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.

Activity Overview

In this activity, you will create an incident report using the knowledge you've gained about networks throughout this course to analyze a network incident. You will analyze the situation using the

National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF). The CSF is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk. Creating a quality cybersecurity incident report and applying the CSF can demonstrate a proactive approach to security, improving communication and transparency with stakeholders, and improve security practices within your organization. You can also add the incident report you create to your cybersecurity portfolio when you complete it.

The CSF is scalable and can be applied in a wide variety of contexts. As you continue to learn more and refine your understanding of key cybersecurity skills, you can use the templates provided in this activity in other situations. Knowing how to identify which security measures to apply in response to business needs will help you determine which are the best available options when it comes to network security.

Be sure to complete this activity before moving on. In the next course item, you will be able to self-assess your response. After that, there will be a completed exemplar to compare to your own work. It will also provide an opportunity for you to answer rubric questions that allow you to reflect on key elements of your professional statement.

Scenario

Review the scenario below. Then complete the step-by-step instructions.

You are a cybersecurity analyst working for a multimedia company that offers web design services, graphic design, and social media marketing solutions to small businesses. Your organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved.

During the attack, your organization's network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.

The company's cybersecurity team then investigated the security event. They found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack.

To address this security event, the network security team implemented:

- A new firewall rule to limit the rate of incoming ICMP packets
- Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets
- Network monitoring software to detect abnormal traffic patterns
- An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics

As a cybersecurity analyst, you are tasked with using this security event to create a plan to improve your company's network security, following the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). You will use the CSF to help you navigate through the different steps of analyzing this cybersecurity event and integrate your analysis into a general security strategy. We have broken the analysis into different parts in the template below. You can explore them here:

- Identify security risks through regular audits of internal networks, systems, devices, and access privileges to identify potential gaps in security.
- Protect internal assets through the implementation of policies, procedures, training and tools that help mitigate cybersecurity threats.
- Detect potential security incidents and improve monitoring capabilities to increase the speed and efficiency of detections.
- Respond to contain, neutralize, and analyze security incidents; implement improvements to the security process.

Recover affected systems to normal operation and restore systems data and/or assets that have been affected by an incident.

Step-By-Step Instructions

Follow the instructions and fill in the sections to complete the activity. Then, go to the next course item to compare your work to a completed exemplar.

Step 1: Access the incident report analysis template

To access template for this course item, click the following link and select *Use Template*.
Link to template:

- Incident report analysis

Link to supporting materials:

- Applying the NIST CSF
- Example of an incident report analysis

Step 2: Summarize the security event

Using the template provided, provide a summary of the security event that occurred. Include information about the security event, its cause, the impact, and the response. You can also include information about targeted systems, the attack source, and the estimated impact.

Step 3: Identify the type of attack and the systems affected

Think about all of the concepts covered in the course so far and reflect on the scenario and define what type of attack occurred and which systems were affected. List this information in the incident report analysis worksheet in the section titled “Identify.”

Step 4: Protect the assets in your organization from being compromised

Next, you will assess where the organization can improve to further protect its assets. In this step, you will focus on creating an immediate action plan to respond to the cybersecurity incident. When creating this plan, reflect on the following question:

- What systems or procedures need to be updated or changed to further secure the organization’s assets?

Write your response in the incident report analysis template in the “Protect” section.

Step 5: Detect similar incidents in the future

It is important to continuously monitor network traffic on network devices to check for suspicious activity, such as incoming external ICMP packets from non-trusted IP addresses attempting to pass through the organization’s network firewall.
For this step, consider ways you and your team can monitor and analyze network traffic, software applications, track authorized versus unauthorized users, and detect any unusual activity on user accounts. Write your response in the incident response analysis worksheet in the “Detect” section.

Step 6: Respond to future cybersecurity incidents

After identifying the tools and methods you and your organization have in place for detecting potential vulnerabilities and threats, create a response plan in the event of a future incident. This typically happens after the incident occurred and has been resolved by you and your team. In this case, you will create a response plan for future cybersecurity incidents. Some items to consider when creating a response plan to any cybersecurity incident:

- How can you and your team contain cybersecurity incidents and affected devices?
- What procedures are in place to help you and your team neutralize cybersecurity incidents?

- What data or information can be used to analyze this incident?
- How can your organization's recovery process be improved to better handle future cybersecurity incidents?

Write your response in the incident report analysis template under the "respond" section.

Step 7: Recover from the incident

Consider what steps need to be taken to help the organization recover from the cybersecurity incident. Reflect on all the information you gathered about the incident in the previous steps to consider which devices, systems, and processes need to be restored and recovered.
Consider the following questions:

- What information do you need to be able to recover immediately?
- What processes are in place to help the organization recover from the incident?

Write your response in the "recover" portion of the worksheet.

Pro Tip: Save the incident report analysis template

Finally, be sure to save a copy of your incident report analysis worksheet somewhere accessible so that you can access it as you progress through the course and into the security field.

What to Include in Your Response

Later, you will have the opportunity to assess your performance using the criteria listed. Be sure to address the following in your completed activity.
Course 3 incident report analysis

- Summarize the security event
- Identifies the type of attack and the systems impacted by the incident
- Offers a protection plan against future cybersecurity incidents
- Describes detection methods that can be used to identify potential cybersecurity incidents
- Includes a response plan for the cybersecurity incident and outline for future cybersecurity incidents
- Outlines recovery plans you and the organization can implement in future cybersecurity incidents.

Step 8: Assess your activity
You will complete a self-assessment for your incident report portfolio activity. Please use the questions that are presented to review your own work. The self-assessment process is an important part of the learning experience because it allows you to *objectively* assess your incident report.
To complete the self-assessment, first open the Portfolio Activity Exemplar in the next course item. Compare your completed incident report document. Respond yes or no to each statement provided at the end of the Portfolio Activity.
When you complete and submit your responses, you will receive a percentage score. This score will help you confirm whether you completed the required steps of the activity. The recommended passing grade for this project is at least 80%. If you want to increase your score, you can revise your project and then resubmit your responses to reflect any changes you made. Try to achieve at least 5 points before continuing on to the next course item.