**Activity: Use the NIST Cybersecurity Framework to Respond to a Security Incident**

In this activity, you will use the knowledge gained about networking throughout this course to analyze a network incident. You'll analyze the situation using the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF) and create an incident report that you can include as part of your cybersecurity portfolio documentation. The CSF is a voluntary framework consisting of standards, guidelines, and best practices for managing cybersecurity risks. Creating a quality cybersecurity incident report and applying the CSF can help you build trust and improve security practices in your organization.

**Scenario**

You're a cybersecurity analyst working for a multimedia company that offers web design, graphic design, and social media marketing solutions services to small businesses. Your organization recently suffered 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 a flood of ICMP packets. Normal internal network traffic was unable to 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 discovered that a malicious actor sent a flurry of ICMP pings to 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 ICMP Packets Received
* Checking the source IP address at the firewall to check for spoofed IP addresses in incoming ICMP packets
* Network Monitoring Software to Detect Abnormal Traffic Patterns
* An IDS/IPS system to filter 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 the security of your company's network, following the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). You'll use the CSF to help you navigate the different stages of analyzing this cybersecurity incident and integrate your analysis into an overall security strategy:

* Identify security risks through regular audits of internal networks, systems, devices, and access privileges to identify potential gaps in security.
* Protect internal assets by implementing 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 security process improvements.
* Recover affected systems to normal operation and restore data and/or assets from systems that were affected by an incident.

**Step 1: Access the template**

"*Incident Report Analysis*" file

"*2 SUPPORT Applying the NIST CSF*" file

"*3 SUPPORT Completed Example of an Incident report analyis*" file

**Step 2: Identify the type of attack and affected systems**

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

**Step 3: Protect your corporation's assets from being compromised**

Next, you'll 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. As you create this plan, consider the following question:

* What systems or procedures need to be updated or changed to further protect the organization's assets?

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

**Step 4: Determine how to identify similar incidents in the future**

It is important to continuously monitor network traffic on network devices to check for suspicious activity, such as external ICMP packets received from untrusted IP addresses that attempt to pass through the organization's network firewall.

For this step, consider ways in which you and your team can monitor and analyze network traffic, software applications, track authorized and unauthorized users, and detect any unusual activity on users' accounts. Write your response in the incident response analysis worksheet in the "Detect" section.

**Step 5: Create a response plan for future cybersecurity incidents**

Once you've identified the tools and methods you and your organization use to detect potential vulnerabilities and threats, create a response plan in the event of a future incident. This typically happens after the incident has occurred and has been resolved by you and your team. In this case, you'll create a response plan for future cybersecurity incidents. Some items to consider when creating a response plan for 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 in the "respond" section.

**Step 6: Help your organization 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 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 recover immediately?
* What processes are in place to help the organization recover from the incident?

Write your answer in the "recovery" portion of the spreadsheet.

**What to include in your answer**

Subsequently, you will have the opportunity to evaluate your performance using the criteria listed. Be sure to cover the following in your completed activity.

Course 3 Incident Report Analysis

* Identifies the type of attack and the systems impacted by the incident
* Offers a plan to protect against future cybersecurity incidents
* Describes detection methods that can be used to identify potential cybersecurity incidents
* It includes a response plan for the cybersecurity incident and an outline for future cybersecurity incidents
* Describes recovery plans that you and the organization can implement in future cybersecurity incidents.

**Example Completed**

File "*Incident report analysis exemplary*"

**Example Evaluation**

Compare the copy with the full analysis of the incident report and the incident report. Proofread your work using each of the criteria in the issue. What did you do well? Where can you improve? Use your answers to these questions to guide you as you progress through the program.

**Note**: The copy represents an example of how to carry out the activity. Yours may differ in some ways. The important thing is that you have an idea of what your incident analysis should look like.

The copy is accompanied by the activity and presents a complete analysis of the incident report to establish:

* What type of attack occurred, the scope of the incident, and its impact on the organization
* Potential Network Vulnerabilities and Protective Measures
* Detection tools to monitor and protect the network
* How to Respond to Cybersecurity Incidents in the Future
* Recovery plans to restore normal operations