Social Implications of Network Security Policy

George D Smith III

Cybersecurity, Old Dominion University

CYSE 425, Cyber Strategy and Policy

Francis "Skip" Hiser

November 14, 2025

Network security policy plays a vital role not only in protecting computer systems but also in how people, organizations, and entire communities interact with technology. As we continue to integrate more and more systems into our daily lives, we become more dependent on digital technologies for daily essentials. My policy, which guides how networks are secured and monitored, has a great impact on how they interact with our daily lives. In this paper I will go over the security implications from my policy and how cultures have affected it, what social factors led to my policy being developed, and some of the negative effects my policy has.

Social Implications and culture effects

The United States is a capitalistic society, meaning innovation drives us to make ourselves and our country better. This being said, there is always something to improve when it comes to security. With security breaches running rampant, personal security is a must-have. Nobody, including stakeholders, would want to support or back a company that has weak security and gets data breaches constantly. That's why focuses like improved protections for sensitive data are so important. Having systems in place so data breaches are less common, and if there is one, you can know the extent of how long it’s been and what has gotten leaked is vital. All these things are represented in my policy and how most people I talk to feel. In a journal by Wolff, they go over how most private sector stakeholders expect systems to be built “with strong protections for confidentiality, integrity, and availability.” If these expectations are constantly failed to be met, stakeholders will leave and customers will lose trust in a business.

Factors Making Network Security Policy

There are many reasons why my policy was made and expanded upon; a couple are concerns of national security, the increase of cybercrime, and the boom of remote workers all over the world. All of these factors can be major in the eyes of the public. A journal on this topic says, “The increase in civilian exposure to cyberattacks has been accompanied by heightened demands for governments to introduce comprehensive cybersecurity policies (Snider et al., 2021).” Public perception is a huge factor within cyberspace due to our reliance on technology these days. Having a guideline on what the bare minimum should be helps keep people safe and secure but also stops national panic on debating what is secure and what isn’t. If the public doesn’t feel safe, we could see an avoidance of certain jobs and organizations. This can affect priority on national decisions and bills.

Negative Factors

Our reliance on the internet makes us a little too easygoing on what is safe and what isn’t. While my policy focuses on raising security, our country deems that surveillance is also important to security. This can mean that the government or companies can make loopholes to spy and gather information on each of their users. A main example of this can be cookies and data user agreements. Just blindly saying yes to all cookies and data agreements can mean that sites that you visit can gather information to sell off to advertisers and other data brokers at their discretion. Something I know not a lot of people are keen on. This can be seen within social media tracking users. A journal about privacy online talks about how social media tracks and sends metadata on their site into a database for their own means (Ali et al., 2018). Also, with Palantir on the rise and the Patriotic Act, now the USA Freedom Act (*UNITING* , 2010), being in

place, it can mean increased surveillance on users. Which makes me feel more skeptical about the future of "homeland protection."

Conclusion

Network security policies are more than internet security guidelines; they shape how individuals, organizations, and society interact with systems. While these policies improve the protection of sensitive data and reduce the risk of cyberattacks, they also raise important social and ethical questions. Issues such as privacy and surveillance show the balance between security and civil liberties. Cultural values, societal expectations, and upcoming technology all influence the creation and evolution of these policies, while public perception and behavior continually shape their robustness.

References

Wolff, J. (2016). What we talk about when we talk about cybersecurity: security in internet governance debates. *Internet Policy Review*, *5*(3). https://doi.org/10.14763/2016.3.430

Snider, K. L. G., Shandler, R., Zandani, S., & Canetti, D. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of Cybersecurity*, *7*(1). https://doi.org/10.1093/cybsec/tyab019

UNITING AND STRENGTHENING AMERICA BY FULFILLING RIGHTS AND ENSURING EFFECTIVE DISCIPLINE OVER MONITORING ACT OF 2015. (2010). https://www.govinfo.gov/content/pkg/PLAW-114publ23/pdf/PLAW-114publ23.pdf

Ali, S., Islam, N., Rauf, A., Din, I. U., Mohsen Guizani, & Joel. (2018). Privacy and Security Issues in Online Social Networks. *Future Internet*, *10*(12), 114–114. https://doi.org/10.3390/fi10120114