Applying the NIST CSF

Earlier in this program you learned about the uses and benefits of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). There are five core functions of the NIST CSF framework: identify, protect, detect, respond, and recover.

Image: 5 core functions of the NIST CSF

These core functions help organizations manage cybersecurity risks, implement risk management strategies, and learn from previous mistakes. Plans based on this framework should be continuously updated to stay ahead of the latest security threats. The core functions help ensure organizations are protected against potential threats, risks, and vulnerabilities. Each function can be used to improve an organization's security:

- **Identify:** Manage security risks through regular audits of internal networks, systems, devices, and access privileges to identify potential gaps in security.
- **Protect**: Develop a strategy to protect internal assets through the implementation of policies, procedures, training and tools that help mitigate cybersecurity threats.
- **Detect**: Scan for potential security incidents and improve monitoring capabilities to increase the speed and efficiency of detections.
- **Respond**: Ensure that the proper procedures are used to contain, neutralize and analyze security incidents and implement improvements to the security process.
- **Recover**: Return affected systems back to normal operation and restore systems data and assets that have been affected by an incident.

Some questions to ask for each of the five core functions, include:

Identify	Create an inventory of organizational systems, processes, assets, data, people, and capabilities that need to be secured: ● Technology/Asset Management: Which hardware devices, operating systems, and software were affected? Trace the flow of the attack through the internal network. ● Process/Business environment: Which business processes were affected in the attack? ● People: Who needs access to the affected systems?
Protect	Develop and implement safeguards to protect the identified items and ensure delivery of services: ● Access control: Who needs access to the affected items? How are non-trusted sources blocked from having access? ● Awareness/Training: Who needs to be made aware of this attack and how to prevent it from happening again? ● Data security: Is there any affected data that needs to be made more secure? ● Information protection and procedures: Do any procedures need to be updated or added to protect data assets? ● Maintenance: Do any of the affected hardware, operating systems, or software need to be updated? ● Protective technology: Are there any protective technologies, like a firewall or an intrusion prevention system (IPS), that should be implemented to protect against future attacks?
Detect	Design and implement a system with tools needed for detecting threats and attacks: ● Anomalies and events: What tools could be used to detect and alert IT security staff of anomalies and security events, such as a security information and event management system (SIEM) tool? ● Security continuous monitoring: What tools or IT processes are needed to monitor the network for security events? ● Detection process: What tools are needed to detect security events, such as an IDS?

Respond	Design action plans for responding to threats and attacks: ● Response planning: What action plans need to be implemented to respond to similar attacks in the future? ● Communications: How will security event response procedures be communicated within the organization and with those directly affected by the attack, including end users and IT staff? ● Analysis: What analysis steps should be followed in response to a similar attack? ● Mitigation: What responding steps could be used to mitigate the impact of an attack, such as offlining or isolating affected resources? ● Improvements: What improvements are needed to improve response procedures in the future?
Recover	Construct a plan and implement the framework for recovering and restoring affected systems and/or data: ● Recovery planning: How will resources be restored following an attack? ● Improvements: Do any improvements need to be made to the current recovery systems or processes? ● Communications: How will restoration procedures be communicated within the organization and with those directly affected by the attack, including end users and IT staff?

The NIST CSF and its five core functions provide a framework of planning proactive to applying reactive measures to cybersecurity threats. These functions are essential for ensuring that an organization has effective security strategies in place. An organization must have the ability to quickly recover from any damage caused by an incident to minimize their level of risk.