Ivan Wang

Professor Collin Anderson

PSC 324

13 October 2023

Cyber Security and Its Impact on Digital Systems

In our current interconnected digital age of information and technology, the online space has become a home for billions of users where they would also invest a significant amount of their time. Due to the huge number of internet users and the infrastructure of the internet, this would also mean that there is an increasing number of cyber threats that will affect internet users, businesses, and various industries. With the increased number of cyber crimes, cybersecurity is becoming a popular growing career field that is needed to protect personal data to safeguard national and personal interests from bad actors. In this explanatory essay, we will explore all the different types of cyber threats, how these cyber threats operate, and show the critical role cyber security has on people's lives, businesses, and various other industries including manufacturing, finance, and healthcare.

There are many kinds of cybercriminals in the world and they would often have different objectives for committing cyber crimes. According to Badman, some cyber criminals just want money or information, while others might just want to cause problems or do it for fun. Some cybercriminals would also attack digital systems just to destroy them for personal reasons(Badman, 2023). Cybercriminals are individuals or groups that commit cybercrimes primarily for financial gain. The common cyber crimes committed by cybercriminals are ransomware attacks and phishing scams that often trick people into giving personal information such as credit card information, login credentials, or intellectual property. A hacker is another kind of cybercriminal that uses their technical skills to compromise a computer network. However, not all hackers are cybercriminals because some ethical hackers will impersonate cybercriminals to help organizations and government agencies test their computer systems for vulnerabilities. Nation-state actors are another kind of cybercriminal as they frequently fund threat actors to steal sensitive data, gather confidential information, or disrupt another government's critical infrastructure. These types of activities would often include espionage or cyberwarfare and would be highly funded to make them more challenging to detect. Insider threats do not always result from malicious actors but will hurt their companies through human error. For example, an employee could've unwittingly installed malware on a company device or a disgruntled employee could abuse access privileges for monetary gain or revenge.

A cyber threat is an indication that a hacker or malicious actor is attempting to gain unauthorized access to a network to launch a cyberattack. According to Badman, cyber threats can range from emails from foreign potente offering a small fortune to hidden malicious code that evades detection and gains unauthorized access to a network. Some kinds of cyberattacks include Malware, Social engineering and phishing, Man-in-the-Middle (MITM) attacks, Denial-of-Service (DoS) attacks, Zero-day exploits, Password attacks, Internet of things(IoT) attack, and Injection Attacks(Badman, 2023). Malware is malicious software that is written purposely to harm the computer system and its users. Threat actors would use malware attacks to gain unauthorized access, infect the system to the point where it's not operable, destroy data, steal sensitive information, and wipe files critical to the operating system. Some types of malware include Ransomware, Trojan horse, Spyware, and Worms. Ransomware locks the victim's data or device and threatens to keep it locked or leak it to the public unless the victim pays a ransom to the attacker. A Trojan horse is a malicious code that tricks the user into downloading it because it would appear to be a useful program or hiding within legitimate software. Once the user downloaded the Trojan horse, the attacker can create a secret backdoor onto the victim's device or install additional malware once they gain access to the target system/network. Spyware is a highly secretive malware that gathers sensitive information like usernames, passwords, credit card information, etc, and transmits it back to the attacker without the victim knowing. Worms are self-replicating programs that automatically spread to other devices without human interaction. Phishing is frequently referred to as "human hacking" because it uses social engineering such as fraudulent emails, email attachments, text messages, or phone calls to trick people into sharing their personal data or login credentials to download malware, sending money to cybercriminals, or expose them to other cybercrimes. Some types of phishing include Spear phishing, Whale phishing, and Business email compromise(BEC). Spear phishing is a highly targeted phishing attack that manipulates a specific individual by using information from the victim's public social media account to make the scam seem more convincing. Whale phishing is a kind of spear phishing that targets corporate executives or wealthy people. Business email compromise(BEC) are scams where cybercriminals pretend to be executives, vendors, or trusted business associates to trick victims into writing money or sharing sensitive data. Another kind of social engineering scam is domain name spoofing(DNS spoofing) where cybercriminals use a fake website(domain name) that impersonates the real one to trick people into entering sensitive information. In a man-in-the-middle attack, cybercriminals eavesdrop on a network connection to intercept and gather messages between two parties and steal data. MITM attacks usually occur in unsecured WI-FI networks. Denial-of-Service(DoS) attack is a cyberattack that overwhelms an application or system with huge volumes of traffic, which will cause the system to become slow to use or become unavailable to other legitimate users. A distributed denial-of-service attack(DDoS attack), is similar to a DoS attack, except that it uses a network of internet-connected malware bots that aims to cripple or crash a given system. A zero-day exploit is another type of cyberattack that takes advantage of an unknown or unpatched security flaw in computer software, hardware, or firmware. It's called "Zero-day" because the software or device vendor has no time to fix the vulnerabilities. After all, bad actors can use them to gain access to vulnerable systems. A password attack involves cyber criminals trying to guess or steal the password or login information to a user's account. Many password attacks use social engineering to trick victims into unwittingly sharing sensitive data but hackers can also use brute force attacks to steal passwords. In an Internet of Things(IoT) attack, cyber criminals exploit vulnerabilities in IOT devices(like smart home devices or industrial control systems) to take over the device, steal data, or use the device as a botnet for other malicious activities. In injection attacks, hackers inject malicious code into a program or download malware to execute remote commands, this will allow them to read or modify a database or change website data. SQL injection attack is when hackers exploit the SQL syntax to spoof identity, expose or tamper destroy or make existing data unavailable, or become the database server administrator. Cross-site scripting(XSS) is a type of attack that will infect users who visit a website.

Cyber Security plays an important role in protecting people's lives because it would allow digital trust between providers & consumers and would protect user data from malicious actors. Digital trust is defined by ISACA as the confidence in the relationship and transactions among providers and consumers within the digital ecosystem. In ISACA's survey report, one in five consumers in the US, UK, and Australia experience a sense of resignation that there is nothing they can do to protect themselves from cybercrimes, and half of these people are victims of cybercrimes. ISACA Now states that “If consumers’ data are stolen during cybercrimes and are subsequently sold to malicious actors, one attack can turn into a headache of fraud, identity theft, and social engineering scams for the foreseeable future. Cyberattacks that compromise personal medical information in the healthcare industry or important account details in the financial services industry can cause emotional and financial stress.”(ISACA Now, 2022). Consumers have trust when using systems built by providers but when consumer data is stolen by cybercrimes and sold to malicious actors, the consumer would have to deal with fraud, identity theft, and social engineering scams in the future. This would cause the consumer to become victims of cybercrimes and cause emotional & financial stress. ISACA Now stated that “The average cost of a ransomware attack, not even including the ransom payment itself, was US$4.62 million in 2021 ... These rising costs will ultimately be reflected in the price of affected companies’ products and services, hurting consumers’ budgets.”(ISACA Now, 2022). The increased number of ransomware attacks has also caused the average cost of ransomware attacks to increase and this will affect the company’s budget as they try to offset the damages of the data compromises/cyberattacks. The rising cost would also be reflected in the companies’ products and services, which will affect the consumer’s budgets as well. Other countries like China have been collecting data from US consumers. David Vergun states that China has access to US data and that for decades China has used its cyber capabilities to steal sensitive information, intellectual property, and research from US public and private sectors(Vergun, 2023). This shows that Cyber security plays an important role in protecting people from cyber criminals and once the consumer knows that they are protected from cyber criminals, the consumer will gain trust with the provider.

Cyber Security plays an important role in protecting businesses because it would allow smaller businesses with fewer resources to be protected by cyber crimes and it will protect businesses from retaining trust among their consumers. Small business is an increasingly attractive target for cyber crimes because they present an easy way to gain access to customer credit card records, bank accounts, supplier networks, and employee financial, and personal data. Small businesses are particularly vulnerable to email attacks closely mimicking those of banks or other trusted institutions and citing an urgent need to log in to an account or provide some other vital information since multiple employees could have access to vital information(sbir.gov, n.d). Since small businesses have fewer resources and are attractive targets, these cyber attacks will deeply affect their reputation and finances. For those firms whose business banking accounts were hacked, the average losses were $19,948 today – up significantly from $6,927 in 2013. This huge jump in cost is likely due to the increased sophistication in phishing and hacking schemes as well as an improved economy that finds greater funds available in many small firms' bank accounts than was there just two years ago(sbir.gov, n.d). Cyber Security also plays an important role in protecting businesses from retaining trust among their customers. A cyberattack can disrupt your business operations, causing downtime and loss of productivity. Ensuring that your company has a robust cybersecurity strategy in place helps maintain the continuity of your operations and minimizes the potential for costly interruptions(nu.edu, n.d). When this happens, businesses will have to use up additional resources to continue operations, and this will hinder the growth of the business. Once the business is fully operational, the customer would want to have their data protected from cybercriminals. Customers are becoming increasingly aware of the importance of protecting their data. By demonstrating a strong commitment to cybersecurity, businesses can build trust with their customers, leading to increased loyalty and long-term relationships(nu.edu, n.d). This shows that Cyber Security plays an important role in protecting businesses from cyber criminals and once the businesses gain resources to allow their consumers to be protected, the business would also retain trust among the consumers.

Cyber Security plays an important role in various other industries such as manufacturing, finance, and healthcare because they contain sensitive data on their users and prevent intellectual property theft. In 2019, Capital One had to pay 80 million dollars to settle federal charges over a hack of its computer systems that ended up being one of the largest financial data breaches ever. Over 100 million credit card applications were exposed in the cyber attack that was carried out by a single individual(Gandel, 2020). This just shows that cybersecurity plays an important role because huge industries like Capital One ended up being a victim of cybercrime and their consumers' sensitive information were exposed. Capital One did end up learning from this incident because Capital One was also required under the OCC order to establish an independent committee to assess if it has any continuing cybersecurity issues and report with fixes within 60 days. Cyber Security also plays an important role in healthcare because hospitals/clinics contain patient information and any sort of disturbance can cause the hospitals/clinics to shut down. Hospitals and clinics in several states on Friday began the time-consuming process of recovering from a cyberattack that disrupted their computer systems, forcing some emergency rooms to shut down and ambulances to be diverted. Eaton-Robb stated that the latest data security incident took their systems offline which affected the facilities operated by Prospect(which is based in California and has hospitals and clinics in Texas, Connecticut, Rhode Island, and Pennsylvania). As a result, many primary care facilities run by Prospect Medical Holdings remained closed as security experts worked to determine the extent of the problem and resolve it(Eaton-Robb, 2023). This cyber attack caused a bunch of hospitals and clinics to shut down and as a result, many people’s lives were endangered because people with health problems or people who were extremely sick couldn’t have gone to any facilities operated by Prospect. Eaton- Robb stated that “The incident had all the hallmarks of an extortive ransomware but officials would neither confirm nor deny this. In such attacks, criminals steal sensitive data from targeted networks, activate encryption malware that paralyzes them, and demand ransoms.”(Eaton-Robb, 2023). This demonstrates that the Prospect hospitals/clinics were affected by ransomware that would also steal sensitive data from targeted networks and activate encryption malware that paralyzes the network unless they pay the ransom. This would also affect the patients because they went to this specific hospital to make sure they were healthy and knew they might risk the attackers stealing their personal information. Eaton- Robb also stated that healthcare providers are common targets for criminal extortionists because they have so much sensitive patient data, including healthcare histories, payment information, and even critical research data. Cyber Security also plays an important role in manufacturing because it will prevent intellectual property theft. Manufacturers have continued to adopt smart technologies and internet-of-things devices but manufacturers are high-value targets for cyber crimes because of their importance within the economy and the value of their data for purposes of intellectual property. Lombardi states that cyberattacks have become the predominant means of intellectual property theft in the manufacturing sector and the attackers have increased their level of sophistication in their technical and business acumen. An ambitious attacker who lacks the skills to break into a manufacturer’s network can purchase access on the dark web from an “access broker.” and an access broker acquires access to organizations and sells this access to other adversaries, including ransomware operators(Lombardi, n.d).

Therefore, there are many different types of cyber threats and these cyber threats operate differently. Cyber security has an important role in protecting people's lives, businesses, and various other industries including manufacturing, finance, and healthcare. If cyber security isn't an important role as it is now, there would be more cyberattacks that would steal people's data. There would also be less trust between providers & consumers and there would be less protection of user data from malicious actors. There would also be fewer resources for small businesses to be protected by cyber crimes and businesses would lose trust among their consumers. There would be more cyber crimes in various industries that will collect sensitive data and more intellectual property thefts. However, there are also more tools and resources available to keep us safe from cyber threats.

Works Cited

Marketing. “What Is Cybersecurity and Its Importance to Business.” National University, February 13, 2019. https://www.nu.edu/blog/what-is-cybersecurity/.

Eaton-Robb, Pat. “A Cyberattack Has Disrupted Hospitals and Health Care in Several States.” AP News, August 5, 2023. https://apnews.com/article/cyberattack-hospital-emergency-outage-4c808c1dad8686458ecbeababd08fecf.

Gandel, Stephen. “Capital One to Pay $80 Million Fine for 2019 Hack That Exposed 100 Million Accounts.” CBS News, August 6, 2020. https://www.cbsnews.com/news/capital-one-hack-credit-card-applications-settlement/.

Badman, Annie. “Types of Cyberthreats.” IBM Blog, September 1, 2023. https://www.ibm.com/blog/types-of-cyberthreats/.

“The Impact of Cybersecurity on Consumer Behavior.” ISACA. Accessed October 14, 2023. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/the-impact-of-cybersecurity-on-consumer-behavior.

"Tutorial 1: The Impact of Cybercrime on Small Business." Tutorial 1: The Impact of Cybercrime on Small Business | SBIR.gov. Accessed October 14, 2023. https://www.sbir.gov/tutorials/cyber-security/tutorial-1#.

Marlow, Amanda. "Cybersecurity in Manufacturing: It, OT Is Everyone's Job " CBIA." CBIA, September 5, 2023. https://www.cbia.com/news/manufacturing/cybersecurity-manufacturing-awareness/.

Vergun, David. "Leaders Say Tiktok Is Potential Cybersecurity Risk to U.S." U.S. Department of Defense. Accessed October 14, 2023. https://www.defense.gov/News/News-Stories/Article/Article/3354874/leaders-say-tiktok-is-potential-cybersecurity-risk-to-us/.