**Cybersecurity Measures**

Lucy Mills

Colorado State University, Global

ITS 415 - Principles of Cyber Security

Steve Choyce

October 2, 2022

**Introduction**

Innovative cybersecurity approaches are necessary to protect establishments’ intellectual property from threats online; keeping all personnel educated on their organization’s policies for avoiding, preparing for, and experiencing a cyber-attack is vital for reducing the time to recover data and patch the bugs that led to the attack. Recovering from an incident can cost a corporation thousands of dollars in stolen data, loss of sales, fines, and increased expenses; not to mention, commercial partners and clients can become dissatisfied to the point of taking their business elsewhere. Overall, avoiding incidents and mitigating incidents at the first opportunity, supports organizations in maintaining operations and commerce as usual. Identifying the underlying vulnerabilities of a corporation’s system can help it in better avoiding cyber-attacks; for instance, the system’s specific hardware and software vulnerabilities will determine the security techniques that should be implemented. Fundamentally, there are several cybersecurity challenges that all corporations have to face including finding a solid security basis, defending against advanced hackers, finding a collaboration source for security programmers, and hiring quality security professionals (IBM, 2015). In specific cases, companies also have to aware of how they respond to an attack, like a ransomware attack, as it can set ethical implications to related parties. With appropriate cybersecurity policies and procedures set in place, all members of an organization should know how to correctly handle any kind of attack or incident affecting proprietary data.

**Hardware Vulnerabilities**

When trying to make a corporation’s system more secure through different cybersecurity methods, understanding the existing hardware and its potential vulnerabilities can help exponentially in safeguarding the system in the exact ways required. There are many pieces of hardware involved in a corporate system that have to be accounted for with their pre-existing limitations. Consideration has to be taken to each piece in a system’s hardware as certain parts of the device could be infected with insidious malware or be outdated to the point of being incapable of completing advanced tasks. For instance, a Trojan circuit could be added to a device during one of the phases in the processor manufacturing chain, which can cause an attack at any point in time once being used; Trojan circuits have been maliciously modified by an overseas attacker to give them special privileges on the device (Das, 2012). Lastly, the amount of memory currently available on a system needs to be calculated before executing intensive applications to avoid a buffer overflow.

Every aspect of corporate devices’ hardware should be taken into consideration because each piece of hardware, i.e., monitor, keyboard, mouse, has “limited number of memory locations” on a system that have to be protected to keep threats from gaining access to vital system functions (Das, 2012). Additionally, recent research has shown that hackers are able to remotely “extract secret cryptographic data” off of microprocessors in the CPUs from various companies; script kiddies are able to perform this attack by using the amount of power being used by the microprocessor to process encrypted values (Goodin, 2022). Because integrated circuits/ microchips (IC) can be unreliable as some are infected with malicious programs capable of stealing intellectual property, rendering them ‘trojan circuits’, there are methods for computer engineers to tests the authenticity of the circuit, such as the silicon design verification (Das, 2012). A buffer overflow is one of the most commonly exploited susceptibility because an attacker can easily use it to get around a system’s security. Corporations should implore their programmers to constantly check their device’s memory limitations and keep up with proper programming practices like checking boundaries, validating user input, and adding catch statements where applicable in order to avoid a buffer overflow from occurring on the system (Das, 2012).

**Software Vulnerabilities**

Malicious hackers are able to take advantage of a software’s vulnerabilities to conduct illegal activity on personal and corporate systems, making cybersecurity increasingly valuable today. Threats online are constantly evolving at becoming better at finding small bugs in an application’s software, giving them access to an organization’s data before being patched. Of course, millions of different cyber-attacks occurred in 2021, but according to the Cybersecurity and Infrastructure Security Agency, the top vulnerability that year was the “Log4Shell” that affected Java’s utility library, Apache Log4j (2021). Through this vulnerability, actors were able to fully control another user’s system through a remote code execution, which allowed them to steal personal files and data, download ransomware, and pursue other illegal actions. Additionally, the Microsoft Exchange Server had multiple occurrences of criminal actors exploiting a vulnerability chain to hack into users’ emails via ProxyShells and ProxyLogons; the actors were able to gain access to the credentials of user’s comprising many accounts (CISA, 2021).

To defend against exploitations that lead to the loss of a corporation’s intellectual property online, there are several mitigation techniques that can be implemented. Primarily, the CISA recommends for personal and corporate systems to have updated applications and software, uninstalled all end-of-life software, and incorporated a centralized patch management system (2021). To make a malware/ ransomware attack less formidable, users can prepare against potential attacks by taking frequent cybersecurity precautions. For example, a ransomware attack is less intimidating to a user if all of the files being saved on the device’s hardware have already backed up to a secondary storage application online (National, 2020). Avoiding malware all together is the preferred method for keeping a system secure; a user can do this by cautiously opening received emails and files, blocking malicious webpages, inspecting proxies, using security gateways online, and employing signatures for blocking malicious code (National, 2020). In conclusion, all members at an organization have to be proactive on their system with all downloaded software and applications as well as interactions online to defend against an attack by a malicious actor.

**Fundamental Challenges to Cybersecurity**

Of course, there are new challenges arising in cybersecurity all the time with thousands of hackers collaborating and creating new types of attacks, but according to IBM, there are four primary challenges that all organizations have to face (2015). To begin, maintaining a defensive cybersecurity strategy can be much more challenging than most organizations anticipate it to be. Having a secure system requires more than one simple cybersecurity tool, rather it needs to be fundamentally secure through prompt patch management, monitoring the activity of privileged users, and speaking with company stakeholders about identified risks. Keeping up with all of these individual aspects of a company’s security requires more time attention, but this is ultimately the best method for keeping data secure. Next, hackers have become so insanely advanced and numerous because they are largely based out of organized crime rings based off the dark web, making them as profitable and accomplished as renowned corporations. What used to be considered adequate protection from hackers online, like firewalls and antivirus software, now is not nearly sufficient enough to protect a system from breaches. To keep threats at bay, users should perform network and data analytics and check for anomalies in network/ data traffic to detect malware; if a security incident is detected, it needs to be dissipated as quickly as possible to lessen its effects. Furthermore, hackers have more online resources that allow them to collaborate with each other than defensive cybersecurity programmers have. The publication of previous incidents and emerging threats online is severely lacking, leaving programmers who could benefit from this information empty-handed. To help bring more knowledge to this field, IBM released the ‘X-Force Exchange’ as a threat intelligence network in 2015, which openly published information about real threats and attacks from over a thousand organizations. To finish, the cybersecurity skills gap is preventing organizations from being able to find security professionals to hire, which is allowing the number of hackers to outnumber the number of active security programmers. Many companies are turning to universities to train students in security early, increasing the vitality of the cybersecurity workforce. With increased resources and training available for security programmers, the defense against hackers is becoming stronger.

**Ethical Issues Associated with Ransomware**

Ransomware has evolved to become one of the malignant cybersecurity attacks as these attacks usually target their victim and are costly to manage. As these attacks are very prevalent today, all companies have to create a strategy for dealing with the unknown actor; there are some ethical dilemmas involved in resolving ransomware. For instance, a company engaging with or paying the threat either directly or through cyber insurance can give it the reputation of being a ‘paying entity’, making it a more susceptible target for future attacks (Sumner & Simmons, 2019). Every organization needs a detailed incident response plan that includes how to respond to a ransom demand; this should start with notifying the company’s legal department to receive advice on the best procedure for navigating the incident. If the organization’s insurance policy covers the ransom payment, then the insurance company will be contacted to initiate the payment process. However, paying ransom hackers can ultimately be a bad decision for a company to make; for instance, the reputation of the company is damaged, certain legal ramifications can occur, and all the money spent just goes to fueling the hacker to pursue further criminal attacks online. Moreover, the FBI even advocates against paying ransoms as it does “not guarantee access to or the deletion of the stolen data” (Sumner & Simmons, 2019). Some constitute paying ransom actors to be funding criminal, terrorist, and rogue state groups adding another reason to not pay during these attacks. While it may seem like an easy solution to a company to just pay the ransom to resume normal operations, giving money to an attacker violates both legal and ethical principles making it a poor decision for a company to make.

**Conclusion**

Through examining many aspects of cybersecurity, it has been made clear that companies should focus on fundamental security aspects and procedures to best defend themselves from a data breach by an unknown actor. Checking that the system’s hardware is both untampered and capable for a corporate workload can ensure that there are no physical issues with any devices at the company. Keeping the software on corporate computers updated, remaining aware of common attacks, and having quality patch management are all techniques for addressing possible software vulnerabilities. Many of the fundamental issues in cybersecurity can be resolved by diligently keeping up with the basic elements of the system. Resolving a ransomware attack can be stressful for an organization, but with an excellent incident response document all employees will know how to best end the incident without paying the actor. Once an organization has the necessary preparations in place, resolving an incident is made much simpler for everyone involved.

**References**

CISA. (2021). *2021 Top Routinely Exploited Vulnerabilities | CISA*. Cybersecurity and Infrastructure Security Agency. <https://www.cisa.gov/uscert/ncas/alerts/aa22-117a>

Das, S. K., Kant, K., & Zhang, N. (2012). *Handbook on Securing Cyber-Physical Critical Infrastructure* (1st ed.). Morgan Kaufmann. <https://www2.seas.gwu.edu/~simha/research/HWSecBookChapter12.pdf>

Goodin, D. (2022, June 14). *A new vulnerability in Intel and AMD CPUs lets hackers steal encryption keys*. Ars Technica. <https://arstechnica.com/information-technology/2022/06/researchers-exploit-new-intel-and-amd-cpu-flaw-to-steal-encryption-keys/?comments=1>

IBM. (2015). *Four Big Cyber Security Challenges (And How To Overcome Them)*. Forbes. <https://www.forbes.com/sites/ibm/2015/05/14/four-big-cyber-security-challenges-and-how-to-overcome-them/?sh=7fc234795867>

National Cyber Security Centre. (2020). *Mitigating malware and ransomware attacks.* <https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks>

Sumner, P., & Simons, J. (2019). *Ethical, Legal Implications of Paying Ransoms (Updated)*. National Defense. <https://www.nationaldefensemagazine.org/articles/2021/8/17/ethical-legal-implications-of-paying-ransoms>