Cybersecurity Framework

# Name: Jennifer Kral

# Date: 8 September 2019

# Details

              Cybersecurity framework can be described as guidance based on pre-existing standards. The cybersecurity framework also includes a set of guidelines and practices for organizations to aid them in better management and possible reduction of cybersecurity risks. Additionally, the cybersecurity framework was designed to assist cybersecurity communications between both internal and external organizational stakeholders. The cybersecurity framework is important because the framework provides a procedure that not only aids protecting the privacy of individuals, but also helps with the civil liberties when critical infrastructure organizations conduct actions pertaining to cybersecurity. While said organizations usually have their own method in place when it comes to privacy and civil liberties, the framework merely compliments what those organizations are already doing

There NIST framework core contains five different activities. The five activities are; identify, protect, detect, respond, and recover. The five core activities aid organizations in cybersecurity management. Each of the five core activities have their own purpose for being vital to cybersecurity. The first activity is identify. Identify is when development has started that will help with organizational understanding that assists in management of cybersecurity risk to people, systems, capabilities, data and assets. Outcomes of the identify core are assets management and risk assessments. The second core activity is protect. Protect pertains to appropriate safeguards that are developed and implemented to ensure delivery of sensitive services. Potential outcomes are data security and awareness training. The third core activity is detect. Detect occurs when appropriate activities to be able to identify the occurrence of cybersecurity events are developed and implemented. Results of this core activity are continuous security monitoring, and a detection process. The fourth core activity is respond. Respond is when appropriate activities to are used to take action regarding a detected cybersecurity threat are developed and implemented. Improved communications, response planning, and analysis are usually results of this core. The fifth core activity is recover. Recover happens when development is focused on appropriate actives that will maintain plans for resilience and it will restore any capabilities and/or services that were damaged due to a cybersecurity incident. Outcomes of this core are recovery planning and improvements.

# References

(n.d.). 01b - NIST\_Improving Cybersecurity.pdf. Retrieved from https://drive.google.com/open?id=1wPp9kofp-gdlu3NAisszeM8d8ko1djF1

Keller, N. (2019, August 19). Questions and Answers. Retrieved from https://www.nist.gov/cyberframework/questions-and-answers#framework