Social Implications of the NIST Cybersecurity Framework

Devin Johnson

Old Dominion University: School of Cybersecurity

CYSE 425W: Cybersecurity Strategy and Policy

Dr. Shideh Yavary Mehr

July 14, 2025

Social Implications of the NIST Cybersecurity Framework

Abstract

This paper investigates the social effects of the NIST Cybersecurity Framework (CSF) by analyzing its development context, its social effects and cultural elements. The CSF enhances public trust and security awareness but creates issues regarding resource distribution and privacy protection. The analysis of these factors helps maintain ethical and inclusive cybersecurity practices.

Introduction

The NIST Cybersecurity Framework was published in 2014. It has since been updated to CSF 2.0. It's voluntary set of standards and guidelines are set to help organizations manage cybersecurity risks. While the CSF is primarily technical and policy-driven, it also carries significant social implications. This paper examines the social factors that led to its development, the impact of the framework on different communities, and the cultural and subcultural influences that have shaped its structure and adoption.

Social Factors Behind the Framework

The NIST CSF development occurred because of public worries about major cyberattacks targeting vital sectors including energy, healthcare and retail. The public became aware of cybersecurity issues after the Target breach and Sony Pictures hack (2014) occurrence (Nash, 2015). The public demanded action from policymakers because of these incidents which exposed weaknesses in critical infrastructure security and personal data protection. The increasing public dependence on digital services including banking, healthcare portals and social media platforms led to an increased need for enhanced security measures. The growing connection between society led to increased potential for large-scale disruptions. In which motivated NIST to create a flexible yet structured solution.

Social Consequences of the CSF

The NIST CSF has had broad social impacts. The framework at the same time has raised public trust because it enables organizations to establish breach prevention measures and transparent incident response protocols (Bada & Nurse, 2019). The framework has strengthened organizational responsibility because it pushes companies to enhance user data protection and disclose breach information to the public. The open adaptable structure of the framework enables organizations from education, healthcare and finance sectors to create cybersecurity policies which match their social context and community requirements. However, some negative consequences exist. The framework implementation proves challenging for smaller organizations including nonprofits and rural institutions because they do not have sufficient resources. The digital divide expands because wealthier institutions protect their networks while vulnerable communities stay exposed (Tanczer et al., 2018). The increased adoption of monitoring and threat detection technologies by entities following the CSF framework has led civil society advocates to express growing concerns about digital surveillance and privacy erosion (Richards & Hartzog, 2013).

Cultural and Subcultural Influences

The framework received its shape from American cultural values which included individual autonomy together with free-market principles and decentralization. The voluntary nature of this framework demonstrates its adherence to guidance over enforcement and its preference for innovation over compliance (NIST, 2024). The CSF received its technical direction and risk-based methodology from subcultural groups within the cybersecurity community who include white-hat hackers, ethical researchers and InfoSec professionals. The groups support responsible disclosure practices, open-source tools and transparent governance systems which match the CSF's fundamental principles. The CSF has established security awareness throughout different industries. The terms “zero trust”, “risk tolerance” and “resilience” now appear in both corporate boardrooms and public discussions. These discussions are about privacy, democracy and digital freedom. The growing adoption of the framework by organizations has transformed cybersecurity into a social responsibility that extends beyond technical and governmental domains.

Conclusion

The NIST Cybersecurity Framework emerged as a solution to public requirements for enhanced digital security protection of both personal and organizational systems. The framework has achieved its purpose by increasing public understanding while establishing trust and fostering collective responsibility. The framework also introduces three main difficulties which include unequal access to resources, surveillance practices and equity issues. The framework's future success and fairness will depend on its ability to adapt to changing social values and cultural expectations.

References

Bada, A., & Nurse, J. R. C. (2019). The social and psychological impact of cyberattacks: Insights from a study on phishing attacks. *Computers & Security, 86*, 101–110. https://doi.org/10.1016/j.cose.2019.06.004

Nash, K. S. (2015). After Target, Boards Wake Up to Cyberthreats. *The Wall Street Journal*. https://www.wsj.com/articles/after-target-boards-wake-up-to-cyberthreats-1424139537

NIST. (2024). *Cybersecurity Framework (CSF) 2.0*. National Institute of Standards and Technology. https://www.nist.gov/cyberframework

Richards, N. M., & Hartzog, W. (2013). The dangers of surveillance. *Harvard Law Review, 126*, 1934–1965.

Tanczer, L. M., López, J. H., & Wakenshaw, S. Y. L. (2018). Digital inequalities and the cybersecurity divide: Evidence from the UK. *Cyberpsychology, Behavior, and Social Networking, 21*(6), 389–394. https://doi.org/10.1089/cyber.2017.0652