Policy Analysis Paper 2:

The Cybersecurity Framework

Tierra Fields

Department of Cybersecurity, Old Dominion University

CYSE 525: Cyber Strategy and Policy

Professor. Hamza Demirel

Sept. 29th 2024

Introduction

The Cybersecurity Framework (CSF) developed by the National Institute of Standards and Technology (NIST) is one of the most influential tools in enhancing cybersecurity across healthcare, finance, and energy sectors. As part of President Obama's 2013 executive order, the framework aims to provide comprehensive guidelines for mitigating cyber threats, particularly for critical infrastructure. While the technical value of the NIST CSF is widely acknowledged, its political implications are equally significant. In this paper, we examine the reasons for politicians' support or opposition to the NIST CSF, as well as the broader consequences of their decisions.

Political Responses to the NIST CSF

Politicians have engaged with the NIST CSF in various ways, often dividing along party lines. As a non-intrusive and effective government tool for improving cybersecurity across industries, the framework has generally been supported by Democrats. Its voluntary nature has allowed companies to adopt best practices without the burden of federal mandates. The NIST CSF is a thoughtful approach to protecting our nation's digital economy, which was emphasized by former President Barack Obama in introducing it. Republicans, on the other hand, have expressed concern over the federal government's growing role in cybersecurity regulation. While the framework is voluntary, critics argue that it could pave the way for future mandatory regulations, particularly as the threat landscape evolves. Senator Ted Cruz has expressed concern about federal overreach, and stated, "While protecting infrastructure is a priority, we must ensure that the private sector retains its ability to innovate".

Why Politicians Have Taken These Stances

There is a strong ideological influence on the political stances surrounding the NIST CSF. Most supporters of the framework are Democrats, who see it as an important step toward addressing national security threats collaboratively and minimally invasively. As long as industries adopt the framework voluntarily, the government offers guidance without overregulating, which aligns with centrist views on public-private partnerships in cybersecurity. The Republican party, however, is skeptical because it favors smaller government and fewer regulations. Many conservative politicians are wary of policies that impose even voluntary guidelines on private companies, particularly in sectors like finance and energy that are crucial to the economy. Market-driven solutions are more efficient than government interventions in enhancing cybersecurity practices, in their view. Furthermore, corporate lobbying cannot be ignored. Critical infrastructure sectors, in particular, have a vested interest in shaping cybersecurity policy. Although some corporations support the NIST CSF because of its flexible approach, others remain wary of any federal involvement, fearing that voluntary guidelines might eventually become mandatory. Consequently, policymakers align their positions with the interests of influential stakeholders, contributing to polarized political debates.

Ramifications of Political Decisions

Domestic and international cybersecurity policy is profoundly affected by the political discourse surrounding the NIST CSF. As a voluntary framework, the framework has been widely adopted by U.S. companies, but its effectiveness depends on political support. If political opposition results in significant changes to the framework, such as making certain aspects mandatory or dismantling others, it could either enhance or hinder its success. By overregulating, companies might resist compliance, while reducing federal involvement could lead to inconsistent cybersecurity standards. The political response to the NIST CSF affects how other

countries approach cybersecurity internationally. The U.S. is seen as a global leader in cybersecurity practices, and many nations have modeled their frameworks after the NIST CSF. Changing the political support for the framework could disrupt international cooperation, particularly when it comes to securing critical infrastructure globally. The United Kingdom and Japan, both closely allied with the U.S., have adopted similar cybersecurity frameworks, and a change in U.S. policy could affect them.

Conclusion

In addition to the technical components of the NIST Cybersecurity Framework (CSF), its political implications are just as important. Politicians and policymakers remain divided on the framework's role in balancing national security with private sector autonomy. Positions are shaped by ideological beliefs, economic considerations, and corporate stakeholders' influence. The political decisions surrounding the NIST CSF will ultimately have far-reaching consequences for global and U.S. cybersecurity.

References

"Congressional and Legislative Affairs | NIST." NIST, 27 May 2009, www.nist.gov/congressional-and-legislative-affairs. Accessed 29 Sept. 2024.

Gordon, Lawrence A., et al. "Integrating Cost–Benefit Analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model." Journal of Cybersecurity, vol. 6, no. 1, 1 Jan. 2020, academic.oup.com/cybersecurity/article/6/1/tyaa005/5813544, https://doi.org/10.1093/cybsec/tyaa005.

National Institute of Standards and Technology. "The NIST Cybersecurity Framework (CSF) 2.0." The NIST Cybersecurity Framework (CSF) 2.0, vol. 2.0, no. 29, 26 Feb. 2024, nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf, https://doi.org/10.6028/nist.cswp.29.