Name: Zachary Chandler

Date: 1/25/2020

Details

As I understand it, a framework is like a standard. Frameworks give us a structure to a set of tasks and goals. "The cybersecurity framework is a blueprint to enrich your enterprise IT security" (Raam, 2019). A framework also separate entities to operate under a common structure to build their cybersecurity systems. When I first learned about standards and frameworks, I was told to think about electrical outlets. And how hundreds of unconnected companies can work under one framework to build appliances that operate off a "standard" the three prong 120-volt AC electrical system. If it weren't for this idea of frameworks you would have a hard time using your 4-prong flux capacitor Apple charger in a General electric 9 prong outlet. Similarly, we needed a framework that large corporations, military, hospitals and the online economy could all use together to prove a level of security to their Information Systems.

I think NIST says it more eloquently "The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure." (*Cybersecurity Framework*, 2020). A framework creates a structure to support commonality between information systems in differing organizations. Finally, a framework gives a cheat sheet to new organizations. Rather than reinventing the wheel, sectors looking to develop security can lean on the framework and if need be improved or add to.

NIST's Cyber security framework has five core activities:

1) The first core activity is an assessment phase that helps the user of the framework define and quantitate their current cybersecurity posture. This is where the organization looks to see its current strengths and weaknesses.

2) Secondly the core of the framework looks to define the organization's target for Cybersecurity. This is the goal setting phase.

3) This core activity is an ongoing cyclical process that works to improve the current Cybersecurity posture. It's the "always be learning" step.

4) The fourth activity a progress check on the implementation of the improvements and how they lead to the stated goals.

5) Finally, the last activity is about communicating with invested persons within the org and outside. This could be meetings with management or addresses to the users of a program or service.

References

Cybersecurity Framework. (2020, January 17). Retrieved January 26, 2020, from https://www.nist.gov/cyberframework

Raam, G. (2019, July 12). Cybersecurity Frameworks - Types, Strategies, Implementation and Benefits. Retrieved January 26, 2020, from https://thehackernews.com/2019/07/best-cybersecurity-frameworks.html