Jaalen Cooper

CYSE 425W

PAPER 1

Although there are other types of cybersecurity policy, I chose the most notable one, NIST. The NIST, or National Institute of Standards and Technology, cybersecurity framework is the standard used by most, if not all, companies, corporations, and businesses to provide adequate protection and security against threats, such as hackers. It was initially released in 2014 and provides a set of guidelines and standards that are designed to help organizations and corporations manage and reduce cybersecurity risks. The framework highlights the importance of things such as flexibility, scalability, and cost-effectiveness when it comes to businesses, corporations and companies. The structure and contents of the framework has made it very popular because it's very accessible to many businesses and organizations of varying sizes and industries and because it categorizes different activities in cybersecurity into 5 functions.

**Why It Was Developed**

Now why was the NIST framework needed? It was developed because there was an urgent need for a response to the increasing frequency and severity of cyberattacks on big companies resulting in them losing millions and credibility. This increase in attacks not only damaged those companies but also threatened critical infrastructure and the wider economy. The response to this threat was in the form of Executive Order 13636 which was issued in 2013 by Barack Obama, which recognized that there were measures that needed to be taken to improve the cybersecurity of the critical infrastructure sectors of the country. This recognition came with the requirement that NIST create a cybersecurity framework for companies and people in those critical sectors to be able to identify and mitigate cyber risks that had the potential to affect national and economic security. The framework's goal is to strengthen adaptability by giving out tools and knowledge to anticipate, withstand, and recover from cyber threats, as well as reduce the risks posed by those cyber threats, and foster a collaborative relationship between the public and private sectors.

**How It Is Applied**

The framework is applied through its use and implementation, as businesses use it to assess their current cybersecurity structure in order to find places that need targeted improvements. The framework is flexible, allowing businesses and organizations to tailor the recommendations from the framework to fit their specific needs and security challenges. This means whether it's a small business or massive corporation, the public or private sector, anyone would be able to fit the framework into their necessary needs. One reason that the framework is so flexible is because it is categorized into five core functions: Identify, Protect, Detect, Respond, and Recover. These categories help guide organizations in systematically managing cybersecurity risks, such as

identifying vulnerabilities and establishing protocols to follow after an incident has occurred. Implementation of the framework also gives organizations and companies financial incentives via grants, reduced insurance premiums, and tax benefits. This makes the framework more attractive for usage because it provides protection and doesn't come with a heavy financial burden.

**Fit Within National and International Cybersecurity Policy**

The NIST framework seamlessly aligns with both national and international cybersecurity strategies. At the national level, it aligns with and supports initiatives, such as CISA, or Cybersecurity and Infrastructure Security Agency, programs as well as Risk management strategies that are specific to certain sectors of the country. On the global scale, the framework has been implemented and/or adapted by several countries, including Japan and Italy, and it is recognized as the global standard for bolstering cybersecurity. The continuous promotion of the integration and collaboration of the NIST framework contributes to the global effort to address the worldwide impact of cyber threats.

**Scholarly Perspectives on the Policy**

There has been extensive research and analyses done to prove the effectiveness of the NIST CSF. These articles further highlight the importance of the NIST Cybersecurity Framework (CSF) in its efforts in guiding businesses and organizations into effective cybersecurity practices. For instance, Scott Shackelford and his colleagues argue that the framework provides key contribution to the creation and adoption of a global cybersecurity standard, while simultaneously fostering coordination and collaboration between public and private sectors. There is also an article written by Dr. Ron Ross that highlights the framework's flexibility, which is a big component for its popularity as its one size fits all approach helps organizations tailor their security measures to meet their specific risks. Additionally, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou explored how organizations can integrate cost-benefit analysis into the framework which offers a more efficient and economically sound approach to deciding on the cybersecurity strategies and tools that an organization or business wants to implement. These 3 articles are just some quick examples of how the framework has been looked at thoroughly in these studies and they underline the framework's broad applicability to any and everyone as well as its actual effectiveness in dealing with cybersecurity risks and threats.

**Conclusion**

The NIST Cybersecurity Framework offers a practical and adaptable standard that's designed to strengthen and support organizations and businesses' cybersecurity in the modern, digital world. It was developed to address the rapid rise of cyber threats around the nation,and it provides a

flexible, yet structured approach for identifying and managing risks as well as creating alignment with national and international strategies. It has demonstrated since its birth that it has significant potential to protect businesses and critical infrastructure while continuing to be attractive to organizations looking to adopt a policy to deal with the cyber world of today.

Citations


- Gordon, Lawrence A., Martin P. Loeb, and Lei Zhou. "Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model." *Journal of Cybersecurity* 6.1 (2020): tyaa005.
- Ross, Ron. "NIST DELIVERS STRONG AND FLEXIBLE SECURITY STANDARDS." *Public Law* 107: 347.
- Shackelford, Scott J., et al. "Toward a global cybersecurity standard of care: Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices." *Tex. Int'l LJ* 50 (2015): 305.