

Journal Entry 1: Frameworks

Name: Leah Drew

Date: 9/06/2019


Details

A framework is a set of guidelines and best practices that is useful to businesses that want to develop a cybersecurity plan. Best practices vary based on context, so the framework is meant to be very flexible. Because a framework is meant to be adapted to a business's needs, no two businesses will apply a given framework in the same way. Frameworks are useful to businesses because they outline themselves in detail so that someone without prior knowledge of cybersecurity could read the framework and use it to make the right choices for their business (Cornelius, 2018).

The NIST core includes five activities: identify, protect, detect, respond, and recover. Each activity is divided into categories, which are goals the business wants to manage, and subcategories that help support the categories (National Institute of Standards and Technology, 2018).

The first activity, identify, involves identifying risk and becoming familiar with the structure of the business. This helps develop a strategy, which leads into the second activity: protect. Protecting essentially means that the business puts safeguards in place to reduce the chance of a cybersecurity event. The third activity, detect, requires that the business develops a system that will allow them to identify when a cybersecurity event has happened. This is different from the first activity in that "identify" has to do with identifying potential weak points, while "detect" has to do with discovering events that have happened. The fourth activity, respond, involves managing a plan to respond to a potential cybersecurity event. Finally, "recover" requires that the business develops a plan for how to bounce back from a cybersecurity event and recover anything that was lost from it (National Institute of Standards and Technology, 2018).

Even though these activities seem to follow a sequential order, NIST states that the plan developed using the framework core is meant to be managed "concurrently and continuously"



(2018), meaning that the business should always be performing these functions and they should be changing and evolving.

References

Cornelius, T. (2018, July 31). Understanding Cybersecurity & Privacy Best Practices [Linkedin page] Retrieved September 6, 2019 from <https://drive.google.com/file/d/1msnsbAw1LUyeI2WoM90toEcR2Hfhz-1l/view>

National Institute of Standards and Technology (U.S.),. (2018). *Framework for improving critical infrastructure cybersecurity*. Retrieved September 8, 2019, from <https://drive.google.com/file/d/1wPp9kofp-gdlu3NAisszeM8d8ko1djF1/view>