Farah Alhamzawi

Independent Study and Mentorship

Mr. Green

September 1, 2023

Research Assessment #1

For this assessment, I decided to look into the depth of cyber security. When individuals think of cyber security, they only think of protecting themselves from becoming a hacker or something secretive and dangerous. However, that is not even a fraction of cybersecurity. Cyber Security consists of 5 sectors known as the Cybersecurity Lifecycle: Identification, protection, detection, response, and recovery. There is no order in how this cycle runs; depending on the sector a profession is in, the cycle starts there and ends in a different sector. In Cyber Security Identification, professionals identify the party's assets and track and organize their access to data. The next sector would be protection; professionals in this sector identify the assets and develop a solution to protect the assets, as well as conduct security training so that no user information is compromised. Moving onto the Detection Sector, professionals monitor the threats proactively through data logging and security testing. Then, there is a response; once the threat is detected and active, professionals in this sector create a response plan (or CIRP), which includes cyber insurance if there has been any damage to the party's assets. Finally, the recovery sector ensures and establishes a business continuity plan, which helps bring operations back to normal after a cyber attack. These sectors are important and keep users' information secure from cyber threats. In the next couple of paragraphs, I will explore how vital cyber security protection is in our society, from major cyber attacks, transitioning to personal attacks, and ending with personal protection from cyber attack attempts.

MLA Citation:

Team, Threat Intelligence. "Global Ransomware Attacks at an All-Time High, Shows Latest 2023 State of Ransomware Report." Malwarebytes, 3 Aug. 2023, www.malwarebytes.com/blog/threat-intelligence/2023/08/global-ransomware-attacks-at-an-all-time-high-shows-latest-2023-state-of-ransomware-report.

Assessment: Global Ransomware Attacks at an All-Time High, Shows Latest 2023 State of Ransomware Report.

In the past year or two, there have been many ransomware attacks on the global level. Ransomware is malicious software or malware that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. These attacks are done using the information accused by these ransomware attacks and will only give the information back if the amount they request is offered. The United States, Germany, France, and the United Kingdom have had one thousand and nine hundred total ransomware attacks within a year. These attacks started in a surge from July 2022 through June 2023. Makeware bytes threat intelligence team states, "The U.S. shouldered a hefty 43% of all global attacks, which means the U.S. has become the main target for these attacks, with around 1462 attacks recorded just last year. They also predict that there will be a new threat because of the CLOP company. CLOP is a Russian ransomware gang known for demanding multimillion-dollar payments from victims before publishing data it claims to have hacked. Through their significant influence on the dark web, they are selling this ransomware to other hackers, who are targeting the U.S. and are predicting that the next target is the United Kingdom. If CLOP keeps creating this

ransomware, the attacks will become more aggressive, which will cause vulnerability-focused models.

While reading this article, my fascination for cyber protection peaked. I found it fascinating yet dangerous that someone can easily find your information through fake emails, weak passwords, or even fake websites that look legit. When someone adds something to the Internet, it will never go away, even though many think so. Hackers can track your information and learn a lot about you with that information. That is why an individual must check what they post on social media or online, as well as think if they want that type of information to be leaked, because if there were only 1462 attacks that they know of, which means there are a lot more then that, which means that over 1400 business, as well as people, have had there information held for ransom because they either added information on the Internet they did want to be leaked or they have essential identification that was not protected well enough. Either way, these are perilous times that keep getting more dangerous. For that reason, personal protection is important, and I decided to research cyberattacks and the government's protection plans for cyberattacks.

MLA Citation:

Irwin, Luke. "List of Data Breaches and Cyber Attacks in 2023." *I.T. Governance U.K. Blog*, 1 Aug. 2023, www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023#june-2023.

Assessment: List of Data Branches and Cyber Attacks in 2023

This article states all the types of Cyber Attacks that occurred this year. Through these statistics, it is apparent to see how vulnerable we are to cyber-attacks. According to the article, 87 publicly disclosed incidents just in July accounted for over 140 million compromised records. That makes me frightened about the other incidents and the incidents that have not been recorded. The most extensive data attack was on a popular online messaging platform, TIGO, which leaked over 700,000 customers' data, including names, usernames, credit cards, I.P. addresses, photos, and more. With that information alone, a hacker could easily steal a person's identity. Because they have the I.P. address and banking information, they could hack into those accounts and steal even more personal information.

Moreover, if a cyber attack could find that much information on a social media platform, imagine if it was a larger company than that. I was astonished at their weak security systems, even though that platform was popular in China. They would have more substantial data protection for something with that much popularity. However, they did, and as a result of this information being leaked, TIGO is facing many lawsuits from every side. When I was reading through this, I kept wondering why this was so important. I started thinking that if you can get so much information just through a social media platform that might have had a strong enough security firewall with such ease, then what can these hackers really do? Does this mean that these dark hackers have become better, or is our reliance on the Internet caused us to become more vulnerable to these attacks?

MLA Citation:

"Protect Myself from Cyberattacks: CISA." Cybersecurity and Infrastructure Security Agency CISA, America's Cyber Defence Agency, 28 Aug. 2023, www.cisa.gov/news-events/news/protect-myself-cyberattacks.

Assessment: Protect Myself from Cyberattacks: CISA

Because of all the cyber attacks made on the United States in the past couple of years, the United States has set up an online militia to protect citizens from cyber attacks; however, everything in the tech field could be better, from coding to I.T. to Cybersecurity. For that reason, this article presents ways for individuals to protect themselves and the assets they want on their devices. Some topics they address include identifying emails, not giving out personal information online, secure passwords, software updates, authenticity protection, and paying attention. First, the most common way to get hacked is by opening a suspicious email or text and trying to identify what is in it.

I found this interesting because I read this article the day before I went into my cyber security class, where we talked about suspicious emails, and that helped me get a clear understanding of why it is so important to pay attention to what you are clicking into on the Internet; never go in blind. Two types of emails/texts are usually sent by unknown people, either phishing or spam. Spam emails are when an officially registered company sends recurring emails to persuade the user to buy from their store; this is done as a marketing strategy. While phishing emails are quite the opposite. A phishing email is when a cyber attacker sends a user a fake email, which is implanted with malware or a virus, to get the user's information. Many people would have unknown viruses downloaded into their devices by clicking on the website addresses linked to the email, allowing hackers to get the information they were looking for. To protect yourself from this, an individual has to be very observant about emails. From looking at the email address, I can identify if a legitimate company is emailing me or if a phished is trying to access my information. From that, if I identify it as a phishing email, I report it and delete it. Phispher's overlook small details like that, so it is vital to identify every aspect of an email, from the email address to how the email is formatted to how it ends. Everything is important!

Another thing that I found to look out for is weak passwords. With the information that I have learned in my Cyber security class, as well as the article, I can conclude that passwords such as "password" or "123456789" can easily be hacked in less than a millisecond; that is why it is essential to have different passwords for each application and website which has uppercase letters, lowercase letters, numbers, and symbols that mean do not symbolize anything important to you. For example, if I put my password as my high school and birthday, then anyone can know that information because they can just ask me or search it up; instead, if I add the first letter of my favorite quote in a book with a random number combination, then it is harder to hack. There are two types of password cracking: dictionary-based and brute force attacks. The dictionary-based attacks are when they use only singular words from the standard dictionary that do not include slang words, numbers, or symbols to try to crack a code. In contrast, brute force attacks are when a hacker uses an application that helps them determine the password based on the letters, numbers, and symbols used until the password is cracked. The shorter the password is, the easier it is to crack.

The final important thing I learned from this article is never to share personal information online and with unknown people. For instance, if a random person comes up to you, do not share anything about where you live, your friends, or anything about that because anyone can be your hacker, so you always have to protect yourself. Also, keep the information private on social media, like location, family, and personal issues, because anyone can use that information to hack into your account or use it as ransom to get to you.

I believe I only know the basics of cyber protection based on the articles I have read. Before reading these articles, I never knew that we as individuals are so vulnerable to cyber-attacks, and that makes me frustrated because if a hacker can crack a strong password in a couple of hours, what could they do if theft is given a week? For that reason, I believe I have a lot to learn about cyber security, and even though I want to focus on the protection side of cyber security, I want to know how the other sectors are essential when it comes to the sector I am studying. I hope that with the information I have learned in these articles, I will use them as a stepping stone in learning more about cyber protection of an individual's information because I find that it is crucial to secure an individual's identity as well as important information that should not be leaked. I am exploring this field because I find an interest in helping others, and the best way to do that is by searching for it through my curiosity in cybersecurity.