Akela Villegas

Professor Chris Bowman

CYSE 200-T

April 27, 2025

Safeguarding the Future

As time goes on, technology will only evolve; with advancements also come security issues and threats. Persistent cyber threats could lead to the widespread loss of privacy, increased identity theft, manipulation of public systems like power grids or healthcare, and even targeted attacks based on personal genetic information. Cyberattacks could disrupt economies, erode public trust in technology, and create national security threats. Furthermore, as artificial intelligence and quantum computing become more advanced, traditional security measures may become obsolete, leaving systems even more vulnerable if they are not continually updated. This is a major concern because our dependency on technology is growing and will only continue to grow. If we do not take cybersecurity seriously now, the impact of future breaches will be much more catastrophic. Critical services like electricity, water, banking, and healthcare would be interrupted or manipulated. In addition, if genetic data is not secured, people could face ethical and legal dilemmas that society is not yet prepared for.

To address these concerns, I would emphasize continuous updates to security measures, adopting frameworks like NIST, SCADA systems, the CIA triad, and investing in proactive incident response planning. Training and awareness are also crucial, ensuring all employees understand cybersecurity best practices. The government should implement data protection laws

and improve threat intelligence sharing. To begin understanding how organizations protect their data, it's important to start with the fundamental concept of the CIA Triad.

CIA Triad (1)

CIA triad stands for Confidentiality, Integrity, and Availability. All three of these components ensure guidance within polices to companies for security. Confidentiality is information (data) that is restricted to only those who are authorized to access it to ensure safety and privacy. Techniques such as encryption, access control, and multi-factor authentication help protect confidentiality. Integrity ensures that your data is reliable and has not been tampered with., Hashing, digital signatures, and checksums help maintain integrity. An example of this would include a digitally signed email that can be checked for tampering. Availability ensures that information and systems are accessible when needed. Redundancy, load balancing, and DDoS protection help maintain availability (Fortinet). Along with the principles of confidentiality, integrity, and availability, two other key concepts in cybersecurity are authentication and authorization, which define how access is managed.

Authentication vs. Authorization

Authentication verifies the identity of a user, system, or device. It ensures that the entity trying to access a system is who they claim to be. Common authentication methods include passwords, biometrics, and multi-factor authentication (MFA).

Authorization determines what an authenticated user is allowed to do. It involves setting permissions and access controls based on roles or policies.

Example

A user logs into their online banking account:

• Authentication: The system requires the user to enter a username and password, followed by a one-time passcode (MFA) sent to their phone.

• Authorization: After successful authentication, the system allows the user to check their account balance but does not grant them access to administrative banking settings (Cilwerner, 2025).

While protecting personal and business data is critical, another major area of cybersecurity involves safeguarding large industrial systems through SCADA technology.

SCADA (2)

Critical infrastructure systems, such as power grids, water treatment facilities, and transportation networks, rely heavily on automated control systems to function efficiently. One of the most widely used systems for monitoring and controlling these operations is Supervisory Control and Data Acquisition (SCADA). Even though SCADA applications offer significant benefits in terms of automation and real-time monitoring, they also introduce vulnerabilities that can be exploited by malicious actors.

Vulnerabilities in Critical Infrastructure Systems

Critical infrastructure systems are attractive targets for cybercriminals, nation-state attackers, and even insider threats. Some of the most significant vulnerabilities include outdated software and hardware which makes them susceptible to attacks that exploit old vulnerabilities, unsecured communication protocols making them vulnerable to man-in-the-middle attacks, remote access (again, not secure), inadequate encryption of data transmitted which can lead to data breaches, unauthorized command execution, and loss of operational control. Lastly, malware/ransomware attacks have increasingly targeted critical infrastructure, which encrypts

vital data and demands payment to restore access (Alanazi, 2022). The Colonial Pipeline attack in 20221 is a great example of such an attack.

The Role of SCADA Applications in Mitigating Risks

Despite these vulnerabilities, SCADA systems play a crucial role in protecting critical infrastructure by incorporating security-focused enhancements. Some ways SCADA applications help mitigate risks include real-time monitoring and anomaly detection, which can detect irregular patterns that can indicate a possible cyber threat or system failure (advanced systems integrate intrusion detection systems (IDS). Another way is implementing role-based access control (RBAC) and multi-factor authentication (MFA) to restrict access to authorized personnel only. To limit the impact of cyberattacks, SCADA architectures should use network segmentation, isolating critical components from public-facing networks. This approach reduces the spread of malware and unauthorized access. Lastly, one of the most effective ways to prevent cyberattacks is to keep SCADA systems updated with the latest security patches. Organizations must implement a strict update policy to mitigate vulnerabilities (Shakeel, 2024). Although securing infrastructure is vital, organizations also need a comprehensive and adaptable strategy to manage cybersecurity risks, which is where the NIST Cybersecurity Framework comes in.

NIST Framework (3)

The NIST Cybersecurity Framework (CSF) offers organizations a structured approach to managing cybersecurity risks through its five core functions: Identify, Protect, Detect, Respond, and Recover. It provides guidance, enhances communication across technical and non-technical teams, aligns with regulations, and improves overall resilience to cyber threats. At my future workplace, I would use the framework to assess risks, develop a tailored cybersecurity strategy,

implement protective controls, monitor for threats, and establish effective incident response and recovery processes. Additionally, I would promote employee awareness and training to strengthen the organization's security and align cybersecurity efforts with business objectives.

The advantages of utilizing the NIST framework for risk management include:

- Providing customers with transparency and an understanding of the risk management process
- Implementing effective policies to reduce cyber security risk
- Provide struggling organizations with a baseline for implementing an effective risk management system;
- Provide a consistent approach for identifying and prioritizing actions and
- Provide a tier system that enables organizations to prioritize their risk management attempts.

Due to the framework's adaptability, it can be modified according to the demands of every company that utilizes it, making it incredibly practical. Additionally, it protects the privacy of people which enhances the company's reputation because they are confident that their data is secure. The framework is a system that will keep getting regular updates, saving the organization money by preventing them from continually needing to purchase new security systems as soon as its old ones become ineffective. The framework's layer ensures that the company is capable of achieving the quarterly goals they have specified (Nguyen, 2022). Having a framework in place is a strong foundation, but true cybersecurity resilience depends heavily on how well people are trained and prepared within an organization.

Awareness and Training

It's very important to have a team that understands cybersecurity and how to handle a problem spot on. Many businesses don't educate staff members on how to handle the situation like a breach or phishing attack if it arises. I would prioritize training because it is important to have a strong foundation for an effective cybersecurity program. To lower the danger and probability of cyber attacks, training personnel on information security best practices is integral. This means conducting frequent training sessions for every employee, from senior executives to low-level workers. Hacking simulators, managing passwords, and other cybersecurity awareness training can be covered in training sessions. Lastly, I would invest in incident response testing and prepare for it. This is to ensure that the approach is effective, everyone involved is prepared and knowledgeable on what to do and who to contact, and maintaining system availability (SANS, 2023). Ultimately, protecting technology and data requires a combination of ethical responsibility, continuous education, and proactive defense strategies.

Conclusion

Technology is always developing, which means cybersecurity has to develop as well, if not faster. By examining the CIA Triad, SCADA system vulnerabilities, and the NIST Cybersecurity Framework, I have emphasized the need for proactive approaches to mitigate cyber threats. Cybersecurity should prioritize continuous training and awareness. The opposers argue that cybersecurity investments are costly or that current strategies will soon become outdated. While these concerns are valid, the risks of doing nothing far outweigh the costs. Frameworks like NIST are adaptable, allowing organizations to evolve their security practices with technology. In summary, cybersecurity is ever-evolving. By focusing on structured approaches and staying vigilant about emerging technologies and threats, we can better protect our digital systems and safeguard our data.

References

Alanazi, M., Mahmood, A., Jabed, M., & Chowdhury, M. (2022, November 25). SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. *Computers & Security.* https://www.sciencedirect.com/science/article/pii/S0167404822004205#sec0032

Cilwerner. (2025, March). *Authentication vs. Authorization - Microsoft Identity Platform*. Microsoft identity platform | Microsoft Learn. https://learn.microsoft.com/en-us/entra/identity-platform/authentication-vs-authorization

National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Nguyen, S. T. (2022, October 6). *Understanding the NIST cybersecurity framework*. Federal Trade Commission. https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework

SANS Institute. (2023). *Security awareness training: What it is and why it matters.* https://www.sans.org/security-awareness-training/

Shakeel, I. (2024, April 8). 10 strategies to fortify SCADA System Security. *LevelBlue.* https://levelblue.com/blogs/security-essentials/10-strategies-to-fortify-scada-system-security

What is the CIA triad and why is it important?. Fortinet. (n.d.). https://www.fortinet.com/resources/cyberglossary/cia-triad