Assignment 3: Chanakya Gaur: NIST Cybersecurity Framework

Critical infrastructure is defined by the EO as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”

On February 12, 2013, President Obama issued an executive order “Improving Critical Infrastructure Cybersecurity” to strengthen critical infrastructure on which the national and economic security of the United States of America depended upon. According to this order, a framework was to be developed that provided prioritized, flexible, repeatable, performance based and cost-effective approaches to manage cybersecurity risks for all processes, information and systems involved with the delivery of critical infrastructure services.

The Framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts:

* Framework Core
* Framework Implementation Tiers
* Framework Profiles

Framework Core consists of cybersecurity activities, their desired outcomes, and all applicable references which are common throughout all critical infrastructure sectors. The core represents industry standards, guidelines, and practices that allows communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five Functions: Identify, Protect, Detect, Respond, Recover. These functions provide a high-level, strategic view of the lifecycle of an organization’s management of cybersecurity risk. It also identifies categories and subcategories for each Function, and matches them with example informative references. One such category is:

Risk Assessment (ID.RA):

This category states that the organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. Its sub-categories are:

* ID.RA-1: Asset vulnerabilities are identified and documented
* ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources
* ID.RA-3: Threats, both internal and external, are identified and documented
* ID.RA-4: Potential business impacts and likelihoods are identified
* ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
* ID.RA-6: Risk responses are identified and prioritized

Risk assessment is an important category in NIST as it outlines the basic yet essential functions that are needed to be carried out by every organization in every sector. It also ensures that all organizations check for possible threats which can be mitigated. Not only that but also post-attack methodologies are noted in case of compromise. This category gives a preparedness to every organization which can be very critical in all sectors that can affect the national security or economy.