Analysis of Cybersecurity Systems and Future Policy

Samantha Riggs

December 6th, 2024

Introduction:

The development of technical systems that require cyber security considerations has had a significant social impact on today's society and has influenced the cyber security field as a whole. I believe it is important to consider that there are potential long-term ramifications of these systems that are difficult to predict and should be recognized and addressed when developing future policy and legislation. I believe that the CIA Triad and the NIST Cybersecurity Framework must be used, even if just as a foundation, when developing these policies in order to effectively address present and future cybersecurity concerns.

SCADA Systems and Vulnerabilities Surrounding Critical Infrastructure Systems:

SCADA, which stands for Supervisory Control and Data Acquisition, refers to the systems used to control critical infrastructure processes. These systems allow control and the overall gathering of data from the industrial equipment to be done remotely rather than on site. SCADA constantly monitors the data being received from the equipment and if certain conditions considered to be abnormal are met, it can alert the appropriate human operators. They are complex and can be physically quite large, as these systems are comprised of both hardware and software. Communication within these systems is facilitated through a combination of protocols including IEC, DNP, and TCP/IP (some being comprised of legacy systems). While these systems have hardware that is physically secure and software that is not directly connected to the internet, they are not an exception to a cyber-attack.

CISA (Cybersecurity and Infrastructure Security Agency) is a national coordinator for cybersecurity pertaining to the matter of critical infrastructure. They state that "any threat to these sectors could have potentially debilitating national security, economic, and public health or

safety consequences." Understandably, with the sheer physical size and complexity of these systems, any system failure or hardware faults have the consequence of being costly as well.

Perhaps the largest threat to any critical infrastructure in terms of cyber security would be unauthorized access. These systems control major portions of different infrastructures that keep our country running smoothly, like water and electricity for example. Any unauthorized access to these systems could have drastic and potentially threatening consequences. Any alteration or destruction of these systems could greatly affect a portion, or all, of the country, making unauthorized access a tempting target for those wishing to cause harm.

The CIA Triad, NIST Cybersecurity Framework

Given these vulnerabilities, I believe there is a significant need for future policy and legislation to take potential consequences of the development and implementation of these systems into account. A strong foundation that should be implemented in these future policies should be the CIA Triad.

The CIA Triad is defined as "a model designed to guide policies for information security within an organization." (Chai 2022). This model is composed of three parts : Confidentiality, integrity, and availability. All of these parts provide a solid foundation for an organization's policies and are used to reduce potential vulnerabilities in their systems.

The first letter in the triad stands for confidentiality. This element of the triad ensures that sensitive information is kept private and is only available to authorized users. This data can be categorized by the level of potential damage that could be done should it be accessed by an

unauthorized party. Encryption and the requirement of two factor authentication are ways this element can be included in an organization's security policies.

The second element is integrity. This element is centered around ensuring that data present in a system is reliable and trustworthy. By including this element in security policies, the unauthorized alteration of the data can be prevented. Both human and non-human caused alterations must be taken into account "such as an electromagnetic pulse (EMP) or server crash." (Chai 2022) Data backups in particular are highly important to this element. "Regularly backing up data so that it can be restored to its original state" (University of Tulsa 2024)

The last part of the triad is availability. This element is focused around ensuring that a system or set of data is available to those with authorized access whenever they may need them. Both the hardware and software in a system must be maintained in order to fulfill this element of the triad. Preventative measures to ensure that availability is maintained are key.

The National Institute of Standards and Technology (NIST) is an organization under the U.S. Department of Commerce. The NIST created a framework for cybersecurity policy development in order to provide "guidance to industry, government agencies, and other organizations to manage cybersecurity risks." (NIST, 2024) This framework was developed in a way that any company or organization could utilize the framework and adapt to that organization's specific cybersecurity needs.

Importance of CIA Triad and NIST Framework Implementation:

By utilizing the CIA Triad as a foundation for the development of security systems, especially for systems as important and vulnerable as critical infrastructure systems. The

framework created by the NIST should be followed and taken into consideration and well. Any development of newer systems, along with older ones being upgraded, should include better security measures such as firewalls and specialized VPNs. These upgraded measures will counteract the potential for unauthorized access, a main vulnerability to this industry.

Conclusion:

When discussing the current impact of cybersecurity systems and the way we should go about developing new policies and potential legislation, it is important to acknowledge that there are factors that are not easily resolved, and questions and concerns that can potentially go unaddressed. Additionally, arguments could be made against utilizing these cybersecurity frameworks discussed and the alternative analysis should be considered equally compared to this one.

Given the evidence of the vulnerabilities present and how both the CIA Triad and the NIST Cybersecurity Framework address the vulnerability concerns, I believe that future policy must use both of these guidelines as foundations. These frameworks and guidelines were created with the purpose of being considered and transformed to fit individual organizational needs, and provide, at the very least, a jumping off point for the creation of strong policies. Once again, it is important to consider the importance of systems such as critical infrastructure systems, in which a breach could affect the nation as a whole if cybersecurity policy is not set and followed accordingly.

References

1. *Cybersecurity framework*. NIST. (2024, November 26). https://www.nist.gov/cyberframework
2. Chai W. (2022, June). *What is the CIA Triad? Definition, Explanation, Examples*. Tech Target. https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA?jr=on
3. University of Tulsa. (2024, Jan). *What Is the CIA Triad?*. https://online.utulsa.edu/blog/what-is-the-cia-triad/
4. Critical Infrastructure Security and resilience. Critical Infrastructure Security and Resilience | Cybersecurity and Infrastructure Security Agency CISA. (n.d.). https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience
5. SCADA systems. SCADA Systems. (n.d.). https://www.scadasystems.net/
6. Learn all about SCADA systems: What is SCADA?: Scadapedia. SCADA International. (2024, October 23). https://scada-international.com/what-is-scada/#:~:text=What%20does%20SCADA%20stand%20for,data%20from%20the%20industrial%20equipment