Analytical Paper

Matt McClintock

December 8, 2021

CYSE 201T

Prof. Bowman

As we all know, there is an obvious connection between the advancement of technologies in society and problems that arise from a cyber security angle. These problems arrange from different aspects from cultural, ethical, political domains and more. Combatting these issues can be done using both technical skills and looking at the issue from an interpersonal scope.

A common victim in cyber security related attacks are small businesses. Small businesses are easy targets for hackers as they have a smaller budget to spend on cyber security operations. This and tied with the fact that 1 in 4 small business owners have little knowledge of these attacks make a recipe for massive profit or even business loss. The first thing Small Business should do is understand their risks that way they know where to put the most effort. Next, they should use some money to bring in some personnel to create a risk management plan. This team will identify the risks and levels of protection they involve. With all this going on there needs to be the cost of buying all of the equipment for these processes. Being a small business, there isn't enough money to buy a whole security team worth of computers and servers. It is important to have some though, and on those devices have anti-malware programs as well as a firewall setup. As you can see things can add up quick when developing a cyber security program. However, I believe the costs are a good investment to protect the business from a cyber-attack. These attacks can be business ending so it is imperative that these small businesses have some sort of security program in place.

Another common victim for cyber-attacks are large industrial organizations. Specifically, those that use SCADA systems. Supervisory control and data acquisition is a control system architecture comprising computers, networked data communications and graphical user interfaces for high-level supervision of machines and processes

SCADA systems are industrial control systems that are used to supervise and control machinery or other processes (2). The processes can cover a large region such as electrical plants. SCADA systems are very versatile and are found in many places all over the world. Unluckily, because these systems are a part of huge networks they are often targets to cyber-attacks. These attacks have the potential to harm many people especially in places that the SCADA systems are used in volatile areas. For example, a nuclear plant. Another way that these attacks can have real world consequences is in a breach that attacks power generation or water treatment centers. These industries all use SCADA systems, so it is very important that they are as secure as possible.

One topic I have always found interesting is the dynamic of cyber bullying and harassment connected to anonymity. "The fact that an individual can purchase a temporary cell phone which does not require a registered name or can create social networking accounts using pseudonyms is a serious concern for legislators, law enforcement, and prosecutors when attempting to deter and respond to CH/CS." (3). On every social media site, you will find those with hateful and harming posts or comment that are on fake accounts. Fake account meaning they either have no name/pictures or they use someone else's name/picture, both equally harming. This anonymity gives offenders a sense of protection almost like a shield that protects them from any repercussions on their actions. These accounts are breeding grounds for things like cyber bullying, cyber stalking, and cyber harassment. As stated in this paper, it can make it hard for law enforcement to find these people when conducting an investigation. So, what can be done? Maybe these social media sites should require some forms of valid identification whether it be a selfie or a driver's license. However, in doing this it will no doubt spark major controversy and privacy. It will be hard to find the line between securing privacy while also having the safety of verifying these accounts.

This constant battle between privacy and safety is one that may never be fully solved. Having privacy does provide secrecy, but it also provides independence and freedom which I believe is very crucial. The notion that "I have nothing to hide, so why do I need privacy?", takes away your liberty. Who's to say that what's legal today, doesn't become illegal the next day? Those who act immorally behind the shield of secrecy still deserve privacy the same way the freedom of speech allows people to say whatever they want (to an extent). On the other side, if that immoral act turns in to something illegal it should be reprimanded that same way yelling "fire" in a movie theatre would. Concluding, privacy is a given right that should not be taken away from us because it gives us the freedom to be ourselves without any judgmental eyes watching us.

Conclusion

Cyber security, although a relatively newer field, is very wide and has become a part of the world as we know it. As more innovative cyber related technologies advance our society, it will also create more opportunities for criminal behaviors. It is important that we continue to not only use technical skills to defer these attacks but also interpersonal approaches. We have to be able to use cultural and ethical concepts. It is only a benefit when you are able to see things from a different approach and use societal standards to examine a situation. We have to examine how things like social media impact the victimization rate of people in society. Social media has had a massive grip on society in the past decade, especially in teens and young adults. Oversharing has become a word and making sure you are being proactive when using social media is a must. Its also vital to have a sense of how cyber security has had an impact across the world and has changed processes globally. More and more companies are encrypting their data to protect themselves from third party attacks (1). Ultimately, cyber security is more than hacking and coding. It is an advanced filed that combines social sciences into the mix.

Combining these skills will make whoever possess them a strong asset that can help protect companies from cyber attacks.

Citations

1. *How Is Cyber Security Changing in the World of Digital Information?*, https://www.ecpi.edu/blog/how-is-cyber-security-changing-in-the-world-of-digital-information.
2. "What Is SCADA?" *Inductive Automation*, https://inductiveautomation.com/resources/article/what-is-scada#:~:text=Supervisory%20control%20and%20data%20acquisition%20(SCADA)%20is%20a%20system%20of,that%20allows%20industrial%20organizations%20to%3A&text=Directly%20interact%20with%20devices%20such,%2Dmachine%20interface%20(HMI)%20software.
3. Ariyadasa, author: Aparrajitha. "Harassment beyond Borders; Can Victims Be Protected by Cyber Bullying in Sri Lanka? ." *Colombo Telegraph*, 20 Apr. 2019, https://www.colombotelegraph.com/index.php/harassment-beyond-borders-can-victims-be-protected-by-cyber-bullying-in-sri-lanka/.