Jeggo Paolo V. DyCok

CYSE200T

Analytical Paper

INTRODUCTION:

An ex-chief executive of Microsoft Steve Balmer once said “The number one benefit of information technology is that it empowers people to do what they want to do...” Technology has indeed empowered people and it has reshaped society as we know it. With the growing trend of technology, society has taken on a new form as it integrates with our growing need for efficiency. Despite its growing benefits, cybersecurity-related technical systems have also created certain problems that can negatively affect its users as virtual communication evolves to normalcy. The social meaning of cybersecurity-related technical systems has become increasingly impactful in ways that it has bolstered our need to protect personal data, identity and the overall structure of businesses and society’s critical infrastructures. It is difficult to ascertain as to what end cyber technology would go as it branches out into multiple mediums that has its positive and negative effects. This essay will describe how critical infrastructure management systems such as SCADA as well as small business must continue to develop in order to sustain societal functions and the impact of framework in its structure.

(1) Industrial systems are built on a myriad of systems that support each other in order to sustain the service they provide. SCADA (Supervisory control and data acquisition) is a system of applications utilized for controlling industrial processes which has the function of gathering data in real time from distant locations to provide an accurate statistic of equipment and conditions in which machine systems operate. It represents the heart and brain of processes that control critical

infrastructures ranging from traffic lights, to manufacturing systems. SCADA was built with the tools needed to facilitate data-driven functions regarding industrial processes. SCADA is comprised of software and hardware systems that work hand in hand to compile data needed to accurately monitor real time processes for accurate control. The hardware systems of SCADA gather and deliver information to the software to produce readable data. Just like computers and computer systems, SCADA is prone to vulnerabilities. Its systems of sensors, controllers, software can be a subject of attack from malicious actors. Successful attacks on SCADA can prove to be fatal for societies that utilize and depend on its benefits. These damages can involve disruption of certain services such as oil, gas, water, waste treatment, manufacturing, energy and even food production. Improvements in modern SCADA will continue to provide benefits in the future, however lingering vulnerabilities make them perfect targets for bad actors. According to data ranging from 2015 to 2019, the number of vulnerabilities has been continuing to rise with the number surpassing tripled amount from 2017's 144 vulnerabilities to 2018's 467. The rise in vulnerabilities stem from the use of mobile devices used to control PLCs and RTUs, which can be easily compromised due to their wireless features. Continuous use of strong passwords, multifactor authentication, input validation and updates will be the best policy for security to continue reaping benefits of using legacy and modern SCADA.

Any forms of damage have been proven to cause rippling effects to society's overall capacity no matter how big or small. Industries, critical infrastructures and small business have been the more favorable target of bad actors as much as individual user. With that in mind, it is more vital to focus on less cybersecure entities as they tend to be targets for bad actors. Small businesses are commonly less secure than large businesses and they often are a target for malicious entities, especially when they are linked with any other businesses that rely on their

services. Although it is true that they don’t often have the best security around, they can still maximize their capabilities with simple practices that can take them a long way with regards to maintaining security. For starters, small businesses need to focus on physical security. This can be done by locking doors, limiting access to certain areas and establishing an account for people to know what they have and don’t have access to. This also applies to virtual access. Employees need to have individual accounts and each account must be configured based on the amount of access they need, and it must be screened from time to time. They must also be limited in terms of what they can and cannot access online. This would involve installing certain filters and blocking non-secure sites that may compromise the system. Another thing that is essential and must be updated is the antivirus software. Antivirus software is a must and would help secure systems on top of blocking certain ports that attackers can take advantage of. Understanding vulnerabilities and threats can help small businesses be aware of what could go wrong. Although not all vulnerabilities can be patched, it is good to know what attackers can use against you and be cautious of utilizing certain functions with the vulnerability. Last, but not least is personnel security training. A good number of attackers rely on social engineering to take advantage of ignorance and curiosity. It is best to make personnel aware of what they should and should not do. The best cybersecurity is taking caution and being continuously educated in the topic.

(4) As mentioned in the previous paragraph, small businesses aren’t necessarily hopeless when it comes to starting and maintaining their security overall. Cybersecurity can take many forms depending on its subject of protection. In order to properly tailor security to businesses and infrastructures, cyber professionals developed what is known as a framework. Framework is an overview of implementing cybersecurity procedures to better protect the infrastructures vital to the society's functions. It is important that we take framework as a guide in order to create a

backbone to the series of protection implementation for the aforementioned infrastructures because that is what has allowed our society grow to what it is to this day. As technology continues to advance, it is critical that we implement cybersecurity framework to increase our understanding of how to defend what it is that makes everything work together, to uphold and to evolve as technology does on a daily basis. Since Framework is not tailored with very specific procedures and requires flexibility depending on the subject of its nature, cybersecurity framework consists of 5 core activities, Identify, protect, detect, respond and recover. Before we endeavor to protect something, we would first have to identify what it is we are protecting. Identify covers the understanding of how a certain business work, its intricate parts, priorities and core functions, this allows the effective allocation of resources to fortify certain aspects of an infrastructure which leads to protection. Protect serves to reduce the amount of vulnerabilities once the priorities and vulnerabilities have been identified. This allows for proper implementation of safety practices necessary to reduce casualties. Detect allows for the efficient discovery of cybersecurity threats with means of monitoring and detection tools and practices. Respond serves to mitigate and contain the potential damage of a cybersecurity threat. Once the threat has been mitigated, recovery can begin. Recover supports the timely recovery of the entire system to its normal function. This procedure is critical to restore the system to its intended functional capacity.

CONCLUSION:

Cyber-related technology has made a significant impact on society no matter how big or small, and it will continue to do so as we continue to advance in its limitless frontier. We still exist in its younger years and as it grows, so should our awareness. For now, it comes as a standard that we clarify the boundaries of its operability in order to mitigate its negative impacts. Further, it is

also our individual responsibility to educate ourselves in its potential in order to see where it is heading. Societal success depends on the capabilities of our cybersecurity procedures and policies as they serve as a bulwark that protects important components of society such as infrastructures under SCADA and small business with framework as the basis of their development.

WORKS CITED

What is SCADA (supervisory control and data acquisition)? Retrieved December 4, 2022, from https://www.techtarget.com/whatis/definition/SCADA-supervisory-control-and-data-acquisition

One flaw too many: Vulnerabilities in SCADA systems. (n.d.). #1 in Cloud Security & Endpoint Cybersecurity | Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/one-flaw-too-many-vulnerabilities-in-scada-systems

Kevin M. Stine, Kim Quill, et al. "Framework for Improving Critical Infrastructure Cybersecurity | NIST." *ITL Bulletin* -, Feb. 2014.

Comerford, Linda. "Why Small Businesses Are Vulnerable to Cyberattacks." Security Magazine, 25 May 2022, www.securitymagazine.com/blogs/14-security-blog/post/97694-why-small-businesses-are-vulnerable-to-cyberattacks.

St