NIST Practice Concept

**Scenario:** Implementing NIST CSF in a Small Manufacturing Company

You are a cybersecurity consultant hired by a small manufacturing company that specializes in producing custom industrial components. The company operates a small factory floor with CNC machines and employs a team of engineers and production staff. Recently, the company fell victim to a ransomware attack that encrypted critical design files and disrupted production schedules, causing significant financial losses and customer dissatisfaction.

**Objective:** Your objective is to guide the manufacturing company in implementing the NIST Cybersecurity Framework (CSF) to strengthen its cybersecurity posture, protect intellectual property (IP), and ensure operational resilience. Focus on practical measures that align with the unique challenges of manufacturing environments, emphasizing the protection of sensitive design data, operational technology (OT) security, and compliance with relevant industry standards

**Current Situation Post Ransomware Attack:**

* The manufacturing company utilizes CNC machines controlled by networked industrial control systems (ICS) for production.
* Critical design files and proprietary software were encrypted during the ransomware attack, disrupting production schedules and causing financial losses.
* There is a lack of comprehensive cybersecurity policies and procedures tailored to the manufacturing environment, with a reliance on basic network security measures.
* The ransomware incident has highlighted vulnerabilities in OT security and the need for robust defenses against cyber threats targeting industrial environments.

**NIST CSF**

1. Identify the following:
   * 1. Technology/Asset: Which system and devices were affected?

Most likely ICS systems were affected as well as employee work stations and Network infrastructure

* + 1. Process/Business environment: Which business processes were affected in the attack? Many basic functioning tasks such as production schedules and design files were affected causing workflow to slowdown and major losses
    2. People: Who needs access to the affected systems?

The manufacturers and workers

1. Protect and implement safeguards:
   * 1. Access controls: Who needs the affected items? How are non-trusted sources blocked from having access? The workers need the affected items and assumingly the company controls what non trusted sources are blocked
     2. Awareness/Training: Who needs to be made aware of this attack and how to prevent it from happening again? All employees should be made aware of the breach and informed properly of scam attempts and proper online safety procedures to stop other attacks.
     3. Data security: Is there any affected data that needs to be made more secure? Encrypted critical designs need to be made more secure as the number one priority and second to the productions schedules
     4. Information protection and procedures: Do any procedures need to be updated or added to protect data assets? Yes we should add more security on the users end so outside files and items cant be installed without proper access and automatically blocked on workstations
     5. Maintenance: Do any of the affected hardware, OS or software need to be updated? Realistically we should runback to a previous version of most critical systems from before the ransomware attack and update any security procedures.
     6. 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? Firewalls and more through access management should added to stop any unwanted network traffic that could be harmful.
2. Detect threats and attacks:
   * 1. 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? Getting something like spelunk would help keep systems safe and allow for a way to look at security systems.
     2. Security continuous monitoring: What tools or IT processes are needed to monitor the network for security events? A SIEM like snort would allow for this, so you can continually look over such things and keep a log of it
     3. Detection process: What tools are needed to detect security events, such as an IDS? You can also use Splunk for this process as well allowing for the detection of security events
3. Respond to threats and attacks:
   * 1. Planning: What action plans need to be implemented to respond to similar attacks in the future. For similar attacks in the future it is important to have a Incident response team that properly trained and everyone has a role that they will fulfill in case of an emergency like this
     2. 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? Sending emails or alerting people through notifications will be the quickest and ideal way to get the word out about any attack
     3. Analysis: What analysis steps should be followed in response to a similar attack? Make sure to monitor network traffic and logs and properly document and detail everything
     4. Mitigation: What responding steps could be used to mitigate the impact of an attack, such as offlining or isolating affected resources?

Disabling affected resources and offlining affected workstations would be the ideal way of containing and quarantine the problem

* + 1. Improvements: What improvements are needed to improve response procedures in the future? Making sure that the Incident response team is properly informed and trained as well as having all end users properly informed on what security procedures will help others not make mistakes.

1. Recover affected systems or data:
   * 1. Recovery planning: How will resources be restored following an attack? Most likely restoring backups of all affected applications starting with the most critical ones and making sure they are secured
     2. Improvements: Do any improvements need to be made to the current recovery systems or processes? Realistically we want to make sure this current recovery system is functional and effective and as of now we will need a better one
     3. Communications: How will restoration procedures be communicated within the organization and with those directly affected by the attack, including end users and IT staff? Through email or company notifications which would allow people to get what’s going on quickly.