NIST Cybersecurity Framework

+ Briefly Synopsying the goals of the Framework

In the technology infused world that we live in today, many critical infrastructures that provide national and economic security are becoming increasingly open to new threats. In February, 2013, the President of the United Stated of America issued Executive Order 13636, it focuses on improving the critical infrastructure which hold our great country together. This EO called for the development of a risk-based Cybersecurity Framework, which is a set of industry standards and best practices to help organizations manage cybersecurity risks. This Framework was designed to use a common language to address and manage cyber security risk in a cost-effective way based on business needs, without placing additional requirements on the organizations. It is not meant to replace existing methods, but to structure how those methods are used and how they can be improved.

The Framework focuses on three interconnected parts, the Core, Implementation Tiers, and Profiles. The Framework Core, as it sounds, is the center and starting point of the framework with the purpose of laying out the lifecycle of an organizations management of cybersecurity risks. The core is a set of cyber security activities, outcomes, and informative references that are common across critical infrastructure sectors. Within the core, there are five concurrent and continuous functions: Identify, Protect, Detect, Response, and Recover. Each step is used to identify every level of an organizations cybersecurity process.

Framework Implementation Tiers provide a context on how an organization views cybersecurity risk and the processes in place to manage that risk. Organizations are characterized in a range of Tier 1 to Tier 4, where Tier 1 indicates low/poor implementation or understanding of the cybersecurity risks. For example, when considering the Core, during the identification process, if not all assets are managed properly and there is no risk assessment, an organization may be characterized as Tier 1—limited awareness of cybersecurity risks. The four tiers that an organization can be characterized are: Partial, Risk-Informed, Repeatable, and Adaptive. Given that the organization is part of a major infrastructure, they want to be in Implementation Tier 4, Adaptive, which is an approach to manage cybersecurity risk with policies, processes, and procedures established before an incident occurs.

Finally, the Framework Profiles represent the outcomes of an organization, based on business needs that are identified at the Core and Tiers. Profile are the alignment of standards, guidelines, and practices to the Framework in particular scenarios. Profiles can be used for self-assessments and communicate within an organization or between then. They allow for companies to see where they are currently regarding their cybersecurity practices, and where they should be.

So, what is the goal? Simply put, to provide a standardized method of securing critical infrastructure. This represents any systems or assets, whether physical or virtual, so vital that the incapacity or destruction of such system would threated national and economic security.