Policy Analysis

Originally the cybersecurity business community had used various frameworks. However, as technology continued to advance, these standards failed to deter the rise in cyber-attacks and data breaches that occurred within the cybersecurity industry. These frameworks became viewed as outdated, extensive, and tailored more towards management rather than security. This gave way to a need for a more centered framework, a framework that has less depth and will complement well with the ever-changing nature of technology. On February 12th, 2014, NIST Framework for Improving Critical Infrastructure Security was released to the public. The point of the NIST framework is to help businesses pinpoint vulnerabilities within systems and mitigate risks through a set of guidelines.

This framework is built on the idea of risk management, which is the identification, assessment, and evaluation of risks and the coordinated application of resources to minimize, monitor, and control the impact of an attack or a realized threat. It consists of three key components: the core, profile, and implementation and core functions: Identify, Protect, Detect, Respond and Recover. These components and functions give detailed steps to businesses on what actions should be done in each scenario that will ensure the complete security of their systems. Many renowned companies like Microsoft, JP Morgan Chase, Boeing, Intel, Bank of England all have embraced the use of the NIST Framework, as well as many small companies. (Swenson, 2019). Indicating that this framework is easily applicable to any business, big and small market. The framework language is easy to understand and also blends well with organizations' various cybersecurity programs and risk management processes and could work in existence with them rather than outright replace them (Calder, 2018). The NIST framework can work with every company because of how flexible it is in comparison to other frameworks, allowing the ability to be spun to fit any organization’s needs. (Shen, 2014). It is very friendly towards companies that are starting as well, a feature that is uncommon among the other frameworks. The NIST framework includes tiers that help provide context on how to monitor risk management by layering out a process for the organization by taking account of how much money and resources different businesses may have. This allows companies to implement this framework no matter how high or low the budget is, making the NIST Framework for Improving Critical Infrastructure Security is the cream of the crop when it comes to cybersecurity frameworks for companies to implement. The Obama Administration introduced the executive order instructing NIST to work with the industry to create a framework that will address the problems and concerns within the cybersecurity industry. The NIST Framework's purpose is to strengthen the overall cybersecurity of the nation. Obama’s plan for the nation’s cybersecurity consisted of three goals: To establish a front line of defense against today’s immediate threats, to defend against the full spectrum of threats, to strengthen the future cybersecurity environment. (National Archives and Records Administration, 2010). The introduction of the NIST Framework achieves all three of these goals, as the biggest threats in cybersecurity are faced by businesses. The creation of a new concise framework that businesses could follow strengthens the nation’s cybersecurity and it plays into the goals and initiative of the country’s national cybersecurity policy.

References

Shen, L. (2014). THE NIST CYBERSECURITY FRAMEWORK: OVERVIEW AND POTENTIAL IMPACTS. Scitech Lawyer, 10(4), 16-19. http://proxy.lib.odu.edu/login?url=https://www.proquest.com/scholarly-journals/nist-cybersecurity-framework-overview-potential/docview/1681907475/se-2?accountid=12967

National Archives and Records Administration. (2010). *The Comprehensive National Cybersecurity initiative*. National Archives and Records Administration. Retrieved January 31, 2022, from https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative

Calder, A. (2018). Nist Cybersecurity Framework: A pocket guide. IT governance publishing.

Swenson, J. (2019, November 27). *Cybersecurity framework*. NIST. Retrieved January 31, 2022, from https://www.nist.gov/industry-impacts/cybersecurity-framework