Ethical Implications of the NIST Cybersecurity Framework

Akela Villegas

Old Dominion University School of Cybersecurity

CYSE 425W: Cyber Strategy and Policy

Dr. Shideh Yavary Mehr

June 30, 2025

Abstract

This paper analyzes the NIST Cybersecurity Framework, which guides organizations in identifying, protecting, detecting, responding to, and recovering from cybersecurity threats. The framework not only promotes better security practices, but it also raises important ethical questions about individual rights, privacy, accountability, and access to protection. This paper also explores the ethical pros and cons of the NIST Framework. This frameworks promotes transparency, reduces harm to systems, and supports voluntary adoption, but the questions and concerns remains about how well the framework protects privacy, ensuring fairness for small organizations, and continue its flexibility. This paper highlights the importance of following ethical principles when implementing and changing cybersecurity policies like the NIST Cybersecurity Framework.

Overview

The NIST Framework has developed into one of the most trusted tools for improving cybersecurity in both small and large companies. Designed by the National Institute of Standards and Technology, the framework gives organizations a structured way to manage cyber threats and risks through five main functions: Identify, Protect, Detect, Respond, and Recover. Even though the framework is technical in nature, it also carries significant ethical implications that affect many individuals, businesses, and society as a whole.

Pros/Benefits

On the pros side, the NIST Framework is constructed to reduce harm. In this day and age, cyberattacks can expose sensitive data or damage critical infrastructure like shutting down hospitals; protecting systems also means protecting society. By offering a flexible and consistent

framework, NIST gives organizations a way to improve their defenses while taking into account the human impact of a breach. As Taddeo (2017) points out, cybersecurity is not just about technology, it is also about safeguarding human dignity and public trust.

Another pro of the framework is its voluntary nature. Unlike other cybersecurity laws that can feel lacking in cohesion and flexibility, the NIST Cybersecurity Framework allows organizations to adapt the guidance based on their own size, risk, and resources. This flexibility promotes good practices while also respecting the autonomy of businesses. According to Almuhammadi and Alsaleh (2017), ethical cybersecurity should be proportional and context-sensitive, not overly burdensome or rigid.

Cons/Costs

Even though there are pros, there is always some downside to things, especially ethical concerns. One key issue of the framework is privacy. While the framework encourages threat detection and data collection to improve security, it does not always provide strong guidance on how to protect individuals' personal data in the process. If not implemented with caution, these efforts could lead to intrusive monitoring and data misuse, especially in the workplace.

Another challenge is fairness. While large companies often have the resources to adopt such a framework, smaller businesses may struggle to have the resources to implement it fully. Without additional support or incentives, there is a risk in creating a gap where only the wealthy are able to afford strong cybersecurity, ultimately leaving the smaller organizations and their customers to fend for themselves, making them more vulnerable. As Raji and Buolamwini (2019) discuss in the context of tech ethics, fairness must be build into systems from the beginning, or marginalized groups will be unintentionally harmed.

Finally, because of the NIST Framework's voluntary nature, there is the question of accountability. What happens when an organization chooses not to follow it and people get hurt? While flexibility is important, ethical policies also require a level of responsibility and consequences when harm is preventable.

In conclusion, the NIST Cybersecurity Framework provides a strong foundation for ethical cybersecurity, but its success is dependent on how it is implemented. Protecting systems is important, but one must remember that protecting people is even more critical. To truly uphold ethical standards, the Cybersecurity Framework must be used with fairness, transparency, while focusing on privacy.

References

Almuhammadi , S., & Alsaleh , M. (2017, February). *(PDF) information security maturity model for NIST cyber security framework*. ResearchGate . https://www.researchgate.net/publication/314291503_Information_Security_Maturity_odel_for_Nist_Cyber_Security_Framework

Buolamwini, J., & Raji, I. D. (2019, January 27). *Actionable auditing: Investigating the impact of publicly naming biased performance results of commercial AI products*. MIT Media Lab. https://www.media.mit.edu/publications/actionable-auditing-investigating-the impact-of-publicly-naming-biased-performance-results-of-commercial-ai-products/

Taddeo, M. (2017, October 16). *The limits of deterrence theory in Cyberspace - Philosophy & Technology*. SpringerLink. https://link.springer.com/article/10.1007/s13347-017-0290-2