Assessing the Effectiveness of the NIST Cybersecurity Framework

Liana Davis

Old Dominion University

CYSE 425W

Professor Francis Hiser

November 30, 2025

INTRODUCTION

Evaluating a cybersecurity policy begins with understanding how it functions in real-world environments. The NIST Cybersecurity Framework has become one of the most widely used tools for helping organizations identify risks, strengthen protections, and manage incidents, therefore creating a clear need to assess its measurable impact. Many industries rely on this framework to guide their security practices, but its true value is seen in how effectively organizations implement it and respond to threats. Assessing the framework means looking beyond theory to examine how well it supports proactive security, reduces vulnerabilities, and improves overall resilience as cyber risks grow more complex.

ASSESSING EFFECTIVENESS IN PRACTICE

To determine how well the NIST Cybersecurity Framework works, it's important to look at how organizations implement it and the results they achieve. Research shows that organizations using the framework's five core functions often improve their risk management and incident response, though the level of adoption varies depending on resources and organizational size (Salas Riega et al., 2025). These evaluations highlight gaps where additional guidance or policy adjustments could help, such as providing more support for smaller companies or integrating cybersecurity metrics into everyday operations (NIST, 2021). Assessing the framework in practice would involve measuring both quantitative outcomes, like reductions in security incidents, faster response times, and compliance improvements, and qualitative factors, such as staff awareness and the organization's ability to adapt to emerging threats. Based on the evidence, a structured assessment like this would likely demonstrate that organizations

following the framework see tangible improvements in security posture while also identifying areas for continued growth and refinement.

POLICY IMPLICATIONS

Evaluations of the NIST Cybersecurity Framework show that while it strengthens organizational security, there are areas where policy adjustments could make it even more effective. Organizations with fewer resources often struggle to implement all five functions fully, suggesting a need for targeted support or simplified guidance for smaller companies (Salas Riega et al., 2025). These findings also point to the value of integrating cybersecurity metrics into daily operations so that improvements are tracked and gaps are identified early (Bernardo, 2025). At a broader level, the framework's widespread adoption highlights how shared standards can encourage collaboration across industries and even internationally, shaping policies that promote coordinated risk management and resilience (NIST, 2021). By understanding these implications, policymakers and organizational leaders can refine strategies to ensure that the framework is not only adopted but actively improves security practices.

SEEING THE FRAMEWORK IN ACTION

To evaluate the effectiveness of the NIST Cybersecurity Framework, I would combine quantitative and qualitative measures to capture a complete picture. Quantitative data could include the number of security incidents, time to detect and respond to threats, and compliance with internal and external standards. Qualitative measures would assess staff awareness, confidence in cybersecurity practices, and the organization's ability to adapt to new threats. This

mixed approach aligns with methods used in recent studies on cybersecurity policy effectiveness, showing that both metrics and human factors are essential for understanding real-world impact (NIST, 2021; Salas Riega et al., 2025). Applying this framework across different sectors would allow for comparisons, highlight gaps, and reveal areas for improvement. Based on current research, I expect such assessment would demonstrate that organizations following the framework see meaningful improvements in security posture while identifying opportunities to strengthen policy implementation.

CONCLUSION

Assessing the NIST Cybersecurity Framework goes beyond technical performance and includes ethical, political, and social considerations. Ethically, organizations must protect sensitive data and maintain trust. Politically, the framework promotes coordinated risk management and can shape national cybersecurity strategies. Socially, it supports safe technology use, workforce training, and cyber awareness. A thorough assessment combining quantitative and qualitative measures would likely show that organizations adopting the framework improve security and resilience while identifying areas for continued policy refinement.

REFERENCES

Bernardo, L., Malta, S., & Magalhães, J. (2025). An Evaluation Framework for Cybersecurity Maturity Aligned with the NIST CSF. *Electronics*, *14*(7), 1364. https://doi.org/10.3390/electronics14071364

National Institute of Standards and Technology. (2021). *Measuring the effectiveness of U.S. government security awareness programs: A mixed-methods study* (NIST Technical Report). *https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=934952*

Salas Riega, J. L., Riega, Y., & Ninaquispe Soto, M. E. (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), 672–683. https://thesai.org/Downloads/Volume16No6/Paper_72-Cybersecurity_and_the_NIST_Framework.pdf