Frameworks

Name: Joshua Harris

Date: 1/26/2020

Details

Journal Entry 1: Just what is a framework and why can it be useful? Briefly describe the 5 core activities of NIST's Cybersecurity framework.

A framework, in terms of cybersecurity, is a non-legally binding standard for businesses to achieve in cybersecurity. It is a basic set of rules that businesses should try to follow to increase their security. NIST’s framework in particular is made to be vague so that any business could use it and adapt it to meet their particular needs. These frameworks are useful because it helps set a standard and educate the less educated in the field, as many cybersecurity workers are underqualified, to have safe business practices. NIST’s Cybersecurity framework’s five core activities are identify, protect, detect, respond, and recover. They act as basic principles that should be followed for safe business practices. Identify deals with understanding the business and what risks are involved if nothing was secure so that the other steps could best be implemented. Protect has to deal with preventing a security breach or other negatives cybersecurity event to occur. Detect has to deal with identifying when a break or other negative cybersecurity event has occurred, which is important so that one would know how to best respond. Fittingly, the next core activity is respond, which has to deal with responding to these negative cybersecurity events to limit losses and prevent further, similar events. Recover, the final core activity, has to deal with having plans in place so that, even after losses have occurred, these losses can be made back up quickly. Each of these core activities has categories that are more specific and subcategories that deal with specific tasks to be done. Some subcategories for identify would be Asset Management and Risk Assessment. Some subcategories for protect would be Maintenance; Awareness and Training; and Identity Management. Some subcategories for detect would be Security Continuous Monitoring and Detection Processes. Some subcategories for respond would be Analysis and Mitigation. Finally, some subcategories for recover would be recovery planning and improvements.

References

Barrett, M. P. (2018, November 10). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. Retrieved January 26, 2020, from https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11