Akeem N. Campbell

School of Computing and Information Technology, University of Technology, Jamaica

Literature Review

March 24, 2023

The Investigation of Cyber-Crime and Mitigation Strategies in Jamaica

Introduction

In today's business world, Disruptive innovations such as cloud computing, social computing, and next-generation mobile computing are radically transforming how businesses use information technology to share information and perform business digitally. Since more than 80% of all commercial transactions are now conducted electronically, this area necessitated a high level of protection to ensure transparent and efficient transactions (Allodi, 2017). Cybersecurity encompasses not just the security of IT applications within the enterprise, but also the wider digital networks on which they depend, such as cyberspace and sensitive infrastructures (Rahman, 2020). People's care and choices when setting up, maintaining, and using computers and the Internet are critical to cyber security. Protecting both hardware and software of information are confidential and personal and technology services against unwanted access obtained by technical means encapsulates the essence of cybersecurity (Software Technologies LTD).

Cybersecurity is critical to the advancement of information technology and Internet services. According to Allodi (2017), improving cyber security and safeguarding sensitive data infrastructures are critical to every nation's security and economic well-being. Cyber technologies have grown in importance in all aspects of human life, including trade, banking, health care, energy, culture, communications, and national defense. Latest research findings indicate that public anxiety over privacy and personal information has grown since 2006 to Allodi (2017), internet users are afraid that they give up so much personal information and wish to be forgotten because there are no compelling excuses to maintain it.

This literature review is organized into themes and will explain in detail how to reduce cybersecurity risks, cybercrime threats, common cyber-attacks, attack phases, factors contributing to this rise, the impact of these cyberattacks, and countermeasures.

Themes related to papers used

1. **The need for Cyber Security in Today's Society**

The twenty-first century culture has embraced computers and the information revolution at a breakneck pace. We are rarely ever more than a few feet away from a computer or computing device in our everyday lives. Computers are embedded everywhere, from the vehicles we drive and the traffic lights we observe, to the power and water utilities we use every day, even though we might not be conscious of such facts (Rahman, Sairi, Zizi & Khalid, 2020). Society has endorsed program automation's reliability to the point that we now rely on its security and legitimacy for most of our daily activities. Unfortunately, as the early hacker community discovered, the way a machine was programmed to work and how it really operates are seldom the same. And what began as a harmless underground pastime has developed into a multibillion-dollar cybercrime industry.

Cybersecurity is described as the operation, mechanism, capacity, or state of protecting and defending information and communications networks and the data they contain from destruction, unauthorized use or alteration, or exploitation (Rahman, Sairi, Zizi & Khalid, 2020). Cybercrime that targets people's online privacy and welfare may have real-world consequences for their reputations, work protection, identities, and finances.Although this is becoming more widely recognized and appreciated, the general public frequently overlooks the physical dependence of computers and the internet. Our power plants, trucks, drainage systems, and gas

stations are all computer-controlled, and cybercrime aimed at these systems has the potential to affect large segments of society, if not entire countries (Esteves, 2017). Defending our critical infrastructure (financial markets, utilities, hospitals, administration, and transportation) from cybercriminal attacks is thus a national imperative, one that, as we can see, requires international collaboration.

The management of risk to information systems is considered fundamental to effective cybersecurity. Threats (who is attacking), vulnerabilities (weaknesses they are exploiting), and impacts (what the attack does) all influence the risks associated with an attack (Esteves, 2017). Typically, reducing those threats entails removing the threat(s), repairing vulnerabilities, and mitigating their consequences. As a result, cyber security is critical because it protects privacy and avoids unwanted surveillance, and knowledge exchange and intelligence gathering can be useful tools for achieving cybersecurity.

2. Reducing Cyber Security Risks

As the world becomes more technologically advanced, the number of security threats and risks will start to rise (Allodi, 2017). Cybercriminals are becoming more advanced in how they exploit technology, making it arduous to eliminate risks. Cyber-attacks can target either technological infrastructure in the form of malware and viruses, or human personnel through social engineering and cyber bullying tactics(Wang et al., 2020).

2.1 Role of Social Engineering in Cyber Attacks

Social Engineering (Human Hacking) is the use of deception to manipulate individuals into disclosing confidential or personal information which can then be used to obtain access to

networks, accounts, and other systems for malicious purposes (Jefferson, 2020).. Individuals and organizations are now more than ever vulnerable to social engineering attacks. The surge in cybercriminal attacks has generally been defined by the rise in social engineering attacks. Some of the fastest-growing corporate crime threats have recently shifted their attention away from exploiting technologies or vulnerabilities in information security and started focusing on human beings, which are considered to be the weakest link within every organization (Wang et al., 2020).

2.2 Employee Awareness Training

Regardless of the size or scope of an organization, the employees are said to be a company's primary vulnerability. Companies consider innovative ways to involve and inspire employees to proactively contribute to your cyber protection to minimize the danger they pose to the company's security. According to Wang et al., (2020), one of the most effective ways to reduce an organization's exposure to cybercrime threats is through employee preparation. Employees of a company that stores data or conducts operations online should go through and complete security training programs on a regular basis.This can be carried out by creating a cyber security strategy and enforcement plan that educates and encourages staff at all levels of the organization, to understand and follow security best practices.

2.3 Cyber Security Investment

Companies should invest in the education of their staff as continuous employee education contributes to a drastic reduction in the efficacy of social engineering attacks, reducing information systems, network vulnerability, and the risk of other cyber threats within their organization (Wang et al., 2020). This form of cybersecurity awareness through education and training often involves considerable time and financial commitment, though the benefits and the enhanced degree of protection it brings forth is invaluable.

Losses as a result of cyber-criminal attacks may take several different ways, and many aspects of an enterprise can be impacted. To combat these threats, it is important for companies and individuals to adapt their cyber security investment or budgets depending on the different forms of possible attacks (Esteves, 2017). While it is critical to protect one's business by implementing a cyber defense system to counter cybercrime and ensure that the company's objectives are achieved, it may not be as successful as it should be (Kshetri, 2021).. As a result, before agreeing to incorporate a cyber defense program, an organization must first know how to execute a thorough evaluation to identify their needs and level of safety required against specific cyber-attacks.

It is widely acknowledged that cyber-attacks have varying degrees of negative effects on organizational efficiency, with financial implications. There are also several types of defense technologies that can be used to solve these concerns (Kshetri, 2021). Therefore, the type of comprehensive evaluation required is one that involves being educated on the types of cybercriminals as well as the various forms of cyber-attacks to which the organization or individual is most susceptible for the organization to better determine the best type of cyber

security infrastructure(s) to integrate that will provide them with the utmost protection. (Aldawood & Skinner, 2018).

3. Threats to Cybercrime

Threats to cyber security can be roughly divided into two general categories - cyber-attacks and cyber exploitation Kshetri (2021) and Schneier (2020). Cyber-attacks are actions aimed at and intended to damage or destroy cyber systems and cyber exploitation are actions that seek to exploit the cyberinfrastructure for unlawful or harmful purposes without damaging or compromising that infrastructure (Jefferson, 2020).

3.1 Common cyber attacks

A cyber-attack is an intrusion by cyber criminals using one or more machines against a single or more computers or networks. A cyber-attack will maliciously disable computers, steal data, or use a broken computer as a starting point for other attacks (Software Technologies LTD). Cyber criminals employ a range of tactics to conduct cyber-attacks, including malware, phishing, ransomware, denial of service, and more (Software Technologies LTD). Studies show that the four (4) most common cyber-attacks are Malware, Phishing, Man-in-the-middle attack and Distributed Denial-of-Service (DDoS) attack (Jefferson, 2020).

3.2 Phases of a cyber attack

In order for organizations to have a ‘head start’ from cyber-attacks, it would be of great importance to gain awareness on the various phases of an attack, as well as to uncover the strategies of a hacker (Ramalho, 2017). Ramalho (2017) brought together 23 experienced

hackers and made observations on their work. In his observation, he discovered that the hackers went through a series of stages to perform a successful attack (Esteves et al, 2017).

Phase 1 identifies the vulnerabilities. If a hacker feels that an individual/organization is worth hacking, he or she will closely investigate the vulnerabilities, analyze security protocols, and perform other required analysis (Ramalho, 2017). Companies can protect themselves by incorporating an iterative and flexible approach by conducting a high-level “footprint” on their systems on a periodic basis. Phase two is scanning and testing. When a hacker gains network access, bugs in programs running on some devices can be exploited to gain additional unauthorized access. Check your network for potential vulnerabilities to protect your company (Esteves et al, 2017).

The third phase is to obtain entry. Hackers often use both specialized technical knowledge and social skills at work. Possible claimants should take this into account (Conteh, 2016). Phase 4 is the Maintenance of Entry. Hackers seek to maintain "ownership" of the program in order to gain access to it in the future. As a result, organizations must monitor unusual activity in server logs. (2017) Esteves et al. Although hackers are very professional and dedicated about what they do, companies try their hardest to be 'a step forward' in protecting their businesses.

4. Factors contributing to the rise in cybercrime

According to Kshetri (2021) and Schneier (2020), the factors causing the rise in cybercrimes are multifaceted and complex. COVID-19 is a major factor contributing to the rise in cybercrime. Organizations have adopted remote work, making them rely on digital technologies, resulting in new vulnerabilities that cybercriminals can exploit. The increase in sophistication and the rapid technological developments leading to new attack methods have also been identified as key factors (Borgolte et al., 2020). According to Wang et al. (2020), vulnerabilities within organizations' cybersecurity measures, such as outdated software and weak passwords, have further contributed to the rise in cybercrimes.

The literature reviewed provided relevant information concerning our research topic regarding the challenges an organization faces when dealing with cyber threats. They also provided the emerging challenges involved in securing the Internet of Things (IoT) ecosystem. Finally, they also provided insights into the security behavior of employees in an organization with the need for effective training of employees.

4.1 Impact of Cybercrime on organizations

The consequences associated with cybercrime on organizations can be severe and far-reaching. According to Bhattacharjee and Sengupta (2020), the most common impact of cyberattacks on organizations is financial losses attributed to the theft of funds, the cost of responding to and recovering from attacks, and the loss of revenue resulting from system downtime. Reputational damage is another consequence, as this damages customer trust in the organization and can potentially cause a long-term impact (Kshetri, 2021). Organizations could be exposed to legal and regulatory actions resulting from the occurrence of a cyber-attack

(Mokhtar et al., 2021). The research studies greatly contribute to our research domain. They have provided a comprehensive discussion of the cyber threats that organizations face and their consequences.

4.2 Ways to Combat Cybercrime

To deal with the rise in cyber-attacks, organizations can adopt various robust cybersecurity strategies, which include the implementation of antivirus software, firewall, and encryption methods that can protect them against cyber-attacks (Borgolte et al., 2020). According to (Wang et al., 2020) design of compressive training programs regarding cybersecurity for employees also plays a critical role in the fight against cybercrime. Additionally, developing an effective response plan is critical in responding to and recovering from cyber-attacks; this includes procedures for identifying and containing the attacks, notifying relevant parties, and restoring systems and data (Bhattacharjee & Sengupta, 2020). According to Schneier (2020), regular security assessments can also assist organizations in identifying vulnerabilities and gaps in their cybersecurity measures, allowing them to take the necessary steps to address them.

The literature work review discusses the security risks associated with remote work and the need for the implementation of effective cybersecurity measures for the protection of the systems and data. Since most organizations have adopted remote work, the same for organizations in Jamaica, this information is relevant to our research study.

Overall, the reviewed literature provided important information for our research domain. However, they have also revealed that there are still gaps in the cybersecurity knowledge base. For instance, there is a lack of knowledge on the relationship between the various factors

contributing to cybercrimes. There is a need to carry out more research regarding effective ways of tackling cybercrime, especially regarding small and medium enterprises (SMEs).

Concluding Remarks/ Summary

To summarize, while technology can help mitigate the effects of social engineering attacks, the vulnerability lies in human behavior, instincts, and psychological predispositions. Exploitation costs are aligned with or higher than those in 'legitimate' insecure economies, making it easier to work to find causes for sensitivity to responsible risk and to attack economics.

Cybersecurity is important as it can safeguard privacy and deter intrusive surveillance, and information sharing and intelligence gathering can be useful tools to achieve cybersecurityIf organizations wish to reduce the risk of cyber-attacks, they need to understand the mindset of the hacker and the role that technology plays in facilitating offenders. Cybercriminals can be placed in a variety of categories depending on their goals/intent and skillset. However, one thing that most hackers have in common is the fact that they all try to go through four similar phases. In order for individuals/organizations to be a step ahead of cyber-attacks/criminals, one would need to be aware of the different stages of attack as well as to discover the hacker's strategies.

References

Allodi, L. (2017). Economic Factors of Vulnerability Trade and Exploitation. *ArXiv (Cornell University)*. https://doi.org/10.1145/3133956.3133960

Aldawood, H., & Skinner, G. (2018). Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. *IEEE International Conference on Teaching, Assessment, and Learning for Engineering*. https://doi.org/10.1109/tale.2018.8615162

Bhattacharjee, S., & Sengupta, S. (2020). Cybercrime: An analysis of its impact on business. Journal of Risk and Financial Management, 13(9), 205. https://doi.org/10.3390/jrfm13090205

Borgolte, K., Buechner, N. J., & Lechner, U. (2020). Cybersecurity challenges: Prevention, detection, and response. Journal of Business Research, 116, 176-185. https://doi.org/10.1016/j.jbusres.2020.03.025

Esteves, J. (2017, March 6). *To Improve Cybersecurity, Think Like a Hacker*. MIT Sloan Review. https://sloanreview.mit.edu/article/to-improve-cybersecurity-think-like-a-hacker/

Jefferson, B. (2023, March 16). *15 Common Types of Cyber Attacks and How to Mitigate Them*. Lepide Blog: A Guide to IT Security, Compliance and IT Operations. https://www.lepide.com/blog/the-15-most-common-types-of-cyber-attacks/

Kshetri, N. (2021). Cybersecurity of the internet of things ecosystem: Recent developments and emerging challenges. International Journal of Information Management, 56, 102199. https://doi.org/10.1016/j.ijinfomgt.2020.102199

Mokhtar, M. A., Alsaadi, E. A., & Alshaikh, M. A. (2021). Cybersecurity threats and measures: A survey of SMEs in Saudi Arabia. Journal of Cybersecurity, 7(1), tyaa013. https://doi.org/10.1093/cybsec/tyaa013

Schneier, B. (2020). The security risks of remote work. Communications of the ACM, 63(10), 15–17. https://doi.org/10.1145/3413522

Habte, F. (2022, May 26). *What is a Cyber Attack?* Check Point Software. https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/

Rahman, N. a. A., Sairi, I. H., Zizi, N. a. M., & Khalid, F. (2020). The Importance of Cybersecurity Education in School. *International Journal of Information and Education Technology*, *10*(5), 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393

Wang, Y., Tang, J., & Liu, X. (2020). Employee cybersecurity behavior in organizations: A review and research agenda. Journal of Organizational Behavior, 41(7), 613-633. https://doi.org/10.1002/job.2455