Network Security Policy: Foundation of Cybersecurity Strategy

Donte Staves

School of Cybersecurity, Old Dominion University

CYSE 425W: Cyber Strategy and Policy

Professor Francis Hiser

September 14, 2025

Abstract

As cyber threats continue to expand in scale and sophistication, organizations and governments alike depend on formalized network security policies (NSPs) to protect critical digital infrastructure. This paper gives an overview of NSPs, detailing their development, intention, and application in both enterprise and national cybersecurity frameworks. Pulling from foundational and modern scholarly sources, the paper examines how NSPs serve as necessary components in broader cybersecurity strategies and underlines their role in helping national and international security compliance efforts.

Keywords: network security, cybersecurity policy, enterprise networks, national cybersecurity strategy, information security

Introduction

In a day in age where data breaches, ransomware attacks, and state-sponsored cyber operations are becoming increasingly more common, establishing a structured approach to digital defense is crucial. So, the cybersecurity policy I chose is the Network Security Policy. This policy is a formal document that defines the procedures, technologies, and rules organizations use to protect their networks. I chose this policy because not only does it provide protection against unauthorized access and misuse of digital resources but also ensures compliance with internal governance and external regulatory mandates which is important in today's digital world. As the attack of organizations grows with cloud computing, mobile devices, and remote work, security policies serve as a guide to consistently impose protection mechanisms. This paper was written to explore the development of NSPs, putting an emphasis on why they are integral to both enterprise-level operations and national cybersecurity postures.

Overview of Network Security Policy

A network policy outlines the acceptable use, technical configurations, and behavioral standards needed to support a secure computing environment. According to Walker (1985), NSPs were originally developed in response to the need for structured protections in multi-user network environments. Since then, they have evolved to incorporate various domains, that include access control, intrusion detection, data encryption, and incident response protocols. NSPs are implemented through particular security tools like firewalls, virtual private networks (VPNs) and endpoint protection, each is configured in accordance with the policy's specifications. Marin (2005) emphasizes that these policies not only impose technical safeguards but assigns responsibilities as well, which established clear accountability among system administrators and users.

Policy Development and Implementation

As explained by Bera, Ghosh, and Dasgupta (2010), the development of an NSP requires a systematic analysis of enterprise architecture and potential vulnerabilities. In large organizations, formal modeling techniques are used to make sure that polices are in alignment with business objectives and compliance requirements. Once it is developed, policies have to continuously be reviewed and updated to account for changes in technology, organizational structure, and threats that happen to emerge. In practice, NSPs act as blueprints for configuring network defenses, training personnel, and managing risk. They are foundational to internal audits and external assessments as well, providing a documented basis for assessing security posture.

How NSPs Align with National and International Strategies

Network security polices are also crucial at the national level. For example, the U.S. National Cybersecurity Strategy makes it mandatory that federal agencies and critical infrastructure sectors acquire robust NSPs as part of their cybersecurity risk management. Comparably, the European Union’s NIS2 Directive needs consistent implementation of security measures across member states. NSPs also facilitate compliance with international standards like ISO/IEC 27001, which encourages interoperability and trust in global cyber defense efforts. Through this arrangement, organizations can participate in international cyber threat intelligence sharing, cross-border incident response and collective resilience-building.

Conclusion

Network security policies are not just internal administrative tools. They are very strategic assets that support the cybersecurity posture of organizations and nations alike. Their structured approach to managing risk, determining responsibilities, and imposing controls makes them essential in a connected world. As threats continue to evolve, NSPs must also be continuously updated, refined, and incorporated into broader national and international strategies. As a result, organizations and governments can ensure a secure digital future that is built on consistency, accountability, and resilience.

References

Bera, P., Ghosh, S. K., & Dasgupta, P. (2010). Policy based security analysis in enterprise networks: A formal approach. *IEEE Transactions on Network and Service Management, 7*(4), 231–243. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5668979

Marin, G. A. (2005). Network security basics. *IEEE Security & Privacy, 3*(6), 68–72. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1556540

Walker, S. T. (1985, April). Network security overview. In *1985 IEEE Symposium on Security and Privacy* (pp. 62–62). IEEE. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6234837