Emmeline Kuoch

5 May 2022

NIST Cybersecurity Framework Analysis

IT infrastructure is the foundation that supports an organization. It consists of core components such as software, hardware, and networking that are essential to operating and managing IT environments (RedHat, 2019). Without sufficient cybersecurity defenses, an organization's assets run a greater risk of a security crisis. The National Institute of Standards and Technology Cybersecurity Framework, or NIST CSF, is an extremely powerful tool that was created to assist organizations in managing and improving their cybersecurity infrastructure. The framework is a balance collaboration between public and private sectors that are "made up of standards, guidelines, and practices that can be used to prevent, detect and respond to cyberattacks" (Gillis, 2021). The goal is to encourage organizations to address their cybersecurity measures, prioritize actions, and promote awareness.

NIST CSF is composed of three parts: the Core, the Implementation Tiers, and the Profiles. The Framework Core "is the set of cybersecurity activities and desired outcomes common across any critical infrastructure sector" (Gillis, 2021). Its function composes of Identify, Protect, Detect, Respond, and Recover. "Identify" refers to developing an understanding of your organization's cybersecurity risks to people, systems, assets, data, and outside entities (Gillis, 2021). An example is establishing a risk management strategy or governance policy program. "Protect" corresponds to implementing safeguards and defenses to ensure that critical infrastructure services are delivered. This can refer to empowering security awareness of employees through the use of security training. An example of this can be the implementation of security controls and the utilization of security vendor tooling to validate these controls in the

environment. At my last co-op, we applied our controls in Web, Email, Workstations, Mobile Devices, and Remote Access, to protect organizational resources and sensitive data that are constantly leaving and coming into the environment. “Detect” means to identify cybersecurity events that occur within an organization’s ecosystem. This could be continuously applying monitoring applications through third-party tooling such as IBM QRadar to monitor events. “Respond” defines the implementation actions or response planning that need to be taken if a cybersecurity incident were to be detected (Gillis, 2021). And lastly, “Recover” outlines the prioritization process of restoring services or capabilities as a result of a cybersecurity incident. This means implementing improvements and key takeaways of lessons learned from detections or response activities (RedHat, 2022).

Moreover, NIST CSF Implementation consists of Tiers “that provide the context of how an organization views cybersecurity risk” and underlies processes to be in place to manage that risk (Framework for Improving Critical Infrastructure Cybersecurity, 2018, p. 8). The Tiers, ranging from 1 to 4, measures an organization's cybersecurity risk management practices based on the processes that they have in place and how they can react to the threats in the environment as they occur (Gillis, 2021). A Tier 4 organization can be seen as adaptive to external cybersecurity threats, while a Tier 1 organization is generally described as having limited cyber awareness of their environment and prioritization. Last but not least, the NIST CSF Profile describes the current state of an organization's cybersecurity and can be used as a roadmap to fulfill the desired target state (Framework for Improving Critical Infrastructure Cybersecurity 2018, p. 11). Overall, NIST CSF highlights the strategic vision of cybersecurity risks in an organization and stresses the prioritization of having a cybersecurity plan to leverage security challenges in an ever-evolving cyberspace environment (Gillis, 2021).

NIST CSF is not a one-size-fits-all. Every organization has a unique cybersecurity need and there are various different approaches to utilizing the Framework. Essentially, “the decision about how to apply it is left to the implementing organization” (Framework for Improving Critical Infrastructure Cybersecurity, 2018, p. 3). For example, if a small organization worries about risks in its systems and wants to analyze the entirety of its cybersecurity portfolio from the inside and out, NIST CSF would be beneficial for organizations planning to strengthen their related security concerns. However, organizations are left to assume “to have less risk but this framework does not help to measure cyber risk in tangible terms or show any kind of improvements” (Security, 2018). In fact, we still see the recurring cycle of many organizations not having proper defensive measures. And security is still a major hurdle that we face today. It would be beneficial if this framework would address the progress of organizations trying to achieve the best security practices to their fullest. The framework itself cannot answer the question “How Are We Doing on Cybersecurity?” (Security, 2018). As cyberspace continues to evolve, the framework needs to adapt to these changes as well, and yet there is still progress that needs to be made. All in all, NIST CSF provides a strong foundation for organizations that are “looking to put in place basic cybersecurity systems and protocols, and in this context, is an invaluable resource” (Bocetta, 2021).

References

Bocetta, S. (2021, March 3). *3 security issues overlooked by the NIST framework*. Network Computing. Retrieved May 4, 2022, from https://www.networkcomputing.com/network-security/3-security-issues-overlooked-nist-framework

Gillis, A. S. (2021, September 24). *What is the NIST Cybersecurity Framework? definition from searchsecurity*. TechTarget SearchSecurity. Retrieved May 4, 2022, from https://www.techtarget.com/searchsecurity/definition/NIST-Cybersecurity-Framework

National Institute of Standards and Technology. (2018, April 16). *Framework for Improving Critical Infrastructure Cybersecurity*. National Institute of Standards and Technology. Retrieved May 4, 2022, from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Red Hat. (2019, June 17). *What is IT infrastructure?* Red Hat - We make open source technologies for the enterprise. Retrieved May 4, 2022, from https://www.redhat.com/en/topics/cloud-computing/what-is-it-infrastructure

Security, N. (2018, May 15). *3 winners & 2 losers: NIST Cybersecurity Framework 1.1*. Medium. Retrieved May 4, 2022, from https://medium.com/@nehemiahsecure/3-winners-2-losers-nist-cybersecurity-framework-1-1-6f994ea83661

What is the NIST Cybersecurity Framework? Balbix. (2022, April 20). Retrieved May 4, 2022, from https://www.balbix.com/insights/nist-cybersecurity-framework/