Social Implications of the NIST Framework

Kayla Thompson

CYSE 425W

Dr. Mehr

October 28, 2025

Introduction

In the times of digital infrastructure, every aspect of modern civilization, from healthcare and finance to education, has a need for cybersecurity that has become a social problem. In response to this, the National Institute of Standards and Technology (NIST) developed a cybersecurity framework as a basis for guidelines to help businesses manage and reduce cyber threats. The NIST Framework was created from societal demands for trust, transparency, and now its implementation has reshaped how organizations engage with cybersecurity across all cultures and societies.

The Development

As technology improves, so do hackers' capabilities to bypass secure digital infrastructure. Due to this, countless sensitive information have been leaked across the website from an unauthorized user, which can lead to customers' data being stolen, causing severe damage. The 2013 Executive order that led to the NIST framework was a response to numerous cyberattacks, like Yahoo, Snowden, and more. These attacks exposed vulnerabilities in private and public sectors. This caused widespread concern over data privacy and national security. The framework is designed through a public/private partnership that could be adopted by organizations everywhere. By making it accessible to all-sized organizations, it will help minimize cyber risks.

Social Consequences

Since the creation of the cybersecurity framework, it has embedded itself as a non-negotiable department of an organization, making it a shared responsibility in the work

culture. This then causes everyone a part of an organization to take accountability for their actions. An article by GovFacts stated, “The CSF's adoption is increasingly recognized as a benchmark for effective cybersecurity management, contributing to a stronger overall security posture and reputation”. The organizations that incorporate NIST have better relationships with their consumers by creating trust through safeguarding sensitive data. This improves reputation and customers by keeping responsibilities in every sector of an organization.

Cultural Influences

The nature of the NIST framework is a U.S. custom that reflects American values of human rights. With this, organizations are encouraged to tailor their cybersecurity department to their unique profiles. We see this within every sector of a business, for example, in healthcare, every patient has HIPAA rights, which emphasizes patient privacy, shaping how the framework is applied. In finance, your money that you earn is all FDIC insured, this is to protect consumers of banks from having their money being misused or stolen, which influences risk assessment models. The popularity of the framework became a global standard in many countries. The framework has inspired other countries like Japan, Peru, Switzerland, and more, showing how cultural values adapt globally. Torres-Calderón and Angelo et al, “Provided robust evidence that structured implementation of framework controls significantly improves organizational cybersecurity posture, achieving increases ranging from 40% to 55.6% in cyber maturity within SMEs and organizations in Peru”.

Conclusion

The NIST framework represents more than just a technical guideline used by organizations, but is a social contract between business, consumers, and technology that shapes our lives. The framework reflects the society's demand for transparency, trust, and accountability. During this exploding technological era. Ultimately, the NIST framework shows how cybersecurity policy is inseparable from society, as it aims to protect. It is a reflection of what we value when it comes to our rights and how it affects everyone involved. Understanding the social implications allows us to improve, but also encourages inclusivity and ethical decisions.

References

Federal Trade Commission. (n.d.). *Understanding the NIST cybersecurity framework*. Federal Trade Commission. https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework

GovFacts. (2025, July 19). *The NIST Cybersecurity Framework: A guide for U.S. businesses*. GovFacts. https://govfacts.org/federal/commerce/the-nist-cybersecurity-framework-a-guide-for-u-s-businesses/

Salas-Riega, J. L., Riega-Virú, Y., Ninaquispe-Soto, M., & Salas-Riega, J. M. (2025). *Cybersecurity and the NIST Framework: A systematic review of its implementation and effectiveness against cyber threats*. International Journal of Advanced Computer Science and Applications, 16(6). https://thesai.org/Downloads/Volume16No6/Paper_72-Cybersecurity_and_the_NIST_Framework.pdf

Trautman, L. J., & Ormerod, P. C. (2017). Corporate directors' and officers' cybersecurity standard of care: The Yahoo data breach. *American University Law Review, 66*(5), 1231–1292. https://aulawreview.org/au_law_review/wp-content/uploads/2017/09/03-TrautmanOrmerod.pdf