INCIDENT RESPONSE FOR A MID-SIZED FINANCIAL INSTITUTION USING NIST FRAMEWORK

Executive Overview: When a mid-sized financial institution fell victim to a ransomware attack, I led the incident response using the NIST Cybersecurity Framework. Through a structured simulation exercise, I identified gaps, strengthened response protocols, and ensured the organization could swiftly contain threats, recover operations, and bolster resilience against future attacks. The following are the outlined steps I took:

Step 1: Simulation of the Ransomware Attack Using the NIST Framework

The NIST Cybersecurity Framework (CSF) is structured around five core functions: Identify, Protect, Detect, Respond, and Recover. Below is a step-by-step guide to simulate the ransomware attack response using this framework.

---

1. Initial Detection of the Ransomware Attack

- **Scenario:**
    - An employee reports that they cannot access critical files, and the screen displays a ransom note demanding payment in cryptocurrency. The IT team confirms that multiple systems are locked, and files are encrypted.
- **Immediate Actions:**
    - Escalate the issue to the incident response team.
    - Disconnect affected systems from the network to prevent the spread of the ransomware.

Step 2: NIST Framework Application

2. Identify

- **Objective:** Understand the organizational context, systems, and assets that might be impacted.
- **Actions:**
    - **Asset Management:** Identify and prioritize critical assets that are impacted or at risk (e.g., customer data, financial records).
    - **Risk Assessment:** Assess the vulnerabilities that were exploited (e.g., outdated software, phishing attack).
    - **Business Environment:** Understand the business impact and critical services affected by the attack.
    - **Governance:** Ensure the incident response team follows organizational policies and compliance requirements.

3. Protect

- **Objective:** Implement safeguards to limit the impact of the attack.

- **Actions:**
    - **Access Control:** Review and restrict access to critical systems and data to prevent further unauthorized access.
    - **Awareness Training:** Conduct a quick refresher for staff to avoid panic and ensure proper protocol is followed during the incident.
    - **Data Security:** Ensure backups are secure and assess their integrity for a potential restore.
    - **Maintenance:** Review and apply patches or updates that could close the exploited vulnerabilities.
    - **Protective Technology:** Implement network segmentation to isolate affected systems.

4. **Detect**
    - **Objective:** Identify the occurrence of the ransomware attack and understand its scope.
    - **Actions:**
        - **Anomalies and Events:** Review logs to identify the initial entry point, how the ransomware spread, and detect other potential compromises.
        - **Security Continuous Monitoring:** Implement continuous monitoring to detect further malicious activity during the incident.
        - **Detection Processes:** Confirm the type of ransomware and assess if decryption tools are available.
5. **Respond**
    - **Objective:** Contain the attack, minimize the damage, and communicate effectively.
    - **Actions:**
        - **Response Planning:** Execute the incident response plan.
        - **Communications:**
            - **Internal:** Update executive leadership, legal, and compliance teams.
            - **External:** Communicate with affected customers, law enforcement, and potentially media (if needed).
        - **Analysis:** Investigate the attack thoroughly to determine its impact and origin.
        - **Mitigation:** Contain the threat by disabling affected systems, removing the malware, and securing the network.
        - **Improvements:** Document lessons learned to refine the incident response plan.
6. **Recover**
    - **Objective:** Restore services and return to normal operations.

- **Actions:**
    - **Recovery Planning:** Start with restoring critical business functions from clean backups.
    - **Improvements:** Address the root cause to prevent recurrence, such as improving patch management and employee training.
    - **Communications:**
        - **Internal:** Regular updates on recovery progress to stakeholders.
        - **External:** Inform customers and partners about the recovery status.
    - **Recovery Activities:** Conduct post-incident analysis to ensure that systems are restored securely, and operations are stable.

Step 3: Communication Strategies

Internal Communication:

- Establish a communication channel (e.g., a dedicated incident response chat or email group) for real-time updates.
- Regularly update the management and affected departments on the status of the incident response.
- Communicate specific actions for departments, like disconnecting affected devices or avoiding suspicious emails.

External Communication:

- **Customers:** Send out notifications regarding the ransomware attack, potential data breaches, and how the company is addressing the issue.
- **Law Enforcement:** Report the attack to local or national cybersecurity agencies (e.g., FBI, Cybersecurity and Infrastructure Security Agency).
- **Media:** If necessary, release a public statement, ensuring the messaging is consistent, transparent, and reassures stakeholders of the recovery efforts.

Step 4: Debriefing Session

- **Objective:** Analyse the incident response to improve future preparedness.
- **Key Areas to Review:**
    - **Effectiveness of Initial Detection:** How quickly was the ransomware detected? Could it have been detected earlier?
    - **Response Execution:** Was the incident response plan followed effectively? Were there any delays or miscommunications?

    - **Impact Assessment:** Was the impact of the attack minimized? Could critical assets have been better protected?
    - **Recovery Process:** Was the recovery process efficient? Were systems restored securely?
- **Improvements:**
    - Update the incident response plan with insights from the debriefing.
    - Enhance employee training based on observed gaps.
    - Improve detection mechanisms and tools to better identify and respond to similar threats.

Updating the Incident Response Plan

- Incorporate lessons learned from the debriefing into the incident response plan.
- Update policies, playbooks, and procedures to address the identified weaknesses.
- Schedule regular reviews and tabletop exercises to ensure readiness for future incidents.

This approach ensured that the financial institution effectively managed the ransomware attack, minimized damage, and recovered critical operations in alignment with the NIST Cybersecurity Framework.