The Advantages and Disadvantages of Cybersecurity

Tra’Von Pulliam

CYSE 368

Summer 2023

**Table of Contents**

Introduction —----------------------------------------------------------------------------------- 2

What Is Cybersecuirty —----------------------------------------------------------------------- 2-3

Advantages of Cybersecurity —--------------------------------------------------------------- 3-4

Disadvantages of Cybersecurity —------------------------------------------------------------ 4-5

Impact of Cybersecurity on Modern Society —--------------------------------------------- 5-6

Cybersecurity Impact on Health Services Sector —---------------------------------------- 6

Cybersecurity Impact on Financial Services Sector —------------------------------------- 6-7

Cybersecurity Impact on Retail Sector —---------------------------------------------------- 7

Future of Cybersecurity —---------------------------------------------------------------------- 7

Future of Cyber Warfare —--------------------------------------------------------------------- 7-8

Future of Handling Hackers —----------------------------------------------------------------- 8

Future of Talent Development —--------------------------------------------------------------- 8

Future of Legacy Technology —---------------------------------------------------------------- 8

Future of Artificial Intelligence (AI) —-------------------------------------------------------- 9

Conclusion —-------------------------------------------------------------------------------------- 9-10

References —--------------------------------------------------------------------------------------- 11

**Introduction**

Cybersecurity has evolved and taken the world to new heights. Cybersecurity has not just affected the physical world, but the digital world also. Cybersecurity has become the bridge that keeps the physical world and digital world connected between each other. Cybersecurity is an interesting job within the technological field, but the job can have advantages and disadvantages. These advantages and disadvantages help define what cybersecurity is, the impact cybersecurity has on the modern world, and the future of cybersecurity

**What Is Cybersecurity**

Many people who are non cyber experts or do not work within the cybersecurity field may have little to no knowledge of what defines cybersecurity. Cybersecurity is the practice of protecting sensitive information and critical systems from digital attacks or threats. Cybersecurity measures which include information technology (IT) security are designed to fight off threats that may harm networked systems and applications, whether those threats originated from the inside or outside of an organization. The purpose of cybersecurity is to defend against cyber attacks which includes unauthorized access to personal data, extortion, stealing organizations valuable information, disrupting organizations activities, and damaging someone’s reputation. There are various attacks that may occur within the cybersecurity field. Some common cyber attacks that may occur within the cybersecurity field are phishing, malware, denial-of-service, ransomware, man-in-the-middle (MitM), and SQL injection. Phishing attacks involve tricking or luring users to click on malicious links and attachments which leads them to getting their sensitive information such as login credentials or financial data stolen from attackers. Malware is malicious software that can infect computers or devices to hijack them, steal information, or launch attacks on other systems. Denial-of-service attacks prohibit users from having access to a system or service by flooding the system with traffic and requests that may damage the operation. Ransomware is malware that encrypts files or systems in which hackers can demand a ransom to decrypt them. This type of attack can lead to sensitive data to be lost or operations can be completely shutdown. Man-in-the-middle (MitM) attacks is when attackers can intercept private communications between two parties. Attackers can redirect traffic to malicious servers or eavesdrop on network connections. SQL injection is an attack that is used to inject malicious SQL codes into a database by exploiting a web application’s vulnerabilities. The SQL code can view, modify, or delete data within the database. SQL injection attacks can also take over a server and harm a system with various malicious activities (*Importance of Cyber Security: Benefits and Disadvantages,* 2023). There are many common attacks that cyber experts have to face within day to day operations, but they can be prevented by using the numerous cybersecurity domains that are offered. Within the cybersecurity field, there are various domains. These cybersecurity domains are strong strategies that are layers of protection that are used to defend against cyber attacks or cyber crimes that try to access, destroy, or change data. The strategies or countermeasures that are included within the cybersecurity domain are network security, critical infrastructure security, application security, cloud security, information security, storage security, mobile security, end-user education, and disaster recovery/business continuity planning (*What Is Cybersecurity,* 2023).

Each countermeasure plays a major part within the cybersecurity domain. Network security is a security measure that is for protecting computer networks from unauthorized users which includes wired and wireless (WIFI) connections. Critical infrastructure security is practices that are used for protecting networks, computer systems, and many other components that are relied on by modern day society for national security, public safety, or economic health. According to IBM.com, the National Institute of Standards and Technology (NIST) created the cybersecurity framework to help organizations with this area of security, while the US Department of Homeland Security (DHS) provided additional guidance. Application security are processes that are used to protect operating applications in the cloud. This cybersecurity countermeasure is more effective when the security is built into applications during the design stage with data handling and user authentication considerations. Cloud security is an effective confidential computing that encrypts cloud data in the storage, travels to and from the cloud, and is put to use during the process to support customer privacy, regulatory compliance standards, and business requirements. Information security is a data protection measure, such as the General Data Protection Regulation (GDPR), which secures the most sensitive data from unauthorized users to access, steal, or expose. Storage security uses various safeguards that contain solid data resilience. These safeguards include encryption, immutation, and isolation of data copies. They all remain in the same area so they can quickly be restored to support recovery and minimize the impact of cyber attacks. Mobile security is used to enable users to manage and secure their mobile devices with app security, secured email, and container app security. End-user education is used to build security awareness across organizations to strengthen their endpoint securities by training users to avoid using unknown USB devices, delete suspicious email attachments, and many other cyber precautions. Disaster recovery/business continuity planning are tools and procedures that are used for responding to unplanned events such as power outages, natural disasters, or cybersecurity incidents that have minimal disruption to key operations (*What Is Cybersecurity,* 2023). These countermeasures are useful to minimize cyber incidents and a major part of what defines cybersecurity.

**Advantages of Cybersecurity**

There are various advantages of cybersecurity that will benefit the physical and digital world. Some advantages of cybersecurity are protecting sensitive personal information, preserving organizations reputation, improving productivity, assisting remote workspaces, regulation compliance, better data management, IT team support, educating or training the workforce, streamline access control, maintain trust and credibility, and improving cyber posture. Each advantage benefits organizations and users from cyber threats or data breaches. By protecting sensitive personal information, organizations and individual users will be able to prevent their private data from being collected by malware. Organizations can preserve their reputations by using network and cloud security which will strengthen access or authentication. Organizations can improve their productivity by having automated backups and improved firewalls that will prevent viruses from affecting networks, functioning, or workflows. Cybersecurity can assist remote workspaces by serving as a secure center for stored data and protect home WIFI from tracking users’ data. Regulations such as GDPR or HIPPA have an essential role in protecting users and organizations. Having regulation compliance can prevent penalties or major cyber incidents. By having better data management, organizations can ensure that their data security regulations are being implemented properly which will lead to operational efficiency. Cybersecurity is a strong support for IT teams because they will be able to stay up to date with rapid changes within cyberspace by using the tools, techniques, and knowledge given to handle advanced cybercrimes. Cyber organizations can strengthen their daily operational safety by educating or training employees about how spyware, data breaches, ransomware, and many other cyber threats are potential risks. This type of education or training can make employees become less vulnerable to cyber attacks and they will be able to know the right course of action to take when an incident occurs. Streamlining access control such as systems, resources, and computers can benefit cyber organizations by reducing cybercrime incidents. Cyber organizations will be able to establish some accountability for management strategies. A major advantage is maintaining trust and credibility. Cybersecurity lays the foundation between an organization and its customers. By maintaining trust and credibility, customers can continue to have a relationship with an organization due to them knowing about the history of various safeguards and data protection. Another cybersecurity advantage that will continue to benefit many organizations and users is to consistently improve cyber posture. Cybersecurity already provides many organizations with protection by allowing their employees to have access to the internet in a flexible and safe way. By improving cyber posture, organizations can use cyber tracking technology to quickly respond to cyber attacks which will strengthen their cybersecurity protocols (Williams, 2023). These advantages of cybersecurity can benefit many organizations and users by improving their daily operations while keeping personal sensitive information protected also.

**Disadvantages of Cybersecurity**

There are many disadvantages of cybersecurity that may prevent the digital and physical world from evolving to the next level of technological advancement. Some disadvantages of cybersecurity include regular updates, needing continuous learning, complex to set up, slower systems, constant monitoring, expensive, and employment shortage. If organizations do not regularly update their networks or systems, then they will become vulnerable to attackers. Organizations should always regularly update their software, hardware, and security strategies to stay one step ahead of attackers. If cyber experts do not use the continuous learning process, then they will not be prepared for any new upcoming threats that may occur in the near future. Continuous learning is a beneficial learning process that many cyber experts need to be using to keep up with any new threats that may occur. By using the continuous learning process, cyber experts will have common knowledge on the new threats they will be facing. When setting up security tools or architectures such as firewalls, the process can become complex. The setup can become complicated and take a long period of time. To avoid complex setups, cyber experts can help each other and make sure they are setting up the security tools properly to protect systems or networks from being attacked. Another disadvantage of cybersecurity is cyber organizations that do not constantly monitor their systems or networks. If cyber organizations do not constantly monitor their systems or networks, then they will not know when cyberattacks are occurring and attackers can hack them at any given moment. To solve this problem, cyber organizations should constantly monitor their systems or networks for any new threats because they will be able to detect attacks in advance which will lead them to have access to threat levels for faster problem solving. A major disadvantage that many cybersecurity organizations come across is the expenses of cybersecurity implementation. Cybersecurity implementation can be a very expensive process that requires plenty of spending and learning. This can be a challenge for small organizations and other businesses that have more than 1000 employees have to increase their spending to receive the most advanced cybersecurity implementation resources. A solution to solve this challenging issue is for cyber organizations to try to budget and increase their revenue by continuing to use their current tools. If organizations continue to use the current cybersecurity implementation tools without increasing their vulnerabilities, they will be able to have enough to increase their revenue to afford more advanced and up to date cybersecurity resources. A disadvantage that many cyber organizations do not want to face is employment shortage. Cybersecurity is an enormous field, but the number of skilled employees is scarce. This challenge can be solved by cyber organizations training more newly hired employees and giving all the resources they need to prepare themselves for any cyberattacks that may occur in the future. These are some disadvantages of cybersecurity that may setback the digital and physical world from reaching the next level or evolving. To prevent these disadvantages or setbacks from happening, cyber organizations or experts can use all the resources they are given to make sure they stay ahead of any incoming threats (Williams, 2023).

**Impact of Cybersecurity on Modern Society**

As cybersecurity has evolved over the years, the cybersecurity field has affected and impacted modern day society. Cybersecurity has been rapidly growing as an industry that has been potentially impacting modern society in numerous ways. These effects are very important for organizations and people to be aware of. The impact of cybersecurity has effects on our everyday lives, security, and privacy. Cybersecurity affects our everyday lives and quality of life. A major way that cybersecurity affects our everyday lives is securing our personal sensitive information such as financial data, health records, login credentials, and any other private information. There are various cyber techniques, methods, and regulations that many businesses use to make sure people’s personal information is not accessed by unauthorized users (*What Impact Does Cyber Security Have On Our Society,* 2022). Many services such as healthcare, financial, and retail are strengthening their regulations to prevent hackers getting access to consumer’s personal information.

**Cybersecurity Impact on Healthcare Services Sector**

Within the healthcare sector, healthcare providers are confined to the Healthcare Information Portability and Accountability Act (HIPAA) which they use to take measures in making sure that patients’ health records or protected health information (PHI) is secured from any cyberattacks. The Healthcare Information Portability and Accountability Act (HIPAA) outlined the standards for protecting electronic protected health information (PHI) through numerous technical and operational controls that implement patient confidentiality. Many healthcare organizations must be able to demonstrate the Healthcare Information Portability and Accountability Act (HIPAA) compliance to avoid any fines or legal action due to data breaches. The Healthcare Information Portability and Accountability Act is considered the primary regulation that healthcare providers adhere to, but Congress and the FDA has introduced many others as the years have gone by such as the Medical Device Cybersecurity Act and the Internet of Medical Things Resilience Partnership Act (*The Cybersecurity Regulations Healthcare, Financial Services, and Retail Industries Must Know About,* 2018). These regulations and guidelines make sure that healthcare providers are protecting and handling them in a proper manner.

**Cybersecurity Impact on Financial Services Sector**

The financial services sector has to follow several guidelines and regulations. The primary regulation that the financial services sector has to follow is the Financial Industry Regulatory Authority (FINRA). The Financial Industry Regulatory Authority (FINRA) requires any written procedures and policies to be submitted that regards the protection of consumer information from cyberattacks. The Financial Industry Regulatory Authority (FINRA) also outlines rules for the mitigation and detection of cyber threats that can get access to consumers’ identities. The financial services sector is recognized globally as a critical infrastructure. For example, many financial service firms in New York must consent to the 23 NYCRR 500 cybersecurity regulation that was issued by the Department of Financial Services. This regulation requires banks and firms to have an effective cybersecurity plan and enforce the disclosure of cyber incidents within 72 hours (*The Cybersecurity Regulations Healthcare, Financial Services, and Retail Industries Must Know About,* 2018). There are many other global financial service regulations that have been developed to prevent consumers’ financial data from being stolen.

**Cybersecurity Impact on Retail Sector**

Another major sector that cybersecurity has an impact on is the retail sector. The retail sector is mainly targeted for consumers’ stored credit card data. The regulation that retailers have to adhere to is the Payment Card Industry Data Security Standard (PCI DSS). The Payment Card Industry Data Security Standard (PCI DSS) provides guidance on how retailers should store consumers’ credit card data and transmit payment information to minimize any risks of data breaches or fraud. In order for retail organizations to keep data secured and maintain compliance to the Payment Card Industry Data Security Standard (PCI DSS), they must position security controls that meet the regulatory requirements and create compliance reports that prove their adherence. The Payment Card Industry Data Security Standard (PCI DSS) is a regulation that is beneficial to the retail sector because the standards help build trust between the retail services and consumers to make sure their data is being protected and stored properly (*The Cybersecurity Regulations Healthcare, Financial Services, and Retail Industries Must Know About,* 2018).

**Future of Cybersecurity**

There is a lot in store for the future of cybersecurity. The future of cybersecurity is very difficult to predict due to the industry always continuing to evolve with the various numbers of cybercrimes and new cyber attacks that are being developed. Even though nobody knows when the next cyber threat is going to happen, the cybersecurity industry is always developing new components to defend against them to continue to be successful. There are many components that are leading cybersecurity to become one of the most successful industries in the near future. Some components that are shaping the future for the cybersecurity industry are more focused cyber warfare threats, handling multiple hackers all at once, developing more cybersecurity experts, dealing with legacy tech issues, and most importantly, artificial intelligence (AI) (Parker, 2021).

**Future of Cyber Warfare**

A major issue that the cybersecurity industry will have to continue to face is cyber warfare threats. Cyber warfare is when one nation decides to hack or implant viruses in the computer system of another. This type of warfare leads to the borderline or frontier of many wars fought around the world. Over the years, cyber warfare has been an issue the world has been facing for a long time. This issue began in 2010 with Stuxnet when a worm was implanted on Iranian uranium centrifuge computers to cause equipment failure. Another cyber warfare incident happened in 2017, when a Russian hacking group named Sandstorm, decided to go after many targets such as Eastern European energy grids and American corporations. This is an avenue that many small nations or rising economies may turn to get the resources and political support they need in order to get involved in traditional conflicts. In the near future, cybersecurity organizations will have to find ways to use key pieces of infrastructure to make them seem more appealing targets during cyberwars and make them strong enough for digital intrusions by adding many layers of security to traffic systems, hospital databases, and airport management networks (Parker, 2021). These ideas will help the cybersecurity industry deal with cyber warfare in the future.

**Future of Handling Hackers**

There are multiple hackers in the world and they are difficult for cybersecurity experts to handle all at once. According to a study by Michael Cukier, who was a researcher at the University of Maryland, had discovered that computer hacks have been frequently occurring on average at every 39 seconds. Michael Cukier found out that most of the cyber attacks were being done using automated scripts which lurked through digital addresses and databases to search for vulnerabilities to exploit. These automated attack scripts were written by tech-savvy people in which hackers are becoming more skilled and developed when using their techniques. In order for the cybersecurity industry to defeat this issue, cyber experts will have to train and educate more tech-savvy people to prevent them from using their skills for cybercrimes and hacking (Parker, 2021).

**Future of Talent Development**

Since the number of cyber attacks have grown over the years, many businesses have to spend a little more money than usual just to protect themselves. However, there is only so much software can do to protect businesses, so spending on larger security will not achieve much unless they implement protective applications that are run by skilled information security (infosec) experts. The main issue is that there is a significant shortage of skilled workers. Cybersecurity companies will have difficulty hiring more cyber experts who have infosec skills because it will be too expensive. The only solution for cybersecurity companies is to teach their current employees the infosec skills by training them with ethical hacking courses (Parker, 2021).

**Future of Legacy Technology**

As time has passed, legacy systems have become a major cybersecurity risk. For example, in 2017, the WannaCry ransomware attack caused more than 200,000 computers to be infected that ran older versions of Windows in 150 countries. There are numerous reasons that legacy technology is a major risk such as manufacturers having little to no motivation to continue releasing security patches for outdated systems and legacy dependencies. Legacy dependencies are legacy tech pieces that rely on other pieces of hardware or software to run. This is an issue because it has its own security vulnerabilities. Many companies around the world are using legacy technology to save money or they do not know the security benefits of upgrading their systems. These companies do not know they are exposing themselves to cyber risks when using legacy technology. In the future, this could still be a major problem and might get worse if not solved. This issue can be solved if many companies and users keep their legacy technology updated, so hackers will not have access to them (Parker, 2021).

**Future of Artificial Intelligence (AI)**

Over the last few years, artificial intelligence (AI) technology has become satisfying in many different industries. Artificial intelligence (AI) and machine learning algorithms have been used to do tasks, make decisions faster than a human, and process information. However, artificial intelligence (AI) technology can eventually cause cybersecurity risks due to potential exploits that are being released at misunderstood times. This issue can make AI systems to become prominent targets for hackers in which cybersecurity developers will have to create techniques or methods to detect and counteract these AI attacks. Hackers will try to corrupt AI to target organizations, so cybersecurity developers will have to use AI for themselves to detect security issues, address vulnerabilities, and prevent cyber attacks from happening before they begin. There are a lot of ways that AI technology will be used by future cybersecurity developers such as revealing weak points within a system, warning people about risky websites, and creating simulated network attacks (Parker, 2021).

**Conclusion**

As we continue to live in modern day society, we have to learn that technology evolves. As years pass, technology will continue to elevate and we will have to continue to rise with the advancements to be able to stay at some common level with it. Cybersecurity is growing and will continue to rise as an industry. Nobody knows what cybersecurity will have in store for the world, but as long cyber industries still benefit the public then there will always be success in the future. Cybersecurity will always be successful as long as the industry is still that bridge between the digital and physical world. Even though cybersecurity might have its advantages and disadvantages, the cyber industry will always define cybersecurity for what it is, the impact it has on the modern day world, and its upcoming successful future.

**References**

Parker, J. (2021, August 20). *What is the future of cybersecurity?* [Review of *What is the future of cybersecurity?*]. TechRadar; Future US Inc. <https://www.techradar.com/news/what-is-the-future-of-cybersecurity>

Saxena, A. (n.d.). *Importance of cybersecurity: Benefits and Disadvantages* [Review of *Importance of cybersecurity: Benefits and Disadvantages*]. Sprinto; Sprinto. Retrieved July 9, 2023, from <https://sprinto.com/blog/importance-of-cyber-security/>

(2018, August 21). *The Cybersecurity Regulations Healthcare, Financial Services, and Retail Industries Must Know About* [Review of *The Cybersecurity Regulations Healthcare, Financial Services, and Retail Industries Must Know About*]. CSO; Foundry. <https://www.csoonline.com/article/566083/the-cybersecurity-regulations-healthcare-financial-services-and-retail-industries-must-know-about.html>

Williams, T. (2023, January 19). *Advantages and Disadvantages of Cyber Security For Business* [Review of *Advantages and Disadvantages of Cyber Security For Business*]. The Knowledge Academy; The Knowledge Academy. <https://www.theknowledgeacademy.com/blog/advantages-and-disadvantages-of-cybersecurity/>

(2022, August 17). *What Impact Does Cyber Security Have On Our Society?* [Review of *What Impact Does Cyber Security Have On Our Society?*]. Cybersecurity Degree and Career Guide; Cybersecurity Career. <https://cybersecuritycareer.org/what-impact-does-cyber-security-have-on-our-society/>

‌(n.d.). *What is cybersecurity?* [Review of *What is cybersecurity?*]. IBM; IBM. Retrieved July 9, 2023, from <https://www.ibm.com/topics/cybersecurity>

‌