Policy Analysis Paper 3:

The Cybersecurity Framework

Tierra Fields

Department of Cybersecurity, Old Dominion University

CYSE 525: Cyber Strategy and Policy

Professor. Hamza Demirel

Oct. 6th 2024

Introduction

Cybersecurity Frameworks (CSF) developed by the National Institute of Standards and Technology (NIST) are widely used across industries to manage cybersecurity risks, particularly in critical infrastructure sectors such as healthcare, finance, and energy. Despite the NIST CSF's primary goal of improving cybersecurity posture and reducing risks, it raises ethical issues that must be addressed. The paper discusses the ethical implications of the NIST CSF, including costs and benefits, rights and protection, and how well security is balanced with individual and organizational rights.

Costs and Benefits of the Framework

One of the core ethical considerations surrounding the NIST CSF is the balance between the costs and benefits of its implementation. One benefit of the framework is that it provides organizations with valuable tools to protect against cyber threats, reducing the risk of breaches that can lead to financial loss, reputational damage, or harm to the public. It is beneficial for organizations to have a structured and flexible set of cybersecurity guidelines that enhance the security of their infrastructure without imposing regulations (Gordon et al., 2020). Adapting the framework to specific needs minimizes operational disruptions and financial burdens for companies. However, the voluntary nature of the framework raises questions about whether organizations will invest adequately in cybersecurity, particularly those managing critical infrastructure. According to some, companies might prioritize profits over security without mandatory adherence, exposing society to greater risk (Weber, 2020). Therefore, the ethical question is whether the government should enforce stricter cybersecurity standards if it wants to avoid companies compromising security to save money.

Protection and Limitation of Rights

By protecting sensitive data from unauthorized access, NIST's CSF emphasizes protecting individual rights, particularly in industries like healthcare and finance, which have an abundance of personal information. This framework contributes to protecting citizens' rights to privacy and security by strengthening the security of critical infrastructure. The voluntary nature of the CSF also aligns with the rights of companies to self-regulate, preserving their autonomy in determining how best to protect their assets and data (National Institute of Standards and Technology, 2024) The autonomy of individuals can, however, lead to limits on their rights, especially when cybersecurity measures are insufficient to guard against data breaches or cyberattacks. Often, the consequences of organizations' failure to implement robust cybersecurity practices fall on individuals, whose personal information may be compromised. Perez & Spagnoletti (2018) raise ethical concerns about whether the framework adequately protects individuals' rights or prioritizes corporate interests over public welfare.

Balancing Security with Individual Rights

Finding the right balance between enhancing security and respecting individual rights is an ethical challenge in cybersecurity policy. Although the NIST CSF encourages organizations to adopt cybersecurity best practices, some critics argue that some measures, such as increased surveillance and data collection, may violate privacy rights. A monitoring of employee activity and network traffic to detect security threats, for example, might violate the right to privacy (Pérez & Spagnoletti, 2018). Additionally, the framework's focus on protecting critical infrastructure could lead to policies that disproportionately impact certain groups, especially if companies implement intrusive monitoring techniques that target specific employees or

customers. The ethical dilemma here is whether the framework's focus on security justifies potential intrusions on privacy and individual freedoms, or if alternative approaches could better balance these interests.

Conclusion

Several ethical implications arise from the NIST Cybersecurity Framework, such as the costs and benefits of its voluntary nature, the protection and limitation of rights, and the balance between security and individual freedom. While the framework has improved cybersecurity across industries, it raises questions about whether companies should be held accountable for implementing robust security measures. Policymakers must ensure that the framework enhances security and protects individuals and organizations' rights in a fair and balanced manner in order to address these ethical concerns.

References

Gordon, Lawrence A., et al. "Integrating Cost–Benefit Analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model." Journal of Cybersecurity, vol. 6, no. 1, 1 Jan. 2020, academic.oup.com/cybersecurity/article/6/1/tyaa005/5813544, https://doi.org/10.1093/cybsec/tyaa005.

National Institute of Standards and Technology. "The NIST Cybersecurity Framework (CSF) 2.0." The NIST Cybersecurity Framework (CSF) 2.0, vol. 2.0, no. 29, 26 Feb. 2024, nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf, https://doi.org/10.6028/nist.cswp.29.

Pérez, G., & Spagnoletti, P. (2018). Ethics and Cybersecurity: Balancing the Rights of Individuals and Organizations. Journal of Information Ethics, 27(2), 35–47.