Brandon Burke

ENGL 211C

Prof. Perriello

April 21, 2023

Cybersecurity: Imperative Measures

In today's digital era, personal data is vulnerable to cyber threats, making it necessary to implement strategies to protect this data. Cybercriminals are becoming more sophisticated and proficient at targeting personal data, and they are using advanced techniques to bypass the security measures. It is crucial to ensure personal data protection in a constantly evolving technological landscape. Cyber threats are diverse and ever-evolving. They can range from malware and phishing attacks to ransomware and denial of service attacks. The general population is unaware of the security issues surrounding everyday technology use. At the minimum, people, companies, and governments should be working towards understanding the cyber threat landscape to develop effective strategies to protect personal data such as strong passwords, multi-factor authentication, zero trust, encryption, and cybersecurity training.

In 1967, ARPANET was developed to try to connect computers together. ARPANET was the precursor to the internet. The first computer would connect to the network in 1969. Just a few years later in 1971, a proof of concept malware dubbed “The Creeper” was developed. It would display a message to all computers connected to the ARPANET. The message would say, “I'm the creeper, catch me if you can!” (Saengphaibul). This would be known as one of the first examples of computer malware that was created. This is important because it would lead to the creation of black hat, gray hat, and white hat hackers. According to Doug Bonderud, “the stereotypical bad guys” are black hat hackers, since they “compromise and infiltrate systems to

cause harm or steal data." Gray hat hackers "often have good intentions but operate outside the legal frameworks that govern IT security." White hat hackers work for the law or companies to find vulnerabilities. These vulnerabilities are then patched to protect systems from attacks from black hat hackers. White hat and black hat hackers are in a constant cyber information war. The job of a white hat is to thwart attacks, while black hats try to steal information for profit. PII or personally identifiable information is stored in SQL databases that organizations and governments own. The data is often sold on forums that are specifically designed to host files from a data breach. One such website was called BreachedForums. The FBI seized the domain and servers running the website and arrested the owner of the website (Gatlan). Most data breaches occur because of flaws in a company's or government's operational security.

Operational security, also known as OPSEC, is a term used by company and government bodies to put measures in place to protect critical information and information systems. Even though organizations and governments vary levels of security in place, this is not always the case. Companies and governments get compromised on a daily basis. For example, ABC News reported that "Jack Teixeira, a 21-year-old airman in the Massachusetts Air National Guard, allegedly posted documents as early as December in a private Discord server" (Zahn). The leaked documents would later spread to more public social media platforms such as Twitter and 4chan. This shows a data permission violation in the United States military database. Jack Teixeria was able to get his hands on classified information either by himself or through higher authorities, which indicates an insider threat that was not properly secured. If Jack was able to get his hands on confidential information, this indicates that the data was not properly secured with encryption, multi-factor authentication, and no enforcement of a zero trust policy. In 2016, a popular Minecraft server's database was hacked. The server stored over 7 million emails and

passwords in a hashing algorithm called MD5 (Cox). MD5 has been outdated and compromised since December 31, 2008. The server's database also had a lack of encryption of user data, which allowed attackers to get all user passwords relatively quickly. This shows that company and server owners do not have sophisticated measures in place to prevent attacks that expose customer and player data. In addition to the lack of security measures in governments and companies, many individual people do not use strong passwords and multi-factor authentication on their accounts. According to Karola Marky, many people believe that "2FA [or MFA] mechanisms usually exhibit user experience issues that create user friction and even lead to poor acceptance, hampering the wider spread of 2FA [or MFA]" (1). In other words, many believe that multi-factor authentication can hinder productivity and is more of an annoyance rather than a crucial security measure. Missing the step often leads to brute force attacks and eventual account hijacking. The same can be said with user passwords. Many users frequently use passwords that are easy to remember. Once a user memorizes a specific password, they begin to use the same password on multiple devices and accounts. If one account or device gets compromised, this leads to other devices and accounts being indirectly compromised without a user's knowledge. However, there are simple steps companies, governments, and individuals can use to mitigate or prevent black hat hackers from accessing personal and confidential information for the public to view.

Password protection is the first and most straightforward step to protect personal data. Passwords should be complex and unique, consisting of upper and lowercase letters, numbers, and symbols. Passwords should also be changed regularly, ideally every 90 days. Passwords or keys are a form of authentication into an account or service. It is important to have a strong password to prevent account or service hijacking. Passwords should include the following:

> At least 12 characters long, but 14 or more is better. A combination of uppercase letters, lowercase letters, numbers, and symbols. Not a word that can be found in a dictionary or the name of a person, character, product, or organization. Significantly different from your previous passwords. Easy for you to remember but difficult for others to guess. Consider using a memorable phrase like "6MonkeysRLooking^" (Microsoft).

In addition to the parameters above, securing passwords is just as significant as never sharing passwords with anyone and using multi-factor authentication. Password managers are also recommended. A password manager is an application or service that stores user passwords in a salted and encrypted format ("What Is a Password Manager?"). A user only has to memorize one password to access the vault of passwords for various other applications and accounts. Admittedly, password managers have been hacked in the past, leading to compromised passwords. However, most password manager companies such as Bitwarden store user passwords in a salted and encrypted format, which makes it nearly impossible for malicious actors to access the stolen information. The main benefits of a password manager are auto-generated passwords, little memorization, and alerts of data breach ("What Is a Password Manager?"). Strong passwords can also be coupled with multi-factor authentication to harden any account or service from malevolent actors.

Multi-factor authentication consists of three groups: something you know, something you are, and something you have. In order for multi-factor authentication to occur, "factors from two groups are combined to form an authentication mechanism" (Marky et al. 2). Multi-factor authentication or MFA works by sending a password and a text message or using an authentication app. This means that users have to provide two or more forms of authentication to

access an account or services, thus protecting confidential information. For instance, WordPress is the world's most popular website building and hosting platform. People host ecommerce and personal portfolios sites to promote themselves. Because of the popularity, malicious attackers constantly attack WordPress sites by exploiting website plugins, code, and login pages. Exploiting code on a WordPress site is significantly harder than launching a brute force attack against a login page. Without MFA configured on the website, an attacker could launch bots to try various combinations of usernames and passwords. MFA can also be used on databases which house the most important data for a company and government. Database information can include payroll, student information, employee information, and secret documents. MFA on a database significantly increases the security and provides a layer of confidentiality on whom or what can access a database for information that is sensitive. In addition to having multi-factor authentication, a zero trust architecture can be adopted to prevent unauthorized access as well.

Cybersecurity frameworks are beginning to use a concept called zero trust framework architecture also known as ZTA. ZTA is "an approach to cybersecurity and risk management that safeguards the environment no matter where data and people reside" (Hubbard et al. 15). In other words, zero trust is the process of not trusting any device, file, or configuration unless it is properly verified and authorized to connect, run, or implement on a system. Practices such as multi-factor authentication (MFA), role-based access controls (RBAC), mobile device management (MDM), next generation firewall (NGF), and data loss prevention (DLP) need to be in place for zero trust architecture to work properly. RBAC is the process of having controls for specific roles in a company, government, or school. For example, ODU has multiple roles such as student, instructor, administrator, and more. Students are only allowed to view their classes and upload assignments that the instructors create. Instructors are only allowed to view the

classes that they are instructing and give grades based on the students' performance. Administrators can access student and instructor records that the other two roles cannot. RBAC can be viewed as having what a role can and cannot do to prevent having too many privileges to a single account. Mobile device management is the means of managing a company or government owned device remotely. According to IBM, “IT and Security departments can manage all of a company’s devices, no matter their type or operating system.” The goal of MDM is to track and secure the company or government owned devices from unauthorized third-party access. For instance, the United States Government banned TikTok on all government owned systems because of data collection concerns. Next generation firewall is an advanced firewall that has application awareness, deep-packet filtering and inspection, intrusion prevention systems, high performance, and external threat intelligence (VMware). Firewalls act as a first line of defense on the technical side of cybersecurity. By inspecting the internet traffic coming in and out of a network, a firewall can detect anomalies and block those connections if they are malicious. According to Juliana De Groot, data loss prevention “is a set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users.” Data loss prevention can be in the form of backups, disaster recovery plans, and training. This wards off any potential loss that may occur such as a hurricane striking a company site and taking out databases where data is stored. Furthermore, ZTA should also include encryption of sensitive data and information.

Encryption is the process of converting data into a code that only authorized parties can understand. Encryption can be used to protect personal data in transit and at rest. This includes emails, messages, and files. Utilizing encryption can significantly reduce the risk of data breaches and unauthorized access. One of the most secure encryption algorithms is called

AES-256. AES-256 uses a randomized, complex mathematical algorithm that converts unencrypted information into an encrypted form. It then generates a key to unlock the encrypted data for viewing. Only authorized parties should have access to the key. Another security measure that should be in place is called hashing and salting. Hashing is just like encryption, where it takes plaintext and converts it to a string that is impossible to revert to the original. This is because a hashing algorithm is one way. One of the most secure hashing algorithms is called SHA-256, also known as the Secure Hashing Algorithm. For example, running the string 'this is my example password' with the command 'echo [password here] | shasum -a 256'in the terminal will run through a hashing function and output '86c30572b03d7bab6379429642ede7a4f634bd458cbce2e2e83176c7bc146b0b' as the hashed information. Salting can also be used with hashing. Salting is adding random information to the hashed data to prevent brute force attacks against the data. Encryption, hashing, and salting should be used in combination with each other. This will secure information from prying eyes. If a database storing the information gets hacked, the hacker will have to decrypt the encryption algorithm, hashing algorithm, and the salting key. Putting these measures in place will take centuries to crack the data with modern computing power. However, the most effective way to prevent black hat hacker activity is cybersecurity awareness training.

Cybersecurity awareness training programs can educate employees on how to identify and prevent cyberattacks. Training programs can help develop a culture of safety and security within organizations. Cybersecurity awareness training is important because "human error accounts for almost 82% of all data breaches" (Grigas). In addition, $4.35 million dollars is the average cost of a data breach globally. Cybersecurity awareness training should consist of social engineering awareness, password security, insider threats, CEO fraud, internet use, mobile device

use, and social media policies. For example, Canadian law forces companies and individuals to have cybersecurity training with the Personal Information Protection and Electronic Documents Act also known as PIPEDA. The act states:

> Businesses are responsible for personal information under their control and must designate an individual or individuals who are accountable for compliance with the principles set out in Schedule 1 of PIPEDA. Security safeguards must protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification, regardless of the format in which the information is held. The methods of protection should include physical measures (e.g., locked filing cabinets and restricted access to offices); organizational measures (e.g., security clearances and limiting access on a "need-to-know" basis); and technological measures (e.g., the use of passwords and encryption) (Marrocco et al. 81-94).

In short, employees and businesses are responsible for safeguarding data against malicious attacks. This act also sets punishments for not securing data, which results in financial loss in addition to the cybersecurity breach that occurs. This forces employees to have training such as company lectures and sending test phishing emails to the employees. However, many find a lack of motivation to participate in the training. One way this is countered is through a term called gamifying. Gamifying means turning the training into a game that employees participate in. Rewards can be added to the training game, such as a small bonus. Giving employees a small bonus will be significantly cheaper than a data breach occurring with millions of dollars on the line and loss of customer loyalty. Human error is the leading cause of cybersecurity breaches

across the globe and people must be trained to safeguard themselves, companies, and governments.

Strong passwords, multi-factor authentication, zero trust, encryption, and cybersecurity training are paramount to implement in every individual's life, company, and government. Any form or combination of the following will greatly decrease security risks involved with hosting and storing valuable data. Cyber threats are becoming more potent and evasive, thus resulting in exponential evolution and higher rates of data theft. Personal data is at risk and must be protected from black hat hackers to prevent the stealing and selling of personal data on the dark web.

Works Cited

Bonderud, Doug. “Breaking Rules the Right Way: Regulations for Ethical Hacking.” Insights for Professionals, 22 May 2020, https://insightsforprofessionals.com/it/security/breaking-rules-right-regulations-ethical-hacking. Accessed 17 Apr. 2023.

Cox, Joseph. “Another Day, Another Hack: 7 Million Accounts for Minecraft Community 'Lifeboat'.” *VICE*, 26 Apr. 2016, https://www.vice.com/en/article/bmvj9m/another-day-another-hack-7-million-emails-and-hashed-passwords-for-minecraft. Accessed 19 Apr. 2023.

Gatlan, Sergiu. “FBI Confirms Access to Breached Cybercrime Forum Database.” *BleepingComputer*, BleepingComputer, 24 Mar. 2023, https://www.bleepingcomputer.com/news/security/fbi-confirms-access-to-breached-cybercrime-forum-database/. Accessed 18 Apr. 2023.

Grigas, Lukas. “What Is Cybersecurity Awareness Training and Why Is It so Important?” *NordPass*, 17 Oct. 2022, https://nordpass.com/blog/cybersecurity-awareness-training/. Accessed 8 Apr. 2023.

Groot, Juliana De. “What Is Data Loss Prevention (DLP)? Definition, Types & Tips.” *Digital Guardian*, 8 Feb. 2023, https://www.digitalguardian.com/blog/what-data-loss-prevention-dlp-definition-data-loss-prevention. Accessed 19 Apr. 2023.

Hubbard, Tony, et al. “Zero Trust in a Virtual Cybersecurity World.” *Journal of Government Financial Management*, vol. 70, no. 2, Summer 2021, pp. 12–19. *EBSCOhost*,

https://search.ebscohost.com/login.aspx?direct=true&db=oih&AN=152457695&scope=site. Accessed 8 Apr. 2023.

IBM. “What Is Mobile Device Management (MDM)?” *IBM*, 2023, https://www.ibm.com/topics/mobile-device-management. Accessed 18. Apr. 2023.

Marky, Karola, et al. “‘Nah, It’s Just Annoying!’ A Deep Dive into User Perceptions of Two-Factor Authentication.” *ACM Transactions on Computer-Human Interaction (TOCHI)*, vol. 29, no. 5, Oct. 2022, pp. 1–32. *EBSCOhost*, https://doi.org/10.1145/3503514. Accessed 8 Apr. 2023.

Marrocco, Andrae J., et al. “Data Protection and Cybersecurity in Canada.” *Franchise Law Journal*, vol. 39, no. 1, Summer 2019, pp. 81–94. *EBSCOhost*, https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=139320795&scope=site. Accessed 8 Apr. 2023.

Microsoft. “Create and Use Strong Passwords.” *Microsoft Support*, 2023, https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb. Accessed 8 Apr. 2023.

Saengphaibul, Val. “A Brief History of the Evolution of Malware: FortiGuard Labs .” *Fortinet Blog*, 15 Mar. 2022, https://www.fortinet.com/blog/threat-research/evolution-of-malware. Accessed 18 Apr. 2023.

VMware. “What Is Next Generation Firewall: Vmware Glossary.” *VMware*, VMware Inc., 16 Mar. 2023, https://www.vmware.com/topics/glossary/content/next-generation-firewall.html. Accessed 19 Apr. 2023.

"What Is Encryption and How Does It Work?" *Google Cloud*, Google, 2023, https://cloud.google.com/learn/what-is-encryption. Accessed 20 Apr. 2023.

"What Is a Password Manager?" *Malwarebytes*, 2023, https://www.malwarebytes.com/what-is-password-manager. Accessed 16 Apr. 2023.

Zahn, Max. "Classified Documents Leak on Social Media Sparks Debate Over Government Monitoring." *ABC News*, ABC News Network, 18 Apr. 2023, https://abcnews.go.com/Business/classified-documents-leak-social-media-sparks-debate-government/story?id=98582225. Accessed 19 Apr. 2023.