Title: Post-Secondary Cyber-Aware to Cyber-Crimes

Capstone Project: Cyber-Aware Project

Author: Darlene Sunderland / j0005588

Program Name: BESMS Capstone 4900

Institution: Justice Institute of British Columbia

Date: April 3, 2018

Instructor: Beth Larcombe

Abstract

Security departments at post-secondary institutions are vulnerable to cyber-attacks such as malware/ransomware, phishing, distributed denial of service (DDoS) and password attacks on applications. The literature reviewed for this critical appraisal report looked at cyber-criminals, their crimes and what security specialists are doing to protect institutions from falling prey to attacks. In order to determine how to protect data and networks from cyber-attacks the institutions must first determine weaknesses, vulnerable areas and establish goals to mitigate attacks that are most likely to occur, and potentially impact thousands. Once security specialists identify the weak areas, and the most likely cyber-attacks then they can determine how to mitigate those identified risks. My research question has therefore been identified as follows: "What are the three most likely cyber-attacks in relation to a security department at a post-secondary institution, and how can these risks be mitigated?" The approach taken to review the literature on this topic was to identify the most likely attacks in this environment, and then move from this identification to understanding possible impacts followed by ways to plan to mitigate the risks. There was no time line established to restrict the literature reviewed in order to allow a review of cyber-attack threats from past to present. The research found that the most likely attacks were ransomware, DDoS and phishing. Each had the possibility to have a significant impact to a security department's resources, including shutting down of services run electronically, potential loss of information, and inability to respond to requests for service. Mitigation strategies included education, training and specific information technology (IT) strategies such as regular patches to applications.

Keywords: Cyber-attack, universities, Canadian, post-secondary institutions, vulnerabilities

Table of Contents

Post-Secondary Cyber-Aware to Cyber-Crime

Background – The Problem

Cyber-attacks in businesses, personal and educational arenas are becoming more common each day. There are daily news items outlining the latest attack(s) and the resulting damage caused. There seem to be many types of attacks and the results can be varied. In some cases there can be privacy breaches, in others, operations can be disrupted, and assets can be frozen until ransoms are paid. If cyber-criminals obtain access to secured data via a network breach there could be loss of information and or financial loss, and legality issues. Cyber-attacks are a problem that is likely to increase as our world becomes more dependent on technology. I felt it was important to determine which of these attacks would most likely have a negative affect in a post-secondary security department. Studying the types of cyber-attacks that can affect post-secondary institutions provides an opportunity for me to understand the current issues, and recognize ways to protect against them. If we become more aware of cyber-attacks, then we will be more likely to notice new attacks of this type as they arise in the future and mitigate the risks effectively.

This paper will therefore focus on identifying the three most likely types of cyber-attacks to have a negative impact on a security department's everyday operations at a post-secondary institution.

Define the Question and Rationale

The purpose of the paper is to determine areas of high cyber-crime risk to a security department in a post-secondary institution. The results of the research should provide a road map to steps that security departments may choose to assist them in protecting against a risk area that is often overlooked and which could have significant negative consequences to the department.

Setting

The focus is on security departments within post-secondary institutions. This area was selected as an area that needs addressing to prevent future loss of information and recommendations to assist with planning and mitigation.

Design Type

A critical appraisal was performed of the available literature in the chosen area of study.

Research Techniques

The work was done via review and analysis of secondary sources. A critical appraisal was then used to apply the information found in the research to the planned area of study: The security departments within post-secondary institutions.

Data Collection

The literature researched consisted of secondary sources to provide insight on current cyber-attack trends and mitigation strategies. Articles, news, conferences reports, post-secondary thesis, government documents and scholarly research was considered for secondary source data and analyzed before final consideration. The initial literature that I had noted for the research project included "Effective management of information security and privacy" by Anderson (2016), and "Information security risk management framework for university computing environment" by Singh and Joshi (2016). Also of interest was "Common types of cyberattacks in education and what we can learn from them" by Biddle (2017).

Analysis of Data and Validation

The literature reviewed for the research provides the background to the different types of cyber attacks, likely affects on organizations, and possible strategies for mitigation. This data was then be analyzed in order to determine how it might apply to the security department in a post-secondary institution. This information was used to help validate the findings from the research and to support which risks may have the highest impact on a security department. Also, the research provided some options for risk mitigation, depending on the type of cyber-attack. This information will be used to provide suggestions for security departments in order to better protect themselves from cyber-related risks.

Potential Ethical Issues

There are minimal ethical issues in relation to this research paper, due to the fact that the project focus is on the security departments of post-secondary schools in general rather than a specific department, and the research does not involve any interviews or involvement with individuals, but instead consists of a critical appraisal of secondary sources.

Purpose of Study

The purpose of the study is to determine which cyber-attacks are likely to have the biggest impact on security departments at a post-secondary institution and then determine what mitigation strategies can be taken for damage control. From this purpose, the following research question was developed.

Research Question

“What are the three most likely cyber-attacks in relation to a security department at a post-secondary institution, and how can these risks be mitigated?”

Theoretical Perspective

Per initial review of available theory on cyber-crime, it appears that theorists are approaching it from a criminology viewpoint. The most common framework being used in relation to cyber-crime is that of Routine Activity Theory (Leukfeldt & Yar, 2016). This theory will be considered later in the paper when looking at the ways cyber crime risks can potentially be mitigated and prevented.

Project Scope

The scope of the project is to identify, through research, the current types of cyber-attacks and to determine the impact it could have on security departments at post-secondary institutions. The three most likely cyber-crimes to have a negative impact on security departments of a post-secondary institution were identified. Critical analysis of the likely affects of the attack, in relation to the operation of a security department, will help to identify those attacks most likely to cause damage. Research was done to determine the best methods of mitigating damage from those types of attack.

Significance of Study

By defining the main risks, the research study will provide vital information about the potential impact cyber-attacks could have on post-secondary institutions' security departments, and provide insight about how departments may develop policies to avoid the risk or lessen the impact.

Limitations

Due to the varying types of cyber-attacks that occur, the paper cannot address all potential cyber-attacks. The review will be limited to current high profile cyber-attacks from the recent literature, with a focus on the three most likely to affect post-secondary security departments. The cyber-war is a continuous battle, and as security analysts implement security measures to stop cyber-criminals, new methods are developed. Therefore, it is possible that new cyber-attacks could be of high risk, but not discussed in the paper. Per the initial review of available literature, some discussions around cyber-attacks appear to relate to organizations in general, and not specifically post-secondary institutions. Critical appraisal will therefore be performed to determine how the risks were identified and the affect to a security department at a post-secondary institution. These results will therefore be limited by the understanding and analysis performed by the author.

Finding the Evidence – Literature Search

Search Methodology

The literature for the paper was chosen with the purpose of determining the three most likely cyber-attacks that a security department at a post-secondary institution would be exposed to. Firstly, I performed an initial key word search in my initial search for: Cyber-attacks, universities, post-secondary, Canadian and most likely cyber-attacks on the Justice Institute of British Columbia (JIBC) and University of British Columbia (UBC) library websites, searched Google Scholar and searched the world wide web (WWW). The initial search through JIBC was 186,124 hits and not related directly to my research. Secondly, when I refined my search to include vulnerabilities to universities/post-secondary into the search there were 25,118 hits. The hit counts were from the JIBC, UBC Library and Google Scholar. Due to using an antivirus software program, Total AntiVirus (Total AV) to avoid cyber corruption to my personal electronic devices, the program will not display the total number of searched articles (hits) from the WWW. The Total AV software controls the cache and limits the content displayed. Therefore, I have not provided numbers for the WWW searches. I then reviewed results by title and chose those most suited to my research topic – thirty-one (31) articles were chosen this way. I then reviewed abstracts and other information (where abstracts were not available) of eighteen (18) articles to narrow my search to ten (10) articles. I did not place a timeline on the literature for the project in order to compare older cyber-attacks to the most recent cyber-attacks affecting post-secondary institutions today. The definitions laid out in the older literature still apply currently. Therefore, it was important not to limit the research on cyber-attacks this way. I excluded literature that went into detail about a specific type of cyber-attack to avoid biased opinions. Articles that did not directly relate to the university environment and too technical were also excluded.

Selecting Articles to Review

While searching for literature to determine which information would be used for my research, I chose eighteen (18) articles for abstract review. Of the eighteen (18), seven (7) did not have abstracts therefore I reviewed other aspects of those documents such as the titles, main sections and overview of content discussed within these articles. The authors' biographies were searched to assess if they were specialists in the field and whether the information came from reputable sources. The articles that I performed abstract reviews were chosen because they had titles that related to my research topic. They were either related to post-secondary institutions and cyber-attacks, or identified common cyber-attacks in the field, or discussed ways to mitigate the risk of such attacks.

Of the eighteen (18) articles, the nine (9) noted below were chosen for final review and analysis: Anderson (2006); Biddle (2017); Coughlan (2017); Diaz, Anderson, Wolak & Opderbeck (2014); Harris and Hammargren (2016); Park, Kim, Boyd & Dawson (2001); Polyakov (2017); Simon (2016), and Singh and Joshi (2016). The chosen articles for full review had specific relevance to my research topic. Park et al. (2001) discussed a type of cyber-attack (Denial of Service [DoS]) that was relevant in 2001. Polyakov (2017) explained what DoS and DDoS attacks are and reports DoS cyber-attack is still a security risk to singular devices today. Whereas Biddle's (2017) list of attacks report DDoS as a risk to post-secondary institutions and provides explanations. Vulnerabilities to universities due to their need for large open networks and inability to control all devices using the networks lead to security breaches (Singh & Joshi, 2016). Coughlan (2017) reported the top cyber research university was unable to stop a cyber-attack, but discussed steps it took to protect the data and networks once the breach occurred. Simon (2016) provided data related to universities and ransomware, while providing mitigation strategies for post-secondary institutions to implement. Harris and Hammargren (2016) addressed vulnerabilities, and reported universities suffered financial loss from cyber-attacks, and an inability to protect personal data stored on their networks.

Diaz et al. (2017) reported changes to the law supported individuals due to universities inability to protect data as it looked for ways to secure data in the cloud. Anderson (2006) not only reported that management was responsible for protecting information, but the onus also fell on individuals. Therefore, educating the campus community to mitigate the damage of cyber-attacks and protect information was a strategic approach (Anderson, 2006). With the combination of the selected literature above, along with the remaining sources not discussed, the chosen information supports the research project.

Description of Literature Content for Seven Articles

Anderson. (2006). Effective management of information security and privacy.

Anderson (2006) discussed the importance of a strategic approach to find solutions when it comes to protecting systems and networks against cyber-attacks. Determining the methods of mitigating the risk of cyber-attack and identifying the most likely types of attack is relevant to my paper.

Quotes. “The list goes on, and no university seems immune to these attacks” (Anderson, 2006, p. 15). “Because no single person or group is aware of all the issues reported, the university risks not recognizing the magnitude of threats or responding appropriately” (Anderson, 2006, p. 17). “Unless the handling of security and privacy improves, universities can expect increasing incidents of privacy violation, potentially generating adverse publicity, loss of funding and lawsuits” (Anderson, 2006, p. 19). These quotes demonstrate how common cyber-attack is in the university environment, and the risks involved.

Biddle. (2017). Common types of cyberattacks in education and what we can learn from them.

According to a blog posted by Biddle (2017, October 6), the three common types of cyber-attacks that education facilities should be aware of are: ransomware, DDoS and phishing. This information will assist in identifying the most likely cyber-attacks a security department at post-secondary institutions could face as recent data about current cyber-crimes support.

Quotes. “However, because schools usually keep records of students’ and staffs’ health, financial and personal information, they have now become a one-stop shop” (Biddle, 2017, October 6) “Three of the most popular cyberattack strategies against educational institutions are ransom attacks, DDoS attacks, and phishing scams” (Biddle, 2017, October 6). “Each attack gives insight into how they must prioritize and protect their data and networks” (Biddle, 2017, October 6). Biddle (2017) clearly identified likely forms of cyber-attack in relation to educational institutions, which directly ties to the research topic of this paper.

Diaz et al. (2017). The risks and liability of governing board members to address cyber security risks in higher education.

The report written by Diaz et al. (2017) discussed the continuation of technology advancements and its affect on society. The technology may be a convenience but with that comes the risk of security breaches. There is now an increase in security breaches therefore making room for changes to the law for corporate negligence.

Quotes. "In light of these new world realities, officers and directors at all types of organizations, including colleges and universities, would be well advised to ensure that their organizations engage in a thoughtful process to implement adequate physical, electronic, and other security measures to prevent, manage, and respond to data breaches" (Diaz et al., 2017, p. 50). "Cyber security is no longer an afterthought for only a few information technology functions" (Diaz et al., 2017, p. 61). "The risks of cyber security incident cannot be entirely eliminated" (Diaz et al., 2017, p. 62).

Harris and Hammargren. (2016). Higher education's vulnerability to cyber attacks.

The report by Harris and Hammargren (2016) discussed the number of cyber-attacks to post-secondary institutions; addressed how to decrease the number of attacks, and that the lackadaisical approach was the reason for the financial burden.

Quotes. "…since 2005, higher education institutions have been the victim of 539 breaches involving nearly 13 million known records" (Harris & Hammargren, 2016, para 1). "In 2000, the Federal Trade Commission (the "Commission" or "FTC") promulgated its "Safeguards Rule." This rule, above all, directs institutions providing financial products or services to establish a comprehensive written information security program ("WISP") containing administrative, technical and physical safeguards to protect customers' personal information"

(Harris & Hammargren, 2016, para 2). “Higher education institutions, in particular, should consider focusing on developing and implementing a comprehensive WISP, given the industry’s current statistics for data breaches (Harris & Hammargren, 2016, para 17).

Park et al. (2001). Cryptographic salt: A countermeasure against denial of service attacks.

The scholarly article by Park et al. (2001) not only goes into detail about what DoS is, but provides information on how to recognize and mitigate it. Considering DoS is on the list as a top contender for cyber-attacks in 2017 leads me to question how cyber-criminals infecting devices with DoS have remained ahead of security specialists at post-secondary institutions since this is an old problem. Both DDoS and DoS are similar, however, DoS attacks typically use one computer and its connection to target a system or resource, whereas DDoS attacks use multiple computers and connections (Munson, 2011).

Quotes. “Recently, denial-of-service (DoS) attacks have become a growing concern as Internet services have been used in more aspects of human life” (Park et al., 2001, p. 334). “Authentication protocols themselves do not help prevent denial-of-service attacks but instead may give rise to another environment for denial-of-service attacks” (Park et al., 2001, p. 335). “Our new concept solves all these problems without minimal overhead because it requires no additional public-key operation” (Park et al., 2001, p. 342).

Polyakov, (2017). What cyberthreats do higher education institutions face?

Polyakov’s (2017) magazine article discusses how easy education networks are to access, what infects devices and networks, and how to mitigate cyber-attacks.

Quotes. “If a single device synced to campus network is infected, the whole IT landscape is likely to be affected” (Polyakov, 2017, para 5). “Attack vectors include almost everything from predictable malware or social engineering techniques to even attacks on university applications" (Polyakov, 2017, para 7). "Basic cybersecurity hygiene requires you to patch all your systems in a timely fashion, but there are two pitfalls. First, many system administrators are slow on installing patches. Another danger is that applying patches does not guarantee complete protection" (Polyakov, 2017, para 13).

Simon (2016). The rising face of cyber crime: Ransomware.

Simon (2016) has experience in cyber security and provided insight into ransomware and the impact this cyber-attack has on the educational industry.

Quotes. "Today's cyber criminals have evolved their approach using advanced strains of ransomware that encrypt data on an organization's network or lock users out of their devices" (Simon, 2016, p. 1). "Most ransomware attacks share a common trait: they begin with one seemingly benign email attachment opened by an employee" (Simon, 2016, p. 4). "According to Verizon, only three percent of individuals targeting with phishing emails actually alert management" (Simon, 2016, p. 6).

Critical Appraisal

Early Cyber-Attack Information

The first portion of my research was to search the history of cyber attacks to determine a timeline when attacks began and what types were occurring. Simon (2016) discusses only one specific cyber-attack, which was, ransomware, but the article is specific to educational institutions and provides a very early history to this type of attack. This article looks at early attacks where cyber criminals "were using floppy disks to spread ransomware attacks across computers" (Simon, 2016, p. 1). It shows just how long ago this type of attack first began and sets the stage for similar crime on the Internet today.

Park et al. (2001) discussed DoS attacks, and one type of attack in particular, which has been labeled a connection depletion attack or resource clogging attack due to the fact that it works to "initiate and leave unresolved a large number of connection requests to a Web server, exhausting its resources and rendering it incapable of servicing legitimate connection (or service) requests." (Park et al., 2001, p. 334). This type of attack leaves the server open for cyber-criminals to intentionally slow the relay of information to the person using the Internet site without knowledge an attack occurred (Park et al., 2001).

There are limitations to this article in that it is specific to one type of attack, but it is useful as it gives the reader a clear understanding of what DoS attacks can do, and the understanding that these attacks have been happening for many years. An understanding of DoS attacks here also helps the reader to better understand DDoS, which is discussed later on in the report. The paper will look at options to mitigate these attacks, including the use of *cookies* and *cryptographic puzzles* together as a preventative measure for an institution or person to understand and prevent DoS. "Cookies are pieces of information generated by a Web server and stored in the user(s) computer, ready for future access" (Park et al., 2001, p. 335). *Cryptographic salt* (p. 337) or a *cryptographic puzzle* (p. 336) is an encrypted message or number known to the server sending and receiving messages (Park et al., 2001). The articles from Park and Simon show that cyber-attacks have been ongoing for many years.

Current Cyber-Attacks

There appears to be an increase in cyber-attacks to all industries, including post-secondary institutions. Biddle (2017) and Polyakov (2017) discuss cyber-attacks respectively in relation to the current post-secondary environment, and Simon (2016) discusses the recent increase in the threat of ransomware to the educational environment. Although the blog by Biddle (2017) is not from a scholarly journal, research into her background has shown that she is an IT specialist with eleven (11) years of experience. The topic area is directly relevant to this research. It should be noted though, that her article does contain marketing of solutions to the stated cyber-crimes, therefore there may be some bias. In terms of defining types of attack I felt this was still a source that would provide a good understanding of what each type of attack could do. Simon's (2016) article is from an IT company's website. The company (BitSight) specializes in compiling technology data on security issues in order to help organizations manage risk. Although there is a risk that the data pulled for the article may not be fully verified, they use a patented network mapping process that mapped more than 54,000 companies. The report included data from different industries "For this study, we focused on six industries, analyzed of 18,996 organizations across Finance, Healthcare, Education, Energy/Utilities, Retail and Government" (Simon, 2016, p. 8). The data was considered likely to be reliable considering the reputation of the author. Furthermore, the data is relevant to the current market and provides a comparative to other industries. Polyakov (2017) has written a current article that discusses types of cyber threats in the higher education environment and is the co-founder of an IT company with expertise in security of enterprise business, critical software and industry specific solutions developed.

Biddle (2017) discussed three common attacks on education:

- Ransomware,
- Phishing, and
- DDoS.

Polyakov (2017) and Simon (2016) highlighted cyber-attacks likely to be present for universities:

- Malware/ransomware,
- Social Engineering Techniques (i.e. phishing), and
- Password Attacks on Applications.

Ransomware/Malware

Simon (2016) initially discussed the rise of ransomware which occurred in 1989 when cyber-criminals infected floppy disks with malware and then goes on to note that “More than 27 years later, ransomware is now a lucrative business for cyber criminals, with some experts estimating hackers earn over $90,000 per year through these attacks” (p. 1). Malware encrypts user files rendering them useless until ransom has been paid. Singh and Joshi (2016) discuss cyber issues and information security risk management in relation to the university environment and discuss how this environment is “vulnerable because of its large open networks” (p. 1). This type of environment can make attacks such as malware easier to carry out. This article is helpful to the research as it clearly discusses cyber-crime in the university environment, and it is a peer-reviewed article by authors with a Ph.D. and MA respectively in their chosen fields. The source data is from India, but as borders do not contain cyber-crimes, the information will still be relevant. The risk of an attack at any post-secondary institution is possible since even the University College London, known as the centre of excellence in researching cyber-crimes, was successfully attacked (Coughlan, 2017). It is as easy as clicking on an email attachment, downloading (known or unknown) attachment(s) and or having weaknesses in the software upgrades. Once the device(s) has been infected with Trojans, worms and or viruses, it is too late, since malware can go undetected until the cyber-criminal(s) request ransom (CBCN, 2017; Simon, 2016). CBCN (2017) and Polyakov (2017) report that universities have paid ransoms to regain access to data that was encrypted with malware by cyber-criminals such as the University of Calgary.

Distributed Denial of Service (DDoS)

DoS attacks previously discussed in the paper are attacks that are carried out using one computer and one network (Munson, 2011). A more sophisticated version of this type of attack is known as DDoS and this approach uses multiple networks and computers to carry out the attacks (Park et al., 2001; Polyakov, 2017). Cyber-criminals use DDoS maliciously to overwhelm a network, as well as in a non-malicious manner which still has a negative impact on operations where they increase the traffic for financial gain in processes such as data mining (Biddle, 2017). The key to mitigating these risks is early detection with increased firewalls and patches to regain control. Singh and Joshi (2016) discuss the Operational Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) framework that focuses on the weaknesses, understanding the high-risk areas and then discusses how to mitigate the risk(s) when a cyber-attack occurs.

Phishing

Phishing is an act used to steal personal information or to obtain access to a network in order to then start a different type of attack inside the network. A cyber-criminal sends an email with a link; the receiver clicks on the link and is requested to enter personal data. The link appears as though it is from a reputable and or known source, so the receiver enters his/her information, and the cyber-criminal has what they were looking for, i.e. access to systems or to personal information (Biddle, 2017). Phishing may lead to encryption of data and networks with malware. Therefore, phishing is a concern for security at post-secondary institutions (Singh & Joshi, 2016). Phishing can lead to exposure of personal records on secured networks that may lead to class action lawsuits. Harris and Hammargren (2016) discuss the fact that class action lawsuits, following data breaches, which can result from phishing attack(s), are becoming very common, and that large settlements are possible in relation to these suits. The article covers a discussion of higher education's risks in relation to cyber-attacks and is therefore directly relevant to the research topic. The authors (Harris and Hammargren) are both lawyers with significant experience in data security (2016).

Password Attacks on Applications

Another way cyber-criminals attempt to steal information is by using software programs designed purposefully to crack passwords/phrases. Unlike phishing, when the user provides his/her passwords/phrases to a believed legitimate website and organization, the cyber-criminals crack the code(s) and help themselves to information (Polyakov, 2017). A simple way to deter the loss of information is to change passwords frequently, never use the same password/phrase for multiple sites, and use multiple emails to stay ahead of the cyber-criminals.

Security Department Impact

None of the research articles specifically discussed the effects of the cyber-attacks noted in the section above in specific relation to security departments. However, it is possible to extrapolate from the information above the likely effect of each one on a security department in a post-secondary institution.

Ransomware could result in online systems no longer working – this could affect entry points into buildings, bring down security cameras and make it impossible to look up information for students who need help or who could be causing trouble. DDoS could have similar affects as a slowing of the system could result in delays to information processing and potentially errors with assisting people with building access. If alert systems for fire and other alarms are online, than it may be affected by ransomware and DDoS. Personnel in security departments could be vulnerable to phishing attacks due to lack of specific training, and this could result in data breaches (Neuman, 2009). If other departments have data stolen due to successful phishing attacks, the security department may be a focus point for calls from students, media and police depending on what the breach contains. Password attacks on applications could either take place in the security department itself, in which case the applications the department uses could be jeopardized, or if another department was affected and systems became compromised, this could involve the security department if the systems were important to campus access, cameras, alarm systems etc.

Other Potential Impacts / Factors

Another aspect of impact to post-secondary institutions is the financial cost of cyber-attacks. There is a cost to defend against cyber-attacks in terms of mitigation of risk and response to breaches. The financial burden could be even higher due to potential charges if the laws of institutions choose not to protect the data and networks from the criminals (CBCN, 2016; Coughlan, 2017; Harris & Hammargren, 2016; Hoffman, Rosenberg, Dodge & Ragsdale, 2005; McGinn, 2017). This is important to consider when looking at the impact to security in post-secondary institutions, and the reasons why universities provide open networks. Easy access to networks for those using the system(s) is convenience based. However, convenience comes at a cost when cyber-criminals gain access to information; hold information ransom, or sell information on the dark web. Institutions may have to pay for encryption methods to protect data, implement monitoring, hire consultants and possibly incur legal costs from lack of theft prevention, which is the cause of class action lawsuits due to personal information being exposed or stolen (Diaz et al., 2017; Harris & Hammargren, 2016; Simon, 2016). CTVN (2017) reported a student was charged when malware was found on 287 computers, which in turn, affected 3,323 users.

Young adults at University are very proactive when it comes to technological advancement and this has a significant impact on the types of cyber-attacks. The technological advancement led by young adults may contribute to cyber-attacks since the technology is advancing faster than the security features to protect against it (Singh & Joshi, 2016). Some upgraded devices may not have crucial security features and can be used on the open networks of universities, therefore, making the universities' networks more vulnerable to phishing, malware/ransomware and password attacks (Singh & Joshi, 2016).

Theoretical Reasoning

A theoretical viewpoint known as Routine Activity Theory (RAT) was originally applied to the criminality of physical crime, and is one of the main theories used in relation to cyber-crime. Although this is not the only theory, it is commonly referred to in relation to cyber-crime and provides a structure that can be used in this paper to help understand why these crimes happen. Leukfeldt and Yar (2016) discuss this theory to see if it does fit cyber-crimes such as the ones noted above, and in particular, common attacks such as malware. They look at the background of the RAT structure as follows:

> Considering each of the core elements of RAT's schema of the criminogenic situation (motivated offenders, suitable targets, and absence of capable guardians) testing them in terms of their applicability to the on-line environment. With respect to motivated offenders, these would appear to be in no short supply in the on-line environment—variously fraudsters, hackers, pirates, stalkers, and so on. Similarly, there are numerous targets suitable for predation—proprietary data, personal information, on-line payment and purchasing services, as well as computer systems themselves that may be compromised and disrupted by unauthorized intrusion and interference (Leukfeldt & Yar, 2016, pp. 264-265).

The study determined that aspects of the RAT fit while others did not. They note that one of the factors that most determined the likelihood of attack was just time spent online. This would suggest that this routine behavior did encourage more instances of attack. The study found though that other factors did not fit and that further research would be required to determine RAT's suitability to cyber-crime in general. (Luekfeldt & Yar, 2016). This is only one view of theory relating to cyber-crime and is therefore limited in its approach, but it has been used here to provide insight into potential reasons behind targeting attacks such as ransomware.

Discussion

Three Most-Likely Cyber-Attacks for Post-Secondary Institutions

After reviewing the literature in the critical analysis section above, and based on the descriptions of the types of attacks and their impacts, I have determined that the three most likely cyber-attacks on a post-secondary institution are Ransomware, DDoS and phishing. Ransomware is becoming an increasingly common occurrence in this environment (Simon, 2016), while phishing is often used to gain access to data, which is held in large amounts by post-secondary institutions. DDoS was included as the third because it is a common approach used by criminals to slow systems and has been around for a very long time and is also used by students who are unhappy with the school. (Simon, 2016; Biddle, 2017)

Mitigation Strategies

Framework. Diaz et al. (2017), Simon (2016), and Singh and Joshi (2016) discuss effective management strategies and frameworks to assist post-secondary institutions in the protection of data and networks. Singh and Joshi (2016) provide a framework for university risk management and security specialists to implement. Diaz et al. (2017) discuss the importance of having plans in place to mitigate open storage sites from cyber-attacks.

No matter the reasoning why cyber-criminals breach security systems, it has failed to stop at this time. Therefore, Singh and Joshi (2016) discuss mitigation strategy framework such as the one introduced by Carnegie Mellon University for post-secondary institutions. “The proposed model is based on the most popular risk frameworks in use today, OCTAVE (Operational Critical Threat, Asset, and Vulnerability Evaluation)” (Singh & Joshi, 2016, p. 744). This framework covers three areas of concern to measure the risk quantitatively. In order to mitigate the vulnerabilities within the system, security experts must first recognize the weakness, understand the highest risk areas and have a plan. "The proposed framework uses Common Vulnerability Scoring System (CVSS) to validate which vulnerabilities can be actively exploited" (Singh & Joshi, 2016, p. 744).

Neuman (2009) highlights not only the importance of protecting information such as Singh and Joshi (2016) recommend, but also the importance of protecting physical security from cyber-criminals. It was discussed that understanding the security measures for the physical-security aspect of a system provides insight to vulnerabilities worth considering (Neuman, 2009). Considering the physical side of cyber-crime is an important avenue for a security department. If cyber-criminals demand ransom before releasing controls to the university, there are safety measures affected until control has been regained. If networks and devices shutdown then security would lose control of emergency phone lines, emergency notification systems, controlled access, cameras, alarms and communication with the campus community.

Education. From past to present day, there is a trend to improve mitigation strategies to protect the vulnerable software, networks and information as security specialists attempt to stay one step ahead of cyber-criminals (Anderson, 2006; Diaz et al., 2017; Harris & Hammargren, 2016; Hoffman et al., 2005; Singh & Joshi, 2016). Security specialists recognize the importance of educating the people that use the post-secondary networks since many cyber-criminals access the institutions' networks as people open malicious emails, links and download programs (Polyakov, 2017; Simon, 2016). In a security department, this education would protect the systems directly in contact with employees. Having knowledge of the types of potential cyber-attacks and ways to avoid them would allow staff members to be proactive in their approach to emails, logons to systems and file transfers. Knowledge of attack types would also allow the department to better understand how to support the rest of campus in the case of shutdown or slowdown of systems due to ransomware or DDoS, and how to prepare for the possible shut down of emergency systems that they normally rely on.

Evaluation and Recommendations

The literature reviewed for the report had its high and low points. It was disturbing to learn that attack methods from the past such as DoS which used one device and one network then expanded to DDoS where multiple devices and networks can render networks useless and unprotected (Biddle, 2017; Park et al., 2001; Polyakov, 2017; Simon, 2016). Even when devices, networks and software programs have been updated properly, universities are not always successful in preventing the risk of a cyber-attack, which can leave information unprotected, and the institution open to financial loss (Harris & Hammargren, 2016). As we move into current day, those (not so) simple breaches that seemed more innocent in 2001 ballooned into opportunities for cyber-criminals today and became a lucrative business (Simon, 2016). To think, the Pentagon and the North Atlantic Treaty Organization (NATO) were breached in 2001 and the top university in cyber-crime studies was held ransom in 2017 (Coughlan, 2017; Yesberg & Henderson, 2001). This suggests that despite knowledge and mitigation strategies, data and operational systems are still not secure. As security specialists prepare for one type of cyber-attack, cyber-criminals are plotting new ideas on how to steal information, and this is made easy with advanced technology hitting the market before proper security measures can be implemented (Singh & Joshi, 2016).

Despite the issues noted above, there are ways to protect data from cyber-criminals and it requires people using devices and networks to be vigilant about what they open and download. Simon (2016) recommends having email security protocols in place and to train staff to be more suspicious of links sent in emails and report these emails immediately. Further suggestions include monitoring key stakeholders' devices for criminal activity, and avoiding peer-to-peer file sharing over networks (Simon, 2016).

In addition to the recommendations by Simon (2016), Singh and Joshi (2016) recommend understanding the weaknesses and upgrading networks on a regular basis, therefore being proactive instead of reactive. IT security should be aware of when users log in to high-risk areas of the university networks (Singh & Joshi, 2016). A further security measure would be to ensure the Uniform Resource Locator (URL) address is secure, and provide instructions on how to open links sent internally to eliminate opening malicious links accidentally, and in turn, exposing networks to cyber-criminals (Singh & Joshi, 2016).

Security specialists may not have been as valuable in the past as they are today; trying to remain one-step ahead of the cyber-criminals, protect networks, devices and data has never been so important as it is today (Simon, 2016; Smith, 2015). Creating strategic approaches and frameworks to mitigate the risk and vulnerabilities is a continuous cycle that assures security departments and institutions achieve secure networks (Anderson, 2006; Diaz et al., 2017; Singh & Joshi, 2016).

In order to assure information held within the institutions remains secure, security departments, through education and workshops, must continue to educate the basic users of the system and device vulnerabilities. Through education and workshops, the people using the system will learn protective ideas and gain knowledge related to personal development within the evolving computer world. Changing passwords regularly is extremely valuable, however, having strong passwords or better yet, pass-phrases is recommended (Anderson, 2006; Biddle, 2017; Hoffman et al., 2005; Simon, 2016; Singh & Joshi, 2016).

Institutions can set reminders for its users to change passwords and block users/sites. Providing users the information to understand the impact and what to look for before opening emails, links, social media accounts and or software program updates. Mistakes do happen so it is important to educate users on the next step to take if and when malicious attacks occur (Harris & Hammargren, 2016; Simon, 2016; Singh & Joshi, 2016).

Other than educating the users on what to look for and what to do if a cyber-attack occurred, it is essential to be proactive and update operating systems and programs regularly as discussed by authors of the research (Polyakov, 2017; Simon, 2016; Singh & Joshi, 2016). Updates provide patches to fix the weak and vulnerable areas cyber-criminals are searching for (Polyakov, 2017; Simon, 2016; Singh & Joshi, 2016).

Conclusion

Cyber-attacks have been an issue for many years and will continue to be a risk to all types of industry including post-secondary institutions and their security departments. This report reviewed literature for the purpose of determining the three most likely cyber-attacks that could affect security departments of a post-secondary institution, the potential impact of those attacks and ways in which the department could prevent or mitigate future risks. After reviewing the data, it was determined that security departments at universities are most likely to see attacks such as ransomware, DDoS and phishing. Each of these has the potential to slow down or stop campus services and activities or to result in a breach of campus body data. For a post-secondary institution security department, ransomware and DDoS could affect services such as phone access, campus door access, and emergency systems managed electronically. Phishing could be targeted towards anybody in the university and the security department is as vulnerable to these attacks as any other department. Phishing attacks could lead to access to security information.

Mitigation strategies would include educating and training all users of the security department networks and devices to therefore mitigate potential cyber-attacks. Regular updates to department software and patches to weakened areas could also mitigate the risk of these attacks. Security departments can remain current with cyber-attack news, and can ensure no email links are opened without knowing the source to prevent loss of physical security devices (e.g. emergency phones, alarms, access control, cameras, etc.) internally. Questions remain despite the research. How can a security department truly stay safe, or any department for that matter, when attacks are constantly evolving and technology is changing faster than the mitigation strategies? How can a university best determine where to spend precious funds when this is such a costly process? These are not easy questions to answer and in some ways this research has led to more questions than I had at the beginning.

References

Anderson, A. (2006). Effective management of information security and privacy. *Educause Quarterly* (1). 15-20. Retrieved from https://pdfs.semanticscholar.org/bbc7/dfbd1aff3e511049d61429199d2de245dc19.pdf

Biddle, S. (2017, October 6). Common types of cyberattacks in education and what we can learn from them. [Fortinetblog]. Retrieved from https://blog.fortinet.com/2017/10/06/common-types-of-cyberattacks-in-education-and-what-we-can-learn-from-them

Canadian Broadcast Corporation News. (2016, June 7). *University of Calgary paid $20K in ransomware attack*. Retrieved from http://www.cbc.ca/news/canada/calgary/university-calgary-ransomware-cyberattack-1.3620979

Canadian Television News. (2017, January 5). *Student charged in cyber attack on 304 computers at University of Alberta*. Retrieved from https://www.ctvnews.ca/canada/student-charged-in-cyber-attack-on-304-computers-at-university-of-alberta-1.3229502

Coughlan, S. (2017, June 15). *Top university under 'ransomware' cyber-attack*. BBC News. Retrieved from http://www.bbc.com/news/education-40288548

Diaz, L. J., Anderson, M. C., Wolak, J. T. & Opderbeck, D. (2017). The risks and liability of governing board members to address cyber security risks in higher education. 43(1) 49-75. *Journal of college and university law.* Rutgers Law School. Retrieved from http://jcul.law.rutgers.edu/2017/01/the-risks-and-liability-of-governing-board-members-to-address-cyber-security-risks-in-higher-education/

Harris, C. E. & Hammargren, L. R. (2016, September 6). Higher education's vulnerability to cyber attacks. *University Business* 8(16). Retrieved from https://www.universitybusiness.com/article/0816-wisp

Hoffman, L. J., Rosenberg, T., Dodge, R. & Ragsdale, D. (2005). Exploring a National cybersecurity exercise for universities. *IEEE Security & Privacy*. 3(5), 27-33. Retrieved from https://www.computer.org/csdl/mags/sp/2005/05/index.html

Leukfeldt, E. R. & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*. 37(3), 263-280. https://doi.org/10.1080/01639625.2015.1012409

McGinn, S. (2017, February 1). Universities must take steps to protect against ransomware attacks. *University Affairs.* Retrieved from https://www.universityaffairs.ca/news/news-article/universities-must-take-steps-protect-ransomware-attacks/

Munson, L. (2011, May 29). Denial of service versus disturbed denial of service – What is the difference? *Security – Frequently asked questions*. Retrieved from http://www.security-faqs.com/dos-vs-ddos-what-is-the-difference.html

Neuman, C. (2009). Challenges in security for cyber-physical systems. Center for computer systems security information sciences institute university of California. Retrieved from http://cimic.rutgers.edu/positionPapers/CPS-Neuman.pdf

Park, D. G., Kim, J. J., Boyd, C. & Dawson, E. (2001). Cryptographic salt: A countermeasure against denial of service attacks. In V. Varadharajan & Y. Mu (Eds.). (2001). Proceedings from ACISP 2001: *6th Australian Conference Information Security and Privacy*. Heidelberg: Springer-Verlag. (334-343). Retrieved from https://www.researchgate.net/profile/Willy_Susilo/publication/242499559_Information_Se curity_and_Privacy_13th_Australasian_Conference_ACISP_2008_Wollongong_Australia_July_7-9_2008_Proceedings/links/00b495314f3bcaaa46000000.pdf#page=344

Polyakov, A. (2017, August 21). What cyberthreats do higher education institutions face? *Forbes*. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2017/08/21/what-cyberthreats-do-higher-education-institutions-face/#67f8d96d640d

Simon, N. (2016). The rising face of cyber crime: Ransomware. Bitsight. Retrieved from https://info.bitsighttech.com/bitsight-insights-ransomware?hsCtaTracking=7dce0bd9-bf5d-456c-ab5e-134a1e47cb7d%7Cd54507aa-4e0d-42d3-9d81-b726f0a0f783

Singh, U. K. & Joshi, C. (2016). Information security risk management framework for university computing environment. *International Journal of Network Security*. 19(5), 742-751. Retrieved from http://ijns.femto.com.tw/contents/ijns-v19-n5/ijns-2017-v19-n5-p742-751.pdf

Smith, D. F. (2015, September 23). Putting 2015's higher education cyberattacks into perspective. *EdTech.* Retrieved from https://edtechmagazine.com/higher/article/2015/09/putting-2015-s-higher-education-cyberattacks-perspective

Yesberg, J. & Henderson, M. (2001). Applications of trusted review to information security. In V. Varadharajan & Y. Mu (Eds.). (2001). Proceedings from ACISP 2001: *6th Australian Conference Information Security and Privacy*. Heidelberg: Springer-Verlag. (305-319). Retrieved from https://www.researchgate.net/profile/Willy_Susilo/publication/242499559_Information_Security_and_Privacy_13th_Australasian_Conference_ACISP_2008_Wollongong_Australia_July_7-9_2008_Proceedings/links/00b495314f3bcaaa46000000.pdf#page=315