Simulation: NIST Framework-Based Response to Ransomware Attack

I led the simulated incident response for a ransomware attack that affected critical operations at a mid-sized financial institution. My responsibility was to guide the organization through a structured and compliant response based on the NIST Cybersecurity Framework (CSF), ensuring minimal disruption and long-term resilience.

Simulated Attack Detection

The simulation began with a sudden inability to access client financial records and a ransom note discovered on encrypted servers. I:

- Alerted the Incident Response Team (IRT).
- Verified abnormal file encryption through SIEM alerts and endpoint logs.
- Triggered the incident classification protocol to confirm the ransomware nature.

This fell under the Detect function of NIST: *"Develop and implement appropriate activities to identify the occurrence of a cybersecurity event."*

Applying the NIST Functions to Guide the Response

1. Identify

- Reviewed and validated the asset inventory to determine which systems were impacted.
- Identified critical business functions and dependencies to prioritize recovery.
- Checked existing risk assessments and security policies for gaps related to ransomware threats.

Key Action: Confirmed which data, applications, and systems were classified as mission-critical.

2. Protect

- Verified that network segmentation was in place to contain the spread.
- Ensured that data backups were secure and isolated (air-gapped).
- Coordinated the shutdown of non-essential systems to prevent further infection.

VIVIAN OKECHUKWU

Key Action: Implemented least privilege protocols and disabled compromised accounts.

3. Detect

- Reviewed SIEM data and endpoint logs to trace initial infection vectors.
- Identified patient zero and analyzed the behavior of the malware across the network.
- Notified third-party vendors to review their logs and interactions.

Key Action: Created a timeline of the breach and initial compromise indicators.

4. Respond

- Activated the Incident Response Plan (IRP) and assembled the IRT including IT, legal, PR, and compliance.
- Communicated internally to halt affected systems and isolate infected endpoints.
- Notified regulatory authorities (as required by FFIEC/GLBA) and legal counsel.
- Avoided paying ransom and prioritized forensic containment and investigation.

Key Action: Engaged a third-party incident response firm to assist in containment and root cause analysis.

5. Recover

- Initiated system restoration from clean backups.
- Monitored for reinfection and residual malware.
- Verified system integrity and resumed business operations in phases.

Key Action: Updated systems with patched vulnerabilities and hardened configurations.

Communication Strategy

Internal:

- Sent structured updates via secure channels to staff and executives.

VIVIAN OKECHUKWU

- Implemented a need-to-know basis approach to limit information leakage.

External:

- Coordinated with PR and legal teams to prepare a transparent, compliant public statement.
- Informed affected customers and stakeholders of the breach and resolution steps taken.

Key Message: Focused on transparency, containment, and long-term improvements.

Post-Incident Debrief & Lessons Learned

Following recovery, I led a formal post-incident debrief:

- Analyzed detection, response time, and communication effectiveness.
- Identified delayed detection due to underutilized logging capabilities.
- Found that backup testing frequency was insufficient.

Action Taken:

- Updated the Incident Response Plan (IRP) to include ransomware-specific scenarios.
- Scheduled quarterly IRP tabletop exercises.
- Implemented automated threat detection tuning and enhanced employee phishing training.

Outcome & Value

- Ransomware incident contained within 36 hours with no ransom paid.
- Critical systems restored from clean backups with minimal customer disruption.
- Institutional confidence increased due to clear, measured incident handling aligned with NIST CSF.

VIVIAN OKECHUKWU