Nathaly Flores

CYSE 600

Short Analytical Paper 5

Old Dominion University

The Cybersecurity Framework Outline

Introduction

The National Institute of Standards and Technology (NIST) was created for the Cybersecurity Framework. The Cybersecurity framework incorporates policies, standards, and procedures for companies of all forms to evaluate, execute and enhance a cybersecurity strategy. At first, the Cyber Framework was executed and developed to support companies that belonged and operated with what is considered critical infrastructure enterprises since developed into a prototype that all companies and manufacturers, either public or private sectors, can now implement (NIST, 2022).

Cybersecurity Composition

The cybersecurity framework is not a sanctioning framework that institutions must execute. Rather, it is an unforced institution that can embrace and perform with the support as a set, control, and decrease its cybersecurity threats. The framework is formulated into three primary elements, and the three primary parts are Core, Tiers, and Profile. Furthermore, the Cybersecurity framework embodies four tiers of companies and executes the framework into a cybersecurity strategy (Shen, 2014).

The Roles

Elements of the core of the cybersecurity framework are the key/ essential elements because it includes the expected results that the institutions want to accomplish regarding cybersecurity objectives. The core parts of the framework employ terminology that is simple to comprehend for everyone from the top level of the company to the low-level employee.

Furthermore, the core elements support the companies assess, oversee, and decrease the risks constructed on the infrastructure and strategy they formerly had in place. Generally, the core policies, strategies, and guidelines assist an institution in using what they need to improve Cybersecurity and lessen the risk. The cybersecurity Framework's core comprises five classifications and twenty-three overall types. The core top five primary classifications are determined as identify, protect, detect, respond, and recover (Shen, 2014).

1. Identify the role of the core section the institution must perform to identify the company's risks, support, environment, and procedures in how they are related to cybersecurity risks.
2. As reported by NIST, the institution employs the protected core element to design and execute the proper controls and securities to confirm that the company's facilities are provided. This process performs as to aid a company in discovering assertive methods how to decrease cybersecurity attacks or threats and upon impact.
3. Institutions utilize the core element's detect process to execute practices and training for a company's systems to identify and swiftly recognize cyber-attacks or threats.
4. The company's assets in the respond process of the core of elements to execute tools and techniques for the right actions are carried out to respond to and take measures against a discovery.
5. The recovery process in the core element is where a company makes a recovery strategy in which they disclose how they plan to recover from a cyber incident and how they plan to patch any affected systems by a cybersecurity incident or attack.

The Tiers

The second cybersecurity framework part is the Tiers element. The companies operate this section to determine the tier disposed of with their objectives and usefulness to execute. The tiers sections are incorporated into four executions in which the company's cybersecurity procedures are determined and disposed to the framework's four execution tiers. The four execution tiers are partial, risk-informed, repeatable, and adaptive (Shen, 2014).

1. One of the first executions tier, Tier 1, is a partisan performance. Companies that recognize Tier 1 company controls their risk in a sensitive method where the cybersecurity procedures are conducted without particular importance on a case-by-case foundation as they are not a priority by the administration. These companies, at times, convey their data to other companies as they ought to be informed of where they are suited in their companies' manufacturing.
2. The second tier, Tier 2, is a risk-informed performance. The administration/management of a company is conscious of the risks and strategies to handle. These strategies are not procedures utilized to a great extent by the companies.
3. The third tier, Tier 3, is a repeatable performance. Companies and administrations have enforced procedures and strategies that are often utilized all over the companies to address their risks and are often being updated as threats constantly vary.
4. The fourth and final tier, Tier 4, is an adaptive performance. The companies in this tier often adjust to their situation and revise their procedures and techniques to enhance their cybersecurity administration. The company's administration/management is conscious of

threats/attacks and has executed strategies to deal with them—the company administration/management issues completing the company's requirements in revising the risks (Bresnahan, 2019).

Cyber Profiling

The cybersecurity framework is composed of three segments. In this section, companies select their layout, risks and risk tolerance, objectives, and a way to create their profile. These firms use their profile to analyze and gain their target's favor as opposed to what they have chosen or wanted before in their profile. These profiles will examine their cybersecurity tactics, methods, and strategies to enhance (Shen, 2014).

Conclusion

Different companies prefer the cybersecurity framework because of its financial support and simplicity. The cyber framework is well known because companies can operate with what they had before without enhancing Cybersecurity further. The cyber framework does not need companies to support its cybersecurity programs because it utilizes what it already contains. This is mainly beneficial for small and medium-sized companies because they inherently have smaller support funds, forcing them to prioritize second-to-last Cybersecurity because of how much finances they have to support and prioritize Cybersecurity.

Works Cited

Bresnahan, E. (2019, October 17). *Security Boulevard*. Retrieved from The NIST Cybersecurity Framework Implementation Tiers Explained: https://securityboulevard.com/2019/10/the-nist-cybersecurity-framework-implementation-tiers-explained/

NIST. (2022, April 14). *Cybersecurity Framework*. Retrieved from NIST: https://www.nist.gov/cyberframework/getting-started

Shen, L. (2014). The NIST Cybersecurity Framework: Overview and Potential Impacts. *Journal of Internet Law*, 18(6), 3–6.