Effectiveness of the NIST Cybersecurity Framework

Devin Johnson

Old Dominion University: School of Cybersecurity

CYSE 425W: Cybersecurity Strategy and Policy

Dr. Shideh Yavary Mehr

July 31, 2025

Abstract

This research evaluates NIST Cybersecurity Framework (CSF) effectiveness through expert assessments, ethical, political, social analysis and proposes evaluation methods for future assessments. The NIST Cybersecurity Framework (CSF) has gained widespread adoption because of its adaptable and expandable design, yet its voluntary status creates both beneficial and detrimental effects. The analysis uses existing literature and previous paper insights.

Introduction

The NIST Cybersecurity Framework (CSF) serves as a tool which enables organizations from different sectors to handle their cybersecurity risks. The framework has received substantial backing from both private industries and government agencies during the past ten years. The evaluation of the CSF's effectiveness requires structured criteria to determine its actual effectiveness. This paper examines academic assessments of the framework while presenting an evaluation approach and discusses the ethical, political and social effects of the policy which were previously discussed.

Scholarly Evaluations

Multiple assessments of the CSF have been conducted by scholars. Bowen et al. (2020) evaluated the framework's adaptability by demonstrating that its flexible structure enables organizations of different sizes and industries to customize their cybersecurity practices. Johnson and Goetz (2018) demonstrated that the framework enables organizations to maintain uniform risk management practices without requiring particular technological solutions. The research indicates that the CSF enables cybersecurity maturity development, yet organizations encounter difficulties with complete implementation because of limited resources. Tanczer et al. (2018) conducted a vital assessment which demonstrated that different sectors have varying levels of CSF adoption. Small and medium-sized enterprises understand the value of the CSF yet they

struggle with personnel issues, financial constraints and technical expertise. This demonstrates that the CSF provides a flexible framework, yet its success depends on the organizational capabilities of each entity.

Proposed Assessment Approach

The assessment of CSF effectiveness would require evaluation across three dimensions which include organizational risk reduction and ease of integration into existing workflows and user satisfaction across public and private sectors. The assessment should measure security incident reductions together with faster incident response times and better compliance achievement. Surveys and interviews with CISOs and IT leaders can provide qualitative insight into perceived value and challenges.

Do Assessments Support the CSF

The existing research together with real-world adoption rates support the CSF according to my assessment. The voluntary nature of this framework along with its sector-neutral approach makes it accessible to all organizations without creating regulatory challenges. The assessments reveal multiple weaknesses regarding consistency, scalability and measurable outcomes. The lack of established benchmarks creates challenges for measuring progress between different industries.

Policy Recommendations and Implications

The CSF has already shaped policy discussions through various assessment activities. Ashford (2022) among other researchers propose that voluntary frameworks need to transition

into mandatory regulations for essential infrastructure sectors. The authors propose providing technical assistance and financial support to organizations with limited resources to create a balanced playing field. The evolving policy framework demonstrates how adaptability needs to combine equity and accountability measures.

Prior Implications

The CSF needs to establish an ethical balance between security measures and individual privacy protection. Focus on best practices decreases risks but becomes invasive when not properly supervised. The CSF establishes a new political framework which promotes public-private sector collaboration through coordinated efforts instead of regulatory approaches. The framework enables organizations to develop cybersecurity cultures but simultaneously creates potential digital inequality because of uneven resource distribution. The assessment model requires inclusion and stakeholder experience representation because of its combined implications.

Conclusion

The NIST CSF serves as a valuable instrument to enhance cybersecurity awareness and preparedness. The evaluations confirm the structure and philosophy of the framework, but more effective assessment methods are required to measure its actual impact in practice. Future improvements to the CSF can be guided by assessments that combine quantitative results with stakeholder viewpoints to maintain its status as a relevant ethical policy tool in the changing digital environment.

References

Ashford, W. (2022). Why voluntary frameworks may not be enough: A call for mandatory cybersecurity standards. *Journal of Cyber Policy, 7*(1), 32–45.

Bowen, P., Hash, J., & Wilson, M. (2020). Information security handbook: A guide for managers.

NIST. (2024). *Cybersecurity Framework (CSF) 2.0*. National Institute of Standards and Technology.

Johnson, M. E., & Goetz, E. (2018). Embedding information security into the organization. *IEEE Security & Privacy, 6*(3), 16–24.

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.