NIST Cybersecurity Framework

Truc L. Huynh, Computer Science

Purdue University Fort Wayne

**NIST Cybersecurity Framework**

According to (1), the NIST Cybersecurity Framework has five cores:

* Identify: focusing on understanding the organization’s context through activities like access management, governance, risk assessment, and risk management.
* Protect: Including activities like identity and access management, access control, awareness, training, data security, and protective technology.
* Detect: Identifying cybersecurity events (anomaly and event detection, continuous monitoring, detection processes, and procedures)
* Response: actions when a cybersecurity incident is detected (communication, analysis, migration, and improvements)
* Recover: combines ongoing efforts to ensure resilience for organizations and environments and the restoration of capabilities and services that were impacted.

Each of these functions within the five cores is then broken down into categories, and each category has sub-categories that describe their concepts in detail. NIST Framework is implemented using tiers that are intended to be matched to the organization’s security goal. There is 4 level of tiers:

* Tier 1/Partial: limited on risk management and risk awareness. The organization is not working effectively with external organizations.
* Tier 2/Risk Informed: risk management is approved but not board support, not effective strategies. The organization is not operating effectively the ecosystem.
* Tier 3/Repeatable: risk management is stable; board awareness as well as appropriate skills and communication. The organization is operating effectively in the broader ecosystem.
* Tier 4/Adaptive: adapt new cybersecurity threats and risks actively, maximize efficiency and effectiveness. Using real-time or near real-time to shape cybersecurity practice and response.

The NIST framework presents potential business opportunities for GTSI. According to (1), the NIST cybersecurity framework (CFS) is considered among the popular security best practices. GTSI as a security firm can help other businesses adopt the NIST CFS to maintain their organization’s security posture and compliance with regulatory standards (PCI DSS)

References

Chapple, M., & Seidl, D. (2023). Chapter 12: Computer Network Defense. In *Cyberwarfare: Information Operations in a Connected World* (Second, pp. 9–20). essay, Jones & Bartlett Learning. (1)

Pithawala, B., (2021) Overcoming the Limitations of VPN, NAC, and Firewalls with ZTA. Retrieved from [Overcoming the Limitations of VPN, NAC, and Firewalls with ZTA (elisity.com)](https://blog.elisity.com/zta-vs-vpn-nac-firewalls#:~:text=NAC%20provides%20binary%20network%20access%20%28either%20%22on%22%20or,NAC%2C%20there%20is%20no%20continuous%20verification%20of%20authorization.)