The NIST Cybersecurity Framework: Bridging Policy and Practice

Liana Davis

Old Dominion University

CYSE 425W

Professor Francis Hiser

September 14, 2025

INTRODUCTION

As technology continues to advance, so do the risks that come with it. What used to be considered just an IT issue is now a national and even global concern. Cyberattacks are no longer rare events but rather everyday challenges for governments, businesses, and even individuals. To address these threats, policies and frameworks have been created to provide guidance and protection. One of the most widely recognized is the NIST Cybersecurity Framework (CSF), which was developed to help organizations strengthen their defenses. I chose this framework for my essay because it takes the complexity of cybersecurity and breaks it down into practical steps that can be applied both nationally and internationally.

OVERVIEW OF THE POLICY

Before the NIST Cybersecurity Framework existed, organizations often struggled with cybersecurity risks and how to address them. There wasn’t a clear roadmap, and many companies didn’t know what areas may need more attention. Hospitals, power grids, banks, and other critical infrastructures were especially vulnerable. A single security incident generally meant major consequences. The framework was developed to provide a common language and structured approach for managing these risks. The framework outlines five key functions—Identify, Protect, Detect, Respond, and Recover—that give organizations a clear approach to cybersecurity.

HOW THE FRAMEWORK IS APPLIED

The NIST Cybersecurity Framework serves as a practical guide for organizations to make sense of the chaos that comes with cybersecurity. Companies start by evaluating their systems to pinpoint areas of risk. For example, a hospital might review all its medical devices and patient systems to determine where extra protection is needed. From there, safeguards like encryption or stronger access controls are put in place, unusual activity is monitored, incidents are handled efficiently if they occur, and operations are restored afterward. This approach allows organizations to move beyond reacting to problems as they arise and start anticipating potential threats, making cybersecurity feel more manageable and less overwhelming.

NATIONAL AND INTERNATIONAL IMPACT

The NIST Cybersecurity Framework was created in the United States, but its influence has reached far beyond national borders. Within the U.S., it is widely used across critical infrastructure sectors such as energy, healthcare, finance, and transportation. By providing a common standard, the framework helps government agencies and private companies work together more efficiently and maintain consistent security practices. Internationally, countries like Japan and Italy have adapted parts of the framework into their own cybersecurity strategies, showing that its approach to risk management works across different regions and industries (Gisbert et al., 2020). The framework also aligns with global initiatives, such as the European Union's Network and Information Security (NIS) Directive, which fosters international collaboration. This widespread adoption demonstrates how shared frameworks like NIST's can help organizations worldwide strengthen defenses and respond to cyber threats in a coordinated way.

CONCLUSION

The NIST Cybersecurity Framework has become a cornerstone of modern cybersecurity policy. It was designed to address growing risks to critical infrastructure, but its flexible structure has allowed it to be adopted by organizations of all sizes and influenced international strategies. By breaking down cybersecurity into five clear functions, the framework gives organizations a practical way to assess risks, implement safeguards, and respond to incidents. Following these steps helps organizations move from reactive approaches to proactive cybersecurity, strengthening defenses and improving resilience. As cyber threats continue to evolve, frameworks like NIST’s remain essential for guiding organizations toward safer, more coordinated, and effective practices.

REFERENCES

Gordon, L. A. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework. *Oxford Academic Cybersecurity,* 6(1), tyaa005. https://doi.org/10.1093/cybsec/tyaa005

Bernardo, L. (2025). An evaluation framework for cybersecurity maturity: A dual-survey approach aligned with the NIST Cybersecurity Framework. *MDPI Electronics,* 14(7), 1364. https://doi.org/10.3390/electronics14071364

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://doi.org/10.14569/IJACSA.2025.0160672