Policy Analysis Paper 1:

The Cybersecurity Framework

Tierra Fields

Department of Cybersecurity, Old Dominion University

CYSE 525: Cyber Strategy and Policy

Professor. Hamza Demirel

Sept. 15th 2024

Introduction

The Cybersecurity Framework (CSF) was created by the National Institute of Standards and Technology (NIST) to address the growing cyber threats impacting organizations, particularly those overseeing critical infrastructure such as healthcare, finance, and energy. The NIST CSF is a crucial tool for enhancing cybersecurity efforts in the U.S and globally. This essay explores the history, practical applications, and international significance of the NIST CSF, as well as academic assessments of its effectiveness in national and international cybersecurity policies.

Overview of the NIST Cybersecurity Framework

Many organizations use the NIST Cybersecurity Framework to improve their cybersecurity defenses. It was developed in response to President Obama's Executive Order 13636 to strengthen security for vital infrastructure and was published in 2014. Although using the framework is optional, many firms choose to do so because it can be adapted to meet specific business needs. The framework has three main parts: the Framework Core, Implementation Tiers, and Profiles. The Framework Core has five basic functions: identifying risks, protecting assets, detecting cyber threats, responding to incidents, and recovering from attacks. This approach helps organizations address cybersecurity threats proactively. The Implementation Tiers allow organizations to assess their current cybersecurity plans, and the profiles can be customized based on a user's unique risk profile (Ross, McEvilley & Oren, 2018).

Why the NIST CSF was Developed

The NIST CSF was created because many companies, especially those managing essential infrastructure, did not have a strong cybersecurity strategy. This put crucial services like banking, healthcare, and transportation at risk of disruption from cyberattacks. The framework

provides businesses with a flexible and robust system for developing their cybersecurity defenses, suitable for companies of all sizes and industries. For example, energy companies can use the framework to protect their infrastructure and reduce the risk of cyber incidents causing power outages. Businesses can tailor the framework to their specific needs, starting with an evaluation of their cybersecurity posture and using the five roles in the Framework Core to create a comprehensive risk management plan. This approach allows companies to develop customized strategies for handling cybersecurity concerns effectively.

NIST CSF in National and International Cybersecurity Policies

The NIST CSF was created for U.S. enterprises but is now popular worldwide. It has been included in the national cybersecurity policies of Japan, Italy, and Australia. The framework is compatible with international cybersecurity standards like ISO/IEC 27001. Many multinational corporations use it, showing its success in promoting global cybersecurity collaboration. By providing a common language for detecting and addressing cybersecurity risks, the NIST CSF allows for easier cross-border communication. This cooperative approach helps countries and organizations fight global cyber threats by pooling resources and sharing intelligence. For instance, the European Union's General Data Protection Regulation (GDPR), which emphasizes data protection and privacy, was influenced by the NIST CSF. This demonstrates the framework's relevance in a global context and its broad impact on the development of international cybersecurity laws.

Scholarly Perspectives on the NIST CSF

The NIST CSF is highly praised by experts for its ability to help businesses manage cybersecurity risks effectively. It can be adapted to different organizational needs and risk scenarios, making it particularly beneficial for industries like technology and finance where

cyber threats are constantly evolving. The framework also aligns with international standards, promoting global cooperation in protecting critical infrastructure and strengthening cybersecurity efforts worldwide. Additionally, it emphasizes continual development, allowing organizations to remain flexible and prepared for new threats by regularly updating their cybersecurity plans. Overall, the NIST CSF is designed to provide long-term support for robust cybersecurity, rather than just a temporary solution.

Conclusion

The NIST Cybersecurity Framework is a valuable tool for organizations looking to improve their cybersecurity. Originally designed to protect critical American infrastructure, it has now become an essential part of cybersecurity strategies on both national and international levels. Its versatility makes it suitable for businesses of all sizes, from startups to large companies. Experts consistently praise the NIST CSF for its adaptability, global importance, and practical value in preventing cyberattacks. As cyber threats evolve, the NIST CSF is likely to remain a crucial resource for organizations and governments aiming to maintain strong cybersecurity defenses.

References

Bowen, Pauline, et al. Information Security Handbook: A Guide for Managers Technology Administration. Oct. 2006.

NIST. "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1." Framework for Improving Critical Infrastructure Cybersecurity, 16 Apr. 2018, nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf, https://doi.org/10.6028/nist.cswp.04162018.

Ross, Ronald S., et al. "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems [Including Updates as of 1-03-2018]." NIST, 3 Jan. 2018, www.nist.gov/publications/systems-security-engineering-considerations-multidisciplinary-approach-engineering-0.