The Merriam-Webster definition of a framework is “a skeletal, openwork, or structural frame” (Merriam-Webster, n.d). For cybersecurity, the NIST Cybersecurity Framework can provide a computer security guide of how private sectors can judge and refine their ability to avert, notice, and answer to cyber attacks. This framework is also useful because any organization can use these cybersecurity principles no matter the organization’s size, threat of cyber attack, or how well the organization understands cybersecurity. While the framework might not work with some unique cyber-attacks that a organization is dealing with, that is because the framework is aimed at reducing the threat of a cyber-attack and optimize the ability to manage cybersecurity. The framework is a live document that will be frequently updated and enhanced as the community and industry provides feedback on implementation. The NIST Cybersecurity Framework core functions are: Identify, Protect, Detect, Respond, and Recover. The Identify function allows an organization to understand how to manage cybersecurity risks to systems, assets, data, and capabilities, which will enable the organization to focus and prioritizes its efforts with its risk management strategy and business needs. The Protect Function allows a safeguard to limit or contain the effect of a potential cybersecurity event. The Detect Function will permit a quick detection of cybersecurity events and implements applicable activities to see the occurrence of the cybersecurity events. The next function is called the Respond Function, which allows the creation and implementation of suitable plans to react to a cybersecurity problem that has been detected. The Respond Function can help with the ability to contain the effect of a cybersecurity problem. The last function is the Recover function, which allows the creation and insertion of actions to maintain plans for recovery of services that may have been damaged from a cybersecurity problem. The Recover Function supports an operation to return to its normal state quickly when it has been effected by a cybersecurity problem (NIST, 2018).

Sources:

Merriam-Webster. (n.d.). Framework. Retrieved February 24, 2020, from https://www.merriam-webster.com/dictionary/framework

NIST. (2018, April 16). Framework for Improving Critical Infrastructure Cybersecurity. Retrieved January 24, 2020, from https://drive.google.com/file/d/1wPp9kofp-gdlu3NAisszeM8d8ko1djF1/view