Anthony Gomez-Reyes
Professor Hind Aldabagh
CYSE200T
1 April 2023

Social Meaning and Impact of Cybersecurity-Related Technical Systems

This paper discusses the social meaning and impact of cybersecurity-related technical systems. It analyzes the CIA triad, a model used to define the three key elements of information security: availability, integrity, and confidentiality. The implementation of cybersecurity-related technical systems represents a form of power and control over information, shaping the relationship between individuals and the organizations that hold their information. The impact of cybersecurity-related technical systems can be analyzed at different levels of society, from the individual to the societal level. The paper also discusses the vulnerabilities associated with critical infrastructure systems, including outdated software and hardware, poor network security, insufficient staff training, and the lack of a comprehensive cybersecurity strategy. Finally, it emphasizes the critical role SCADA applications play in mitigating the risks associated with critical infrastructure systems, such as power plants and transportation networks.

Introduction

The development and implementation of cybersecurity-related technical systems have become increasingly important in the digital age. These systems are designed to protect sensitive information and prevent cyber-attacks, but their social meaning and impact go beyond their technical functions. This paper will analyze the social meaning and impact of cybersecurity-related technical systems, examining their role in shaping our society and the potential consequences of their use.

Social Meaning of Cybersecurity-Related meaning

Cybersecurity-related technical systems are used to safeguard critical infrastructure, government agencies, and private enterprises. One of these systems is called The CIA Triad, also known as the AIC (Availability, integrity, Confidentiality) Triad, which is a model used to define the three key elements of information security. The CIA triad is critical in the design, implementation, and management of information systems, ensuring that sensitive information is protected from unauthorized access, alteration, or destruction.

What does CIA stand for?

The CIA Triad Stands for availability, integrity, and confidentiality. Availability refers to the accessibility of information systems and the data they store. This means that authorized users should be able to access the information they need when they need it. Unavailability could result from hardware or software failure, network issues, or malicious attacks.

Integrity refers to the accuracy and consistency of data. Data integrity ensures that data cannot be altered or deleted by unauthorized individuals, or by mistake. This can be accomplished through the use of checksums, digital signatures, and other security measures.

Confidentiality refers to the protection of sensitive information from unauthorized disclosures. Confidentiality is typically achieved through the use of encryptions, access controls, and other security measures designed to prevent unauthorized access to sensitive Information. The CIA Triad is a fundamental model used to ensure the protection of sensitive information in information systems. Authenticated users are then granted specific authorization to access resources based on their identity and permission. Ensuring the availability, integrity, and confidentiality of information through proper implementation of the CIA Triad and the distinction between authentication and authorization is essential for maintaining the security of information systems.

However, these systems also have social meaning beyond their technical functions. They represent a form of power and control over information, shaping the relationship between individuals and the organizations that hold their information. The implementation of

cybersecurity-related technical systems can have significant implications for social and political relationships, as well as for the distribution of power.

Impact of Cybersecurity-Related Technical Systems

The impact of cybersecurity-related technical systems can be analyzed at different levels of society. At the individual level, these systems can influence the way people perceive privacy and security. In some cases, individuals may feel that their privacy is being violated when they are subject to increased surveillance or when their data is collected and stored. On the other hand, others may feel more secure knowing that their personal information is being protected.

At the societal level, cybersecurity-related technical systems can have implications for power dynamics between organizations and individuals. The implementation of these systems can reinforce existing power structures or create new ones. For example, SCADA (Supervisory Control and Data Acquisition) system. SCADA systems are a type of industrial control system that is used to monitor and control processes and operations in critical infrastructure systems such as power plants, water treatment facilities, and transportation systems. It consists of a network of sensors, controllers, and software that collect and analyze data in real-time to provide operators with insights into the performance of the system. SCADA systems can be used to monitor various parameters such as temperature, pressure, and flow rates, and can also be used to control devices such as valves, pumps, and motors. They allow operators to remotely control and monitor critical infrastructure systems, increasing operational efficiency and reducing the risk of accidents or equipment failures.

Vulnerabilities associated with critical infrastructure systems.

Critical infrastructure systems such as power grids, water supply systems, and transportation networks are vital to the functioning of society, making them attractive targets for cyberattacks and various types of threats, including physical attacks, natural disasters, and cyberattacks. Cyber threats are of particular concern as they can be launched remotely, anonymously, and on a large scale, potentially causing significant damage to the infrastructure and disrupting essential services. Some of the vulnerabilities associated with

critical infrastructure systems include outdated software and hardware, poor network security, insufficient staff training, and the lack of a comprehensive cybersecurity strategy. These vulnerabilities can be exploited by attackers to gain unauthorized access, disrupt services, steal sensitive information, or cause physical damage. It is crucial to identify and address these vulnerabilities to ensure the resilience of critical infrastructure systems and maintain the safety and well-being of society.

Role SCADA applications play in mitigating these risks.

SCADA (Supervisory Control and Data Acquisition) applications play a critical role in mitigating the risks associated with critical infrastructure systems, such as power plants and transportation networks. These applications provide real-time monitoring and control of the systems, allowing operators to identify and address issues before they become serious problems. By remotely monitoring and controlling various parameters such as temperature, pressure, and flow rates, SCADA systems reduce the risk of accidents or equipment failures and minimize the impact of any disruptions. Moreover, SCADA systems employ various security measures such as access control, encryption, and intrusion detection to prevent unauthorized access and protect against cyberattacks. SCADA systems are crucial in today's world where we rely heavily on technology to manage and monitor various processes and infrastructure. Overall, SCADA systems have revolutionized the way we work and monitor industrial processes, and their continued development and implementation will only serve to improve our ability to optimize operations and increase efficiency, but governments may use cybersecurity-related technical systems to control information and suppress dissent, limiting individual freedoms and rights.

Human Factor in Cybersecurity

Additionally, cybersecurity-related technical systems can have significant economic impacts. The cost of implementing and maintaining these systems can be high, particularly for smaller businesses or organizations. This can create a barrier to entry, limiting competition and potentially leading to market consolidation. That's why I believe Balancing the tradeoff between employee training and additional cybersecurity technologies is a critical consideration when managing a limited budget for cybersecurity. Both training and

technology are essential elements of a comprehensive cybersecurity strategy, but it is crucial to determine where to allocate the limited resources to maximize their impact. I think it is essential to prioritize employee training when working with a limited budget. A well-trained staff is better equipped to recognize and prevent cybersecurity threats, which can significantly reduce the risk of a successful cyber-attack. By providing training to employees, organizations can empower them to identify phishing scams, create strong passwords, and avoid risky behavior online. Moreover, ongoing training ensures that employees stay up-to-date on the latest cybersecurity trends and technologies, which is essential in the ever-evolving threat landscape.

Where would I allocate funds?

After investing in employee training, it is critical to invest in essential cybersecurity technologies that can help protect the organization's assets. These technologies include antivirus software, firewalls, and intrusion detection systems. These technologies are the first line of defense against cyber-attacks and can help to prevent many common types of cyber-attacks. Once the essential cybersecurity technologies have been implemented, it is worthwhile to consider investing in additional cybersecurity measures. These measures can include encryption software, multi-factor authentication, and security monitoring tools, among others. While these technologies may not be as critical as employee training and essential cybersecurity technologies, they can significantly enhance an organization's cybersecurity posture and provide an additional layer of protection against more sophisticated cyber-attacks. When managing a limited budget for cybersecurity, it is crucial to prioritize employee training and essential cybersecurity technologies. By doing so, organizations can minimize their risk exposure and maximize the effectiveness of their cybersecurity strategy. Any remaining resources can be allocated towards additional cybersecurity measures to further enhance the organization's cybersecurity posture. Ultimately, a well-rounded cybersecurity strategy that balances employee training and cybersecurity technologies is critical to protect an organization's assets and maintain business continuity.

Conclusion

In conclusion, the social meaning and impact of cybersecurity-related technical systems go beyond their technical functions. They represent a form of power and control over information and can have significant implications for social and political relationships, power dynamics, and economic structures. As the use of these systems becomes increasingly prevalent, it is important to consider their potential consequences and ensure that they are used in a way that respects individual rights and societal values.

References

-mimecast. (2014). Cybersecurity Training for Employees. Mimecast. https://www.mimecast.com/content/cyber-security-awareness-training-for-employees/#:~:text=Cyber%20security%20awareness%20training%20for%20employees%20helps%20to%20address%20one,security%20posture%20and%20cyber%20resilience.

-Cyber Security Training for Employees. (2023). Travelers.com. https://www.travelers.com/resources/business-topics/cyber-security/cyber-security-training-for-employees

-HERO. (2020, March 11). 4 Ways investing in cybersecurity adds value to your business | HERO Managed Services. HERO Managed Services. https://www.heromanaged.com/4-ways-investing-in-cybersecurity-adds-value-to-your-business/

- What is SCADA? (2018). Inductive Automation. https://www.inductiveautomation.com/resources/article/what-is-scada#:~:text=Supervisory%20ontrol%20and%20data%20acquisition%20(SCADA)%20is%20a%20system%20of,and%20process%20real%2Dtime%20data

-What is SCADA Security. (2018, August 9). Forcepoint. https://www.forcepoint.com/cyber-edu/scada-security#:~:text=Malware%2C%20including%20viruses%2C%20spyware%20and,to%20manage%20the%20SCADA%20network.

-The Need and the Vulnerabilities Associated with SCADA – a-alston. (2020, December 6). Odu.edu. https://sites.wp.odu.edu/a-alston/2020/12/06/the-need-and-the-vulnerabilities-associated-with-scada/#:~:text=The%20Role%20SCADA%20Application%20Plays%20in%20Mitigating%20the%20Risks,-Some%20effective%20measures&text=Preventive%20measures%20include%20allowing%20only,the%20network%2C%20and%20other%20issues.

- the. (2023). What is the CIA Triad_ Definition, Explanation, Examples - TechTarget.pdf. Google Docs. https://drive.google.com/file/d/1898r4pGpKHN6bmKcwlxPdVZpCC6Moy8l/view

- Difference between Authentication and Authorization. (2019, June 6). GeeksforGeeks; GeeksforGeeks. https://www.geeksforgeeks.org/difference-between-authentication-and-authorization/

- Hare, V. (2022, July 14). Authentication vs. Authorization - tokenex. Tokenex. https://www.tokenex.com/blog/vh-authentication-vs-authorization/#:~:text=Payment%20authentication%20is%20confirming%20an,to%20fulfill%2a%20transaction%20amount.

-Election Security Spotlight – CIA Triad. (2021, June 15). CIS. https://www.cisecurity.org/insights/spotlight/ei-isac-cybersecurity-spotlight-cia-triad