Policy Analysis Paper 5: Assessing the Effectiveness of the NIST Cybersecurity Framework

The NIST Cybersecurity Framework (CSF) was created to help organizations identify, manage, and reduce cybersecurity risks. One of the greatest strengths of the framework is that it gives organizations a structured way to approach cybersecurity rather than simply reacting after an attack occurs. The framework originally organized cybersecurity around five major functions: Identify, Protect, Detect, Respond, and Recover. The updated NIST CSF 2.0 added a sixth function, Govern, placing greater emphasis on leadership, policy, accountability, and cybersecurity risk management (National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. , 2024). Assessing whether the framework is effective, however, requires looking beyond whether an organization simply claims to follow NIST. Effectiveness should be measured by whether implementation actually reduces risk, improves an organization's ability to detect and respond to incidents, protects individuals' information, and allows the organization to recover from cyberattacks.

Research generally supports the value of the NIST Cybersecurity Framework, although researchers have identified limitations. Salas-Riega et al. (Luis Salas-Riega, 2025) conducted a systematic review of studies published between 2015 and 2024 examining implementation and effectiveness of the NIST CSF. The researchers found widespread recognition of the framework but uneven implementation. Large organizations generally demonstrated stronger performance, particularly in the Protect and Detect functions, while small and medium-sized businesses faced greater challenges because of limited financial and technical resources. The researchers

concluded that the flexibility and risk-based approach of NIST are strengths, but the voluntary nature of the framework and differences in implementation make effectiveness difficult to measure consistently.

Benz and Chatterjee (Michael Benz, 2020) reached a similar conclusion when examining cybersecurity risk in small and medium-sized businesses. They found that the NIST CSF provides a strong foundation for evaluating cybersecurity, but it does not automatically address every need of a smaller organization. They developed a cybersecurity evaluation tool based on the five original NIST CSF functions. Their research demonstrates an important point about policy effectiveness. Organizations need measurable methods for determining their current cybersecurity maturity and identifying areas that require improvement. Simply saying that an organization "uses NIST" does not prove that its cybersecurity program is effective.

Le, Le Dinh, and Uwizeyemungu (Le & Uwizeyemungu, 2025) also examined how NIST based cybersecurity practices could be adapted for small and medium sized businesses. Their research proposed integrating user behavior analytics with the NIST CSF to improve threat detection while maintaining an affordable and scalable approach. Their work supports the idea that NIST is most effective when organizations adapt the framework to their actual technology, risks, resources, and operating environment instead of treating it as a basic compliance checklist.

Together, these studies suggest an additional policy implication. NIST should remain flexible, but organizations need clearer measurements that show whether implementation produces actual security improvements. Policymakers should also consider the resources available to smaller organizations. A cybersecurity policy cannot be considered completely successful if only large organizations have the money, staff, and technology necessary to implement it effectively.

I would assess the NIST Cybersecurity Framework using both cybersecurity performance and organizational outcomes. First, I would establish a baseline for the organization's security before implementation. I would then measure changes in areas such as the number of successful security incidents, phishing success rates, vulnerabilities that remain unpatched, time required to detect an intrusion, time required to respond to an incident, recovery time after an attack, employee security training results, and implementation of controls such as multifactor authentication and access management. I would also examine whether senior leadership actively participates in cybersecurity governance.

This assessment should not rely only on compliance percentages. An organization could technically have policies and controls documented while still having poor cybersecurity practices. Therefore, I would combine documentation reviews with vulnerability assessments, penetration testing, security audits, incident-response exercises, employee phishing simulations, and actual incident data. Results should be compared over time to determine whether the organization's security posture is improving.

The assessment should also consider the ethical, political, and social implications identified in my previous papers. Ethically, stronger cybersecurity controls protect sensitive information and help prevent identity theft and unauthorized access, but monitoring and logging can create privacy concerns. Organizations therefore have to balance security with individual privacy and rights. Politically, the framework represents an ongoing balance between government involvement in cybersecurity and organizational independence. Stronger national cybersecurity standards may improve security, but excessive requirements can increase regulatory and financial burdens. Socially, cybersecurity affects public trust because people increasingly depend on

digital systems for banking, healthcare, education, communication, and government services. The assessment should therefore determine not only whether systems are technically secure, but whether security is being achieved fairly, responsibly, and without unnecessary harm to users.

I believe an assessment using these measurements would demonstrate that the NIST Cybersecurity Framework is successful, but with limitations. Success should not mean that an organization never experiences a cyberattack. No cybersecurity framework can completely eliminate cyber risk. Instead, success should mean that the organization has fewer preventable incidents, identifies threats faster, limits the damage caused by attacks, protects sensitive information, and recovers operations more quickly.

The research also shows that success depends heavily on implementation. Organizations with sufficient leadership support, funding, trained employees, and continuous monitoring are more likely to receive the full benefits of the framework. Smaller organizations may require additional guidance, affordable technology, training, or government assistance to achieve similar results. For that reason, future cybersecurity policy should place greater emphasis on measurable outcomes and resources that allow organizations of different sizes to implement the framework successfully.

In conclusion, I would assess the effectiveness of the NIST Cybersecurity Framework by measuring real improvements in cybersecurity rather than simply checking whether an organization follows the framework. Research shows that NIST provides a strong and flexible foundation for managing cybersecurity risk, but its effectiveness varies depending on resources,

organizational maturity, leadership, and how the framework is implemented. The political, ethical, and social implications also demonstrate that cybersecurity effectiveness cannot be judged only by technology. Privacy, government responsibility, organizational costs, public trust, and equal access to cybersecurity resources must also be considered. Based on these factors, I believe the NIST CSF can be considered an effective cybersecurity strategy when it is properly implemented, continuously assessed, and adjusted as threats and technologies change.

References

Le, T. D., & Uwizeyemungu, S. (2025). *A cybersecurity framework for enhancing Small and medium-sized enterprises (SMEs) security posture using user behaviour analytics*. Retrieved from Enterprise Information Systems: https://www.tandfonline.com/doi/citedby/10.1080/17517575.2025.2529282?scroll=top&needAccess=true

Luis Salas-Riega, J. (2025). *Cybersecurity and the NIST Framework: A Systematic Review of its Implementation and Effectiveness Against Cyber Threats*. Retrieved from The Science and Infirmation Organization: National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0.

Michael Benz, D. C. (2020, July-August). *Calculated risk? A cybersecurity evaluation tool for SMEs*. Retrieved from Business Horizons: https://www.sciencedirect.com/science/article/abs/pii/S0007681320300392?utm_source=chatgpt.com

National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. . (2024, February 26). Retrieved from National Institute of Standards and Technology : https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf