Cybersecurity

Devid Karki, Department of Computer Science and Information System, A&M-Commerce

Abstract

Security dangers differ from one system to the next. Depending on the system, they operate differently. The correct rules must always be in place to support best practices, and the initial actions must start at the top. Cybersecurity is a critical aspect of corporate governance. Top-level management commitment must be backed up by sufficient funding for security software and hardware, training, security expert recruitment, outside security services, and other requirements. As part of policymaking, roles and responsibilities for all important stakeholders should be given. Management must recognize that security is more than a one-time expense when formulating policies. More consumer trust, increased confidence in working with suppliers, the discovery of new revenue channels, and better risk management for future acquisitions, divestitures, and mergers are benefits of strengthening cybersecurity. This paper focuses on the evaluation of cybersecurity, its importance and categories, threats and damages by cyber-attacks, its implementation, and suitable technologies.

Keywords: Cybersecurity, Cyberwarfare, Cyberattacks

Introduction

The term cyber security encompasses all the technologies and tactics used to protect computer systems and electronic data. It's a vast and growing sector in a world where we are doing more and more of our professional and social lives online. It protects our data and information safe from cyber-attacks while maintaining a high level of security. It is about protecting our data and information from cyber-attacks while maintaining strong security policies. Every organization and enterprise needs to protect them against unauthorized access, deletion, and modification to their database, network, and systems. Over that, digital attacks and crimes are evolving continuously. Programmers and hackers are becoming more brilliant and innovative with their malware, and how they sidestep infection outputs firewalls confuses many individuals. Cyber security is vital because it involves everything that has to do with safeguarding our data from cyber attackers who wish to steal it and use it to do us damage in the future. That data might include sensitive data, data from the government or the business, personal data, personally identifiable information (PII), intellectual property, and protected health information (PHI) (PHI). To preserve this information, it is critical to have effective cyber defense plans and methods in place, which is in everyone's best interests. Critical infrastructure, such as hospitals and other healthcare facilities, financial services programs, and power plants, is relied upon by everyone in society. We need them to keep our civilization working smoothly. When it comes to individuals, cyber security assaults may result in identity theft and extortion attempts, both of which can do significant harm to that individual's life. We all depend on the security of our data and personal information to function properly. Examples include login onto a website or entering more sensitive information into digital healthcare systems such as patient records. If these systems, networks, and infrastructures do not have the appropriate security measures in place, our information may get into the incorrect hands. In this context, we're talking about the protection provided by technology and government legislation. The same is true for organizations and corporations, as well as governments, the military, and other socially important groups. Thousands of gigabytes of information are stored in data warehouses, computers, and other electronic devices. A significant amount of this data contains sensitive information. The public disclosure of this information may be very destructive in several ways, including to citizen faith in institutions, corporate competitiveness, personal reputations, and consumer trust in corporations and organizations.

Evolution of Cybersecurity

The first computer virus was created with no malicious intent back in the the70s by Bob Thomas when he realized that the codes he wrote could make the worm that moved quickly between the computers, and it said, "I'm the creeper: catch me if you can!" ("The fascinating evolution of cybersecurity," 2018). Another program named "reaper" was created by Thomas's colleague Ray Tomlinson in response to the teasing that would delete Thomas's "creeper" worm ("The fascinating evolution of cybersecurity," 2018). The introduction of the Reaper widely helped in developing the programming culture. The first denial-of-service attack known as the Morris Worm was reported back in 1989 to slow down and eventually crash each computer infected. Robert Morris created the worm, and the worm caused anywhere from $100,000 to $10,000,000 worth of damage ("The fascinating evolution of cybersecurity," 2018). The government started to set up various CERT's, which stands for computer emergency response teams, to fight against these illegal actions and crises. People started noticing a minefield of unwanted ads, pop-ups, viruses, and malware, and it didn't take long until they evolved into complex forms like Trojans and spyware. The enormous antivirus organizations set up during the 1990s overwhelmed the network safety industry for around 20 years. Yet, since 2014, massive, efficient assaults have introduced another test and requested more imaginative and savvy fixes. Increasingly complex cyber-attacks create fascinating new challenges for those in the rapidly expanding cybersecurity industry, which is striving to resist the ever-present threat of malicious activity by using cutting-edge technology and techniques.

With cyber warfare, new tactics of foreign information infiltration have been introduced to the military platform around computers, transforming it. With more valuable information to mine, cyber-attacks became more recurrent as the internet grew more popular (Bishop & Goldman, 2003). Because of the increasing importance of the internet in our everyday lives, extra protections have been implemented, such as the Social Media Privacy Protection and Consumer Rights Act (SMPPCR) (Grabosky, 2000). If a "black hat" hacker can exploit a flaw in the system that engineers are ignorant of, it might have severe consequences. In 2009, China gained access to critical US urban power, networks, and Russian espionage in Ukraine, which has made governments throughout the globe suspicious of China's activities (Lin & Kerr, 2018). The military isn't the only one affected by these cyber issues; the rest of society is as well. Social media is susceptible to cyberattacks because of the vast amounts of data kept in its servers. As a result of dangerous infiltration tactics and the fear of their data being indexed by black hat hackers, millions of internet users have lost their privacy because of cyberwarfare (Thomas, 2006).

Cyberwarfare has caused significant harm to government political structures. Many countries' internal political difficulties may be breached by foreign organizations and used against them. Hackers are looking for high-profile figures like Bill Clinton, who had his personal information leaked in 2016 and was transmitted to an unapproved website. It has become more commonplace for huge corporations to spy on their customers through social media. As a result of backdoor assaults on these platforms, incidents like the 2015 Facebook data breach may potentially expose millions of users and their personal information. Aside from altering military conflict, cyberwarfare has a negative influence on both the political and social aspects (Lin & Kerr, 2018).

Since the 1990s, cyber warfare has had a significant impact on political situations across the world. Because many people frequently underestimate the impact of cyber warfare in the political system, it's critical to go deeper into this notion of changing legislation (Crawford, 1999). The development of cyber warfare is "comparable to a revolution"; countries worldwide have transitioned from a period of combat conflict to a period of cybersecurity, which will drastically alter political policy (Furnell & Warren, 1999). The author describes how there are a plethora of cyber-attacks that will soon mark the globe, as well as spark a global war in the center of nations. The belief that cybers warfare was a revolutionary strategy of foreign aggression reflects the reality that, over time, nations have become hostile with one another due to the invisibility of cyber-attacks (Rathmell, 1997). Because freshly built computers are vulnerable to viral assaults and backdoors, it may be stated that as technology becomes essential, there will be a rise in international tension.

Cyber-attacks are so common today that no one's privacy can be guaranteed on social media. In this interconnected society, social media has become a fundamental means of communication. People have become so reliant on these messaging services that social media has begun to enter the domain of cyber warfare. Cyberwarfare has explored popular sites, including Facebook, Instagram, and Twitter, one of the most widely used social media applications in the business (Hayes et al., 2012). These large-database websites are more likely to contain accounts related to politically prominent persons. Hackers looking for bad intentions would look for the most valuable material on a popular website like Twitter. Even though many of these websites have extensively protected databases, "nothing is impenetrable" (House, 2016). There are always methods to get beyond the security measures put in place to prevent such a breach. In 2018, Facebook users were inadvertently exposed to this problem, and their whole data was taken in a distant index. Personal information such as their name, address, phone number, and other vital credentials might be used to impersonate or destroy the victim's life (Lin & Kerr, 2018).

Each new year brings new technological developments, as well as an increase in the intensity of cyberwarfare. Developing and impenetrable engineering systems is unachievable since there are many fresh additions to the world's compendium of technology. Because of this, one of the deadliest subcategories of war is the heritage of cyber warfare. Many other monograms fail to realize that cyber warfare is more than merely obtaining the credentials of vulnerable victims through remote access. These assaults can spread to an enormous extent of destruction. A city in the United States formerly had limited access to one of the country's electrical systems. China might have triggered a power outage or blown-up transformers at whim if the electrical infrastructure was infiltrated (Crawford, 1999). Cyber-attacks are so deadly because it is practically hard to trace them back to the perpetrator, forcing many individuals to rely on their sleuthing abilities. Furthermore, since technology is increasingly integrated into everyday items, more people are vulnerable to an attack's wrath.

Chip-set instructions, such as GPS and steering, are largely relied on in today's automobiles, which have been developed by the motor industry. As long as the car's systems aren't affected by a virus, it may be remotely operated by the hacker. In a society founded on technology, it is not possible to be entirely protected from cyber-attacks. This is the point. The most frightening aspect of cyber warfare is not what has already been done but what may be done in the future. "The severity of cyber-attacks is expected to rise as newer technology replaces older appliances, which might have a catastrophic impact on social and political affairs" (Lehto & Neittaanmäki, 2015).

Importance of Cybersecurity

Cyberattacks are widespread these days, and these attacks affect the state-run organization and services to the citizen. "Case in point, the city of Atlanta, was attacked by utilizing the infamous SamSam ransomware. The attackers asked for a ransom of $51,000" (Bishop & Goldman, 2003). The ransomware was so hazardous and harmful that the city of Atlanta was offline for five days. This caused several significant citywide operations to be halted. It ended up having a recovery cost of $17 million (Fung, 2021). Cybersecurity is very important in our daily life as it helps us prevent data leaks and identity theft. The basic knowledge of cybersecurity warns us to avoid using public Wi-Fi and always protect our mobile and gadgets with a strong password. People may get access to our information and data, and they could open new credit cards pretending to be us and even receive medical services. As technology produces more devices that will meet this demand, it also creates more potential for new cyber threats to emerge. The enhancement of advanced and high-speed networks like 5G could create a new ecosystem for hackers and scammers. With the increment in multidimensional cyberattacks and complex models, it is hard to retool how associations would protect the essential networks of the 21st century (Bailetti & Zijdemans, 2014). Cyber-attacks are making many dollars in harm because it is very costly to retrieve the lost data information, and even companies and organizations are subject to penalties and charges to be paid through fines. This load of costs can easily affect high-level chiefs to lose their positions and partners can lose their situation because of the organization reducing expense. With network safety dangers expanding, new laws can be set to shield the buyer from likely assaults. This would imply that expanded guidelines and enactment may before long turn into a reality. Harsher punishments should be set on culprits of the assault. Residents should be made aware of the laws that have been established and should ensure that their organizations comply with the legislation.

All aspects of cyber security are crucial because they safeguard our data from cyber-attackers who may exploit it for malicious purposes. It may include sensitive data, government, and industrial information, personal data, PII, intellectual property, and protected health information (PHI). It is critical and in everyone's best interest to have robust cyber defense procedures and processes in place to safeguard sensitive data. Infrastructure such as hospitals, banking institutions, and power plants provide essential services to everyone in society. These are essential to the functioning of our community. An individual's life may be ruined by cyber security assaults, resulting in identity theft and extortion attempts.

We all depend on the security of our personal information and our data. Logging onto an app or filling out sensitive data in digital healthcare systems, for example, If these systems, networks, and infrastructures are not adequately protected, our data may be compromised and put at risk. In this context, we're referring to technology and regulations as forms of protection. Businesses, governments, the military, and other socially important organizations are all affected by this. Their data centers, computers, and other technology are home to massive quantities of information. Many of these records include confidential information. In many circumstances, the public's faith in institutions, corporate competitiveness, personal reputations, and consumer trust in corporations may be harmed by the disclosure of this information.

Cyber assaults are a constant danger to everyone and everything. Malware, phishing, man-in-the-middle attacks, and drive-by assaults are examples of such attacks. Wait till you hear about crypto jacking before you make a decision. This is the point at which thieves might get access to your computer and exploit it to steal resources such as Bitcoins and other digital money. If they are able to get access to your computer, they will have little trouble stealing your information. If you want to have a fighting chance against these attacks, you'll require cyber security. With the rapid growth of technology, such as high-speed internet, smarter gadgets, and cloud computing, the number of linked devices has increased dramatically in recent years. The number of networked devices in the globe is expected to reach around 21.1 billion by 2021, according to some estimates (Patterson, 2021). This, together with the rise of the dark web, has produced an environment that is conducive to cybercrime activity. Cyber security, on the other hand, might help to reduce your exposure. In light of the fact that practically everyone on our globe has become increasingly dependent on information and communication technology, hackers now have a thriving criminal market to exploit. Many people have become vulnerable to cyber assaults as a result of factors such as the expansion of cloud storage and the proliferation of social media. As a result, cyber security is more vital than ever before. Cyber assaults often render online platforms, such as websites, unattractive or unavailable to users.

Consequently, a terrible reputation may be established, which may be difficult to repair. The protection of your platform against such hazards necessitates the implementation of cyber security measures. It might also aid in the protection of clients against possible hackers. Computer viruses have the ability to spread like wildfire. If you do not keep them under control, they might pose serious difficulties for you and your company. Computer viruses are capable of causing damage to your data and operating system. As a result, it is important to take cyber security seriously since it has the potential to protect your computer systems from infections. The advancement and development of technology have not left the dark web in the rearview mirror. The dark web is a covert cooperation of Internet sites that can only be accessed with specialist web browsers, which are not widely available. It is mostly used for the purpose of concealing Internet activity and maintaining the anonymity and privacy of users. Despite the fact that the dark web may be used lawfully, it is also well-known for being the site of a large number of unlawful activities. On the dark web, criminals have been caught in the act of drug and human trafficking, illicit weapons distribution, software distribution, piracy, and a variety of other prohibited actions, some of which are inconceivable. Since the dawn of technology, the dark web has grown in complexity, as has the dark web itself. It has served as a shelter for cybercriminals and resulted in a rise in danger to those who utilize the internet on a regular basis. The relevance of cyber security has increased as a result of these vulnerabilities.

Categories of Cybersecurity

The form of security that relates to the protection of your computer network from assaults both within and outside the network is known as network security. To keep hazardous viruses and other data breaches at bay, it employs a range of techniques. Network security uses several protocols to thwart attacks while yet giving authorized users access to the secure network. access to the secure network. A firewall, which functions as a protective barrier between your network and external, untrusted network connections, is one of the most critical levels for network security. (Shandler et al., 2021). Based on security settings, a firewall can block or allow traffic into a network. Email security is the most critical aspect in constructing a safe network since phishing assaults are the most prevalent type of cybercrime. Email security might include software that scans both incoming and outgoing communications for potential phishing attempts. By detecting, fixing, and upgrading the security of applications, application security is the most often used approach for making apps more secure. Although most of this happens during the development stage, it also includes tools and tactics to ensure that applications are safe after they have been delivered to the user. Increasingly, programmers are targeting apps with their attacks, making this more important. Detecting and correcting security flaws early in the product enhancement process will make our business safer. Because everyone makes mistakes, the challenge is to find them at the right time. For example, a common coding error might allow dubious sources of information to be used. If a programmer detects these mistakes, they may lead to SQL infusion attacks, resulting in data leaks. Most of our web-based activities are conducted in the cloud. In most cases, online storage structures like Google Drive, Microsoft OneDrive, and Apple iCloud are used. Because of cloud security protocols, it is possible to recover data stored in the cloud if it is accidentally deleted or stolen. Data leaks and system breaches may be reduced to a minimum by avoiding human error or carelessness.

It is vital to safeguard your computer network from both internal and external threats. It uses a variety of methods to avoid malicious malware or other data breaches. Network security employs a variety of protocols to protect the network while allowing authorized users to access it. When it comes to protecting your network from untrusted external connections, a firewall is one of the most critical defenses you may have. A firewall may either block or allow traffic to enter a network, depending on the security settings. Considering that phishing attacks are the most common kind of cybercrime, email security is essential for maintaining a secure network. Email security software that checks both incoming and outgoing messages for phishing attempts may be included in the package.

Application security refers to safeguarding private data inside an app. These security precautions should be applied before the application is deployed. The user may be required to provide a strong password as part of the application’s security measures. Security mechanisms such as two-step authentication, passwords that must be entered twice, and other safeguards may also be included. All internal cybersecurity risks are managed via operational security. To guarantee that a backup strategy is in place if a user’s data is compromised, this sort of management often employs several risk management officers. To ensure operational security, it is essential to educate employees on how to protect their personal information as well as business information.

Threats and damages by Cyber-attacks

Modern cyberattacks, such as malware, phishing, artificial intelligence (AI), and human-made brainpower, as well as cryptographic money, have put the data and resources of organizations, governments, and individuals in constant jeopardy. Cyberattacks known as "phishing" have become more widespread, in which people's personal information and passwords are stolen through email or text messages. There has been a rise in ransomware attacks on high-profile persons and lucrative businesses, where the attackers demand a large sum of money to recover the database. It's not always possible to get ransomware victims to pay since some may not be willing or able to do so, and even if they are, they may not be familiar enough with bitcoin to figure out a method to do so. "Hacked into COVID-19 research data and requesting $1.14 million from The University of California, the photography giant Canon, and were even responsible for deadly instances in this year's cyberattacks" (Gurinaviciute, 2021). Additionally, the Colonial Pipeline ransomware assault is recognized as one of the US's biggest gasoline pipeline ransomware attacks. Cybercriminal outfit Dark Side, which is thought to be in Eastern Europe, was accused by the FBI for the assault, and Colonial has allegedly paid a $5 million ransom to the group (Browne, 2021). This is one of the most significant risks to cybersecurity since criminals are increasingly using artificial intelligence to carry out assaults. A 2.4Tbps Distributed Denial-of-Service assault in August was 140 percent more powerful than the greatest attack bandwidth volume Microsoft observed in 2020, according to the blog by Tom Warren (Warren, 2021). It is quite typical for hackers to employ SQL injection to get access to a database. The successful assault may result in the retrieval, updating, and deletion of data. Identifying and understanding the threat actors and the strategies, methods, and processes is critical to a successful cyberattack response. Criminal gangs, hackers, and terrorist groups, as well as nefarious workers and corporate spies are just a few examples.

Email phishing and other forms of social engineering are the only strategies that may be used to achieve aims by manipulating human psychology. When a user is given access rights for a specific task, the privileges are issued temporarily only. So even if the passwords were stolen, hackers would be unable to access internal systems and critical information (Gurinaviciute, 2021).

To decrypt the infected data, ransomware requires a payment. In 2020, ransom demands will total $1.4 billion, with an average of $1.45 million needed to repair the damage. Ransomware is utilized in 22% of data breaches, making it the third most common malware. Even deadly instances were a result of this year's COVID-19 research data breach and $1.14 million demand from The University of California (UC). A hospital in Germany was held hostage by hackers, and consequently, patient care systems were disabled, resulting in the death of one patient (Gurinaviciute, 2021).

Cybersecurity Implementation and Suitable Technologies

It is the responsibility of every IT leader, professionals, and administrators to make sure that their database, systems, and networks are secured and protected. The use of risk registers, timelines, Gantt charts, and master sheets helps any organization keep track of their performance and aids in evaluating if any infrastructure is needed to the current state of the security environment. The use of antivirus software can prevent possible malware attacks by monitoring traffic as it keeps track of multiple logins attempts and specific patterns such as byte sequences. According to Cristina Lago, “Five of the top network monitoring products on the market, according to users in the IT Central Station community, are CA Unified Infrastructure Management, SevOne, Microsoft System Center Operations Manager (SCOM), SolarWinds Network Performance Monitor (NPM), and CA Spectrum” (Lago, 2019). The cost to repair the database system and retrieve the lost information is very costly, so the CIOs are responsible for following best practices to maintain their reputation and integrity. There is always a greater risk of cyberattacks as cyber threats are evolving rapidly. ‘It’s always the best idea to keep our software, associated systems, and networks updated as it helps us to keep us safe from security patches, and any out-of-date software should be patched to the latest security version(Thomas, 2006). It is better not to click on links or text from unfamiliar websites or unknown senders in emails and texts since they may be infested with malware. Encrypting and protecting websites, browsers, and servers with an SSL is required for businesses of all sizes. Management teams must be prepared for the inevitable, react to new threats, and recover fast after an assault. Social engineering may be thwarted through awareness, training, and strategies.

Because of the COVID-19 epidemic and its effect on remote work, cybersecurity has been hit hard. Cyberattacks are becoming more complex and nastier as the number of competent black-hat hackers and sophisticated tools on the dark and deep web grows. A sophisticated cyber security technique, artificial intelligence, offers extra information and authentication depending on numerous characteristics while data, logs, and transactions are examined using deep learning technology. A user’s identity may be verified using embedded authenticators since pin and password are currently insufficient to safeguard hardware. With the introduction of its sixth generation of vPro chips, Intel has taken a giant step forward in this area. “Human mistake is the major source of data breaches, and blockchain technology automates data storage to eliminate this risk” (Singh, 2021).

AI investments are needed to develop the practice and theory of secure AI-enabled system construction and deployment. To ensure training safety, protect models from adversarial inputs, and verify the model’s robustness, privacy, and fairness, extensive AI management activities are required. For the safe and secure usage of AI-human systems and environments, this includes AI-based security measures. When it comes to integrating artificial intelligence into cyber-physical and computational systems, it will need an engineering discipline and practice, as well as a scientific understanding of the subject matter. To address cybersecurity’s persisting issues, research efforts must implement AI systems throughout key infrastructures. Monitoring the network for software analysis methods, detecting abnormalities with the goal of finding code vulnerabilities, and cyber reasoning systems for synthesizing defensive patches at the first hint of an attack are all currently available approaches. It’s possible that AI systems might undertake these studies in seconds rather than weeks or days; in theory, cyberattacks could be repelled and monitored. However, there is a requirement for safe deployment to understand the many aspects and the repercussions of these AI activities.

Cybersecurity in the United States may use AI to expand awareness, react in real-time, and improve overall effectiveness, just as AI systems need innovative cybersecurity tactics and technologies to improve their resilience and trustworthiness. Self-adaptation and modification are also part of this, in reaction to persistent assaults that change the balance of power between the attackers and the defenders. There are several ways that AI may be used to classify assaults, as well as to guide adaptive responses at scale, such as swiftly recognizing discrepancies and understanding how to fix them, and aiding the adversary’s vulnerabilities, employing techniques of observation, and accumulating learned lessons. It is possible to protect networks against cyberattacks with a small team of cyber defenders. As a result, system security might be expanded, making it abundant and providing the domain knowledge needed to resolve challenges like deterioration of system behavior and quality-of-service limits.

Data generated by current technological systems may be processed more efficiently using AI technology. For AI system development and innovation, this capacity helps to provide the necessary training data. Cybersecurity concepts may be applied to both human-in-the-loop systems and fully automated ones, making them more reliable. Identity management and software solutions might be two possible subjects for discussion. AI can be used to find every fault in a program, as can a review of best practices, the identification of security flaws, and the facilitation of security design for system developers. Coding modifications are a common occurrence in today’s software development. Using AI-based “coding partners” to assist analysts and developers who are less talented in comprehending complex, massive software systems, as well as to advise them on the strength of recommended code revisions and security, would be advantageous.

Additionally, artificial intelligence can aid in the consistent operation and implementation of software systems. After building the code, it is suggested to use artificial intelligence to identify low-level attacks, as well as to inspect logical faults, configuration, and application domain, and come up with best practices to protect them. Due to its widespread use by government and business entities in the United States, the creation of open-source software for AI-based security enhancements has unique and impactful potential. (Obeidat et al., 2015).

Access control and identity management are other planned AI used. Adversaries can undermine many strategies simply by stealing authorization tokens. It is recommended that an AI-based system be utilized, which is based on a history of expected behavior and interactions, as well as being difficult to defeat, transparent, and lightweight. For biometric identification systems, AI can minimize risks and improve accuracy. However, AI tracking of interacting habits might lead to privacy infringement. (Shneiderman, 2020).

Career opportunity in Cyber Security

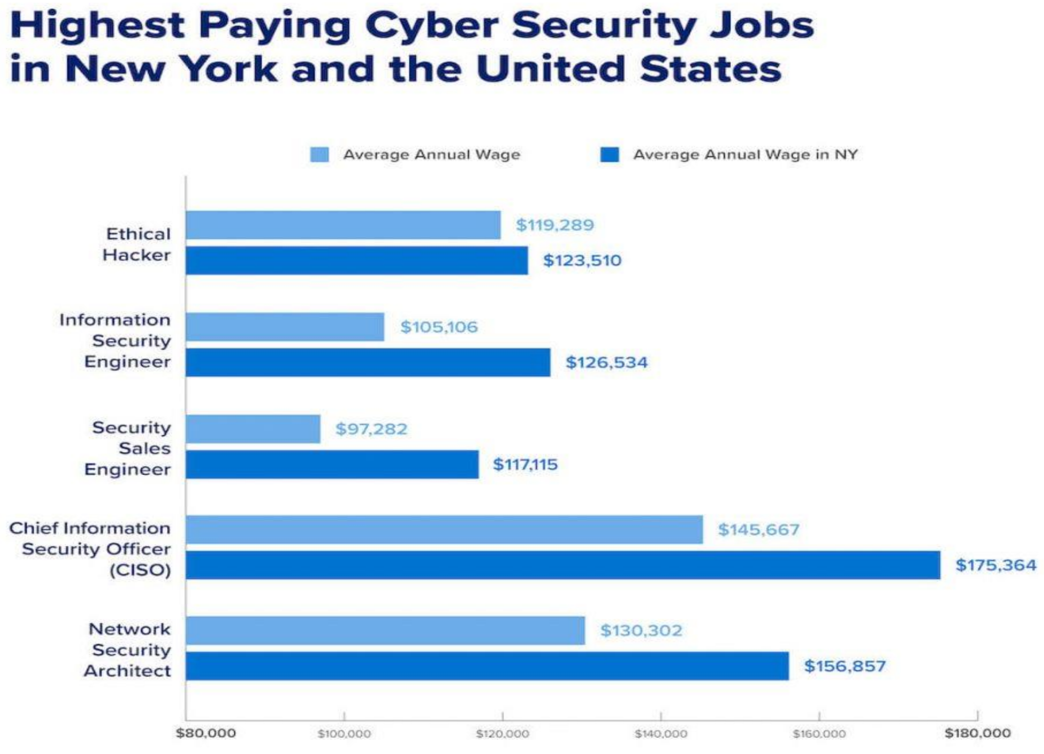
Cyberattacks generate challenges for businesses across a wide range of sectors, including the hotel, healthcare, and insurance industries, among others. Hackers make use of security flaws to steal personal information such as social security and credit card numbers, medical information, passwords, and trade secrets from businesses. Once this information has been obtained, hackers may sell it to the highest bidder or demand a ransom from the firm from whom it was obtained.

Hackers gained access to a central Marriott reservation database in November 2018, stealing information such as names, addresses, credit card numbers, and passport numbers. With 383 million guests compromised, the hack is one of the top five greatest data breaches in history, according to the FBI. According to CNET, Marriott's offer to pay for the stolen passports might result in a loss of $577 million in revenue, as well as unfavorable publicity and a loss of customer trust (Simmons, 2021).

In July of this year, a data breach exposed 100 million Capital One applications that had been created between 2005 and 2019, and the stolen information includes 140,000 Social Security numbers, 80,000 bank account numbers, residences, zip codes, and birth dates, among other pieces of information (Simmons, 2021). Because enterprises of all sizes and types are increasingly reliant on computer networks and systems for their day-to-day operations, cybersecurity graduates may find employment in almost every sector. Some sectors, on the other hand, employ a greater number of cybersecurity specialists and pay them more generously than other industries. Industries may have a wide range of criteria for employees, as well as differences in job titles, pay, and work tasks. Prior to accepting a job offer, cybersecurity graduates should examine the usual career paths and compensation expectations for various sectors in their field (Simmons, 2021).

The computer systems design and associated services business is the most popular industry for information security analysts to work in. Aside from business and enterprise management, other important sectors requiring information security analysts include credit intermediation and associated activities; management and scientific/technical consulting services; and insurance carriers. Information security analysts are in high demand in a variety of sectors, including nonresidential building construction, semiconductor, and other electronic component production, legal services, and automobile repair and maintenance, among others. The financial business is another high-paying job for information security experts. The following tables provide a more in-depth breakdown of the top industries requiring information security analysts.

According to Christine Izuakor's article, "During the last year, while many industries saw decreases in opportunity due to the economic volatility and uncertainty that came with navigating an unprecedented global pandemic, the cybersecurity industry continued to grow" (Izuakor, 2021). The advent of cyber technologies has provided a wide range of career opportunities in the field of cybersecurity. Organizations need to have cybersecurity professionals who can deal with the vulnerable risks of cyberattacks. Most cybersecurity jobs require an individual with a bachelor's degree, while some jobs offer an entry-level position with an associate degree as well. The constantly evolving cybersecurity can be commonly categorized into management, technical and senior leadership. The management includes security governance and oversight roles, and the career opportunities include but are not limited to training & awareness, audits & compliance, third-party risk management, and project management. The technical area covers technical roles which aim to prevent, detect, and respond to cyber threats. The example opportunities include, but are not limited to, cloud security, identity, and access management, security engineering, security operations, and ethical hacking. The senior leadership and company culture focus on the people, and the career opportunities include, but aren't limited to, chief information security officer, managers, and directors of domains. Cybersecurity also includes other career options such as computer forensics, cybercrime investigators, data protection officer, malware analyst and security software developers. Figure 1 compares the national average annual salary to the annual salary in New York for ethical hackers, information security engineers, security sales engineers, CISOs, and network security architects ("What are the highest paying cybersecurity jobs? plus," 2021).



ZipRecruiter, "Real Salaries from Real Employers." (2021)
https://www.ziprecruiter.com/Salaries

Figure 1: Cyber security jobs with the highest pay in New York and the United States in 2021 Adapted from "*What Are the Highest Paying Cyber Security Jobs? Plus, a Special Guide to NYC Salaries*." Columbia Engineering Boot Camps. Retrieved December 5, 2021, from https://bootcamp.cvn.columbia.edu/blog/highest-paying-cyber-security-jobs-starting-salary-nyc/.

Conclusion

There is no one-size-fits-all approach to security issues. They operate differently depending on the operating system. To encourage best practices, the necessary regulations must always be in place, and the first steps must start at the top. The term cyber security encompasses all the technologies and tactics that are used to protect computer systems and electronic data. It’s a large and rising sector in a world where more and more of our business and social lives are conducted online. Thanks to the rapid evolution of cybersecurity, there is no indication of slowing down. Your computer network’s protection from internal and external threats is referred to as “network security.” Everyone who works in IT must ensure that their databases, systems, and networks are safe and secure.

References

Bailetti, T., & Zijdemans, E. (2014). Cybersecurity startups: The importance of early and rapid globalization. *Technology Innovation Management Review*, *4*(11). Retrieved from https://timreview.ca/article/845

Bishop, M., & Goldman, E. (2003). The strategy and tactics of information warfare.*Contemporary Security Policy*, *24*(1), 113-139. Retrieved from https://www.tandfonline.com/doi/abs/10.1080/13523260312331271839

Browne, R. (2021, May 18). *Hackers behind Colonial Pipeline attack reportedly received $90 million in Bitcoin before shutting down*. CNBC. Retrieved September 28, 2021, from https://www.cnbc.com/2021/05/18/colonial-pipeline-hackers-darkside-received-90-million-in-bitcoin.html.

Columbia Engineering Boot Camps. (2021, July 7). *What Are the Highest Paying Cyber Security Jobs? Plus, a Special Guide to NYC Salaries*. Columbia Engineering Boot Camps. Retrieved October 14, 2021, from https://bootcamp.cvn.columbia.edu/blog/highest-paying-cyber-security-jobs-starting-salary-nyc/

Crawford, B. C. H. (1999). Information warfare: Its application in military and civilian contexts. *The Information Society*, *15*(4), 257-263. Retrieved from https://www.tandfonline.com/doi/abs/10.1080/019722499128420?journalCode=utis20

Fung, B. (2021, August 16). *Colonial pipeline says ransomware attack also led to personal information being stolen*. CNN. Retrieved October 14, 2021, from https://www.cnn.com/2021/08/16/tech/colonial-pipeline-ransomware/index.html.

Furnell, S. M., & Warren, M. J. (1999). Computer hacking and cyber terrorism: The real threats in the new millennium? *Computers& Security*, *18*(1), 28-34. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167404899800066

Grabosky, P. N. (2000). *Cybercrime and information warfare*. Australian Institute of Criminology. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.519.6210&rep=rep1&type=pdf

Gurinaviciute, J. (2021). 5 biggest cybersecurity threats. Retrieved from https://www.securitymagazine.com/articles/94506-5-biggest-cybersecurity-threats

Hayes, S., Shore, M., &Jakeman, M. (2012). The changing face of cybersecurity. *ISACA Journal*, *6*, 29. Retrieved from https://gattonweb.uky.edu/Faculty/Payne/ACC624/8-ISACA%20-%20The-Changing-Face%20of%20Cybersecurity.pdf

House, W. (2016). Fact sheet: Cybersecurity national action plan. *The White House*. Retrieved fromhttps://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

Izuakor, C. (2021, September 22). *Find a cybersecurity career*. Cybersecurity Guide. Retrieved October 14, 2021, from https://cybersecurityguide.org/careers/.

Lago, C. (2019, July 10). *How to implement a successful cybersecurity plan*. CIO. Retrieved September 28, 2021, from https://www.cio.com/article/3295578/how-to-implement-a-successful-security-plan.html

Lehto, M., &Neittaanmäki, P. (Eds.). (2015). *Cyber security: Analytics, technology and automation* (Vol. 78). Springer. Retrieved from https://link.springer.com/content/pdf/10.1007/978-3-319-18302-2.pdf

Lin, H., & Kerr, J. (2018). On cyber-enabled information/influence warfare and manipulation. *Influence Warfare and Manipulation (August 8, 2017). in an Oxford Handbook of Cybersecurity*. Retrieved from https://www.americanbar.org/content/dam/aba/administrative/law_national_security/Herbert%20Lin%20Cyber-Enabled%20Info%20Influence%20Warfare%20and%20Manipulation.authcheckdam.pdf

Obeidat, M., North, M., Richardson, R., &Rattanak, V. (2015, January 2). *Business Intelligence Technology, Applications, and Trends*. DigitalCommons@Kennesaw State University. Retrieved November 1, 2021, from https://digitalcommons.kennesaw.edu/facpubs/3445/.

Patterson, N. (2021).What is Cyber Security and Why is it Important? Retrieved December 1, 2021, from https://www.snhu.edu/about-us/newsroom/stem/what-is-cyber-security

Rathmell, A. (1997). Cyber-terrorism: The shape of future conflict? *The RUSI Journal*, *142*(5), 40-45. Retrieved from https://www.tandfonline.com/doi/abs/10.1080/03071849708446185

Shandler, R., Gross, M. L., Backhaus, S., & Canetti, D. (2021). Cyber terrorism and public support for retaliation–a multi-country survey experiment. *British Journal of Political Science*, 1-19. Retrieved from https://www.cambridge.org/core/services/aop-cambridge-core/content/view/179C0560441076100DB4A4E5BBCB992F/S0007123420000812a.pdf/cyber-terrorism-and-public-support-for-retaliation-a-multi-country-survey-experiment.pdf

Shneiderman, B. (2020). Human-centered artificial intelligence: Reliable, safe & trustworthy. *International Journal of Human–Computer Interaction*, *36*(6), 495-504. Retrieved from https://www.tandfonline.com/doi/abs/10.1080/10447318.2020.1741118

Simmons, L. (2021). Cybersecurity Jobs: Overview. Retrieved from December 1, 2021, from https://www.cyberdegrees.org/jobs/

Singh, S. (2021, July 16). *Potential Use Cases of Blockchain Technology for Cybersecurity*. IT Business Edge. Retrieved October 16, 2021, from https://www.itbusinessedge.com/security/potential-use-cases-of-blockchain-technology-for-cybersecurity/.

The fascinating evolution of cybersecurity.(2018). La Trobe University. Retrieved December 2, 2021, from https://www.latrobe.edu.au/nest/fascinating-evolution-cybersecurity/.

Thomas, T. L. (2006). *Cyber Mobilization: A Growing Counterinsurgency Campaign*. FOREIGN MILITARY STUDIES OFFICE (ARMY) FORT LEAVENWORTH KS. Retrieved from https://apps.dtic.mil/sti/citations/ADA465348

Warren, T. (2021, October 12). *Microsoft says it mitigated one of the largest DDoS attacks ever recorded*. The Verge. Retrieved October 14, 2021, from https://www.theverge.com/2021/10/12/22722155/microsoft-azure-biggest-ddos-attack-ever-2-4-tbps.