Just what is a framework and why can it be useful? Briefly describe the 5 core activities of NIST’s Cybersecurity framework

Amy Lawson-Gunkel

6 September 2019

Details

In the previous module for this class, one of our module readings was “Framework for Improving Critical Infrastructure Cybersecurity,” in this reading we learned about the benefits of the framework to the cybersecurity community. A framework is intended to be a universal standard for businesses and organizations of all sizes to help mitigate cybersecurity risks. The framework is very versatile, being that there is no limitations involving its scalability, geographic location, and functionality regardless of economic influence.

The desired goal of the framework is to provide the following functions: identify, protect, detect, respond, and recover. These core functions act as set of guidelines that should be continuously to performed in order to produce an outcome displaying its maximum benefit to the organization adhering to framework model. The purpose of the identify function is to gain an understanding of how the organization “manage[s] cybersecurity risk to systems, people, assets, data, and capabilities” (Framework for Improving Critical Infrastructure Cybersecurity). This essentially gives the organization a layout of which areas need attention in order to better protect them from risks. The next phase in the framework is protect; once an assessment of the organization is made, a plan can be developed and implemented to minimize the effects of a threat. Following this phase is the detect phase; this phase is intended to assist the organization with the discovery and identification of dangerous events. If and when an event occurs, the response phase should allow for the business to act quickly and appropriately. The fifth, and final core activity of the framework, is the recovery phase; in this phase, the company is responsible for “develop[ing] and implement[ing] appropriate activities to maintain plans for resilience” (Framework for Improving Critical Infrastructure Cybersecurity). Should these core activities be implemented in an organization’s cybersecurity plan, it should set a strong foundation to mitigate major cybersecurity risks.

References

National Institute of Standards and Technology. (2018, April 16). 01b -NIST\_Improving Cybersecurity.pdf. Retrieved from https://drive.google.com/file/d/1wPp9kofp-gdlu3NAisszeM8d8ko1djF1/view