data, UUM should consider measures to strengthen its cybersecurity.

Future Research

As for future research, the reported findings are based on a sample of participants that is limited in size and was identified through purposive sampling. This suggests that future research should develop a survey instrument that can be used for a larger scale quantitative study that would confirm and generalise the variables.

Acknowledgement

The authors wish to thank the Ministry of Education Malaysia for funding this study. The grant is coded as 13598.

REFERENCES

Adams, M., & Makramalla, M. (2015). Cybersecurity skills training: An attacker-centric gamified approach. *Technology Innovation Management Review, 5*(1), 5-14.

Adnan, Rizal Haris & Norhayati Husin, (2017). Information Security Challenges: A Malaysian Context *International Journal of Academic Research in Business and Social Sciences* 7 (9), 397-403.

Bedi, R. (2018). Education minister confirms exam analysis system suspended. *Star Online*. (10 June). Access on 13 October 2019 at https://www.thestar.com.my/news/nation/2018/06/10/online-school-exam-analysis-system-suspended-says-education-ministry/.

BitSight Insight Report. (2006). The rising face of cybercrime: Ransomware. www.bitsightech.com. Access on 13 October 2019.

Bordoff, S., Chen, Q., & Yan, Z. (2017). Cyber-attacks, contributing factors, and tackling strategies: The current status of the science of cybersecurity. *International Journal of Cyber Behavior, Psychology and Learning*, 7(4), 68-82.

Brumfield, J. (2016). Verizon Data breach investigation report finds cybercriminals are exploiting human nature. Access on 13 October 2019 at https://www.verizon.com/about/news/verizons-2016-data-breach-investigations-report-finds-cybercriminals-are-exploiting-human.

Caldwell, T. (2013). Plugging the cyber-security skills gap. *Computer Fraud & Security, 2013*(7), 5-10.

Carapezza, K. (2015). Cyber ed: How higher education is re-evaluating a growing threat. *WGBH News*. Access on 13 October 2019 at http://www.pri.org.

Ciampa, M. (2010). *Security awareness: Applying practical security in your world*. Boston: Course Technology.

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

Costa, P., Montenegro, R., Pereira, T., & Pinto, P. (2019). The Security Challenges Emerging from the Technological Developments. *Mobile Networks and Applications*, 1-6.

Gioia, D., Corley, K., & Hamilton, A., (2012). Seeking qualitative rigor in inductive research: On the Gioia methodology. *Organisation Research Method,* 16(1), 15-31.

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

Jajodia, L. S., Swarup, V., & Wang, C. (2010). *Cyber situational awareness*. New York: NY: Springer.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management,* 45, 13-24.

Luker, M. A., & Petersen, R. J. (2003). *Computer and network security in higher education*. Jossey-Bass: John Wiley & Son. Inc.

Moody's Investor Report (2019). Cyberattacks represent growing risk for the global higher education sector. Access on 13 October 2019 at https://www.moodys.com/research/Moodys-Cyberattacks-represent-growing-risk-for-the-global-higher-education--PBM_1176397.

Muniandy, L., & Muniandy, B. (2012). State of cyber security and the factors governing its protection in Malaysia. *International Journal of Applied Science and Technology*, 2(4), 106-112.

Payne, S. (2003). Campuswide security education and awareness. In M. Luker & R. Peterson (Eds.) Educause leadership strategies, 8. *Computer and network security in higher education* (pp.31-44). San Francisco, CA: Jossey-Bass.

Peacock, D., & Irons, A. (2017). Gender inequality in cybersecurity: Exploring the gender gap in opportunities and progression. *International Journal of Gender, Science and Technology,* 9(1), 25-44.

Potter, L. E., & Vickers, G. (2015). *What skills do you need to work in cyber-security?: A look at the Australian market.* Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research, ISBN: 978-1-4503-3557-7, DOI: https://doi.org/10.1145/2751957.2751967.

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 cyberattacks and novice IT management in a small university. *Journal of Cases on Information Technology*, 8(4), 24-34.

Roman. (2014). Add Butler University to breach list - Latest incident highlights breach vulnerabilities in academia. Access on 30 September 2019 at http://www.databreachtoday.com/add-butler-university-to-breach-list-a-7007.

Sigholm, J., Falco, G. & Viswanathan, A. (2019). Enhancing Cybersecurity Education through High-Fidelity Live Exercises (HiFLiX). In: Proceedings of the 52nd Hawaii International Conference on System Sciences: . Paper presented at 52nd Hawaii International Conference on System Sciences, January 8-11, 2019, Grand Wailea, Maui, USA (pp. 7553-7562). IEEE conference proceedings

Straumshein, C. (2015). A playground for hackers. From inside higher ed. Access on 3-September 2019 at https://www.insidehighered.com/news/2015/07/06/pennsylvania-state-u-cyberattackspossibly-part-larger-trend-experts-say.

Turner, C. (2109). Universities are failing to protect themselves from cyberattacks, report warns. *The Telegraph. Education* (14 April). https://www.telegraph.co.uk/education/2019/04/03/universities-failing-protect-cyber-attacks-report-warns/ Accessed 23 July 2019

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

Young-McLear, K., Wyman, G., Benin, J., & Young-McLear, Y. (2016). A white hat approach to identifying gaps between cybersecurity education and training: A social engineering case study. *Advances in Human Factors in Cybersecurity* (pp. 229-237): Springer.

Zalaznick, M. (2013). Cyberattacks on the rise in higher education. Foreign governments and organized crime targeting institutions' most sensitive information. *University Business*. Access on 30 September 2019 at www.universitybusiness.com/article/cyberattacks-rise-higher-education.