Topic 7 Discussion 2

Regardless of a company's security protection measures, it is very important to prepare for when security measures fail. Describe in detail the six incident response steps recommended by NIST.

Hello Class,

Preparing for potential security incidents is crucial for any organization, and the National Institute of Standards and Technology (NIST) provides a comprehensive framework for incident response. The NIST incident response process consists of six key steps that organizations should follow to effectively manage and mitigate security incidents.

**Preparation** - This initial step involves establishing and training an incident response team, developing incident response policies and procedures, and ensuring that necessary tools and resources are in place. Organizations should also conduct regular training and simulations to ensure that team members are familiar with their roles and responsibilities during an incident.

**Detection and Analysis** - In this phase, organizations must identify and analyze potential security incidents. This involves monitoring systems and networks for unusual activity, utilizing intrusion detection systems, and analyzing alerts to determine whether an incident has occurred(Cichonski et al, 2025). Effective detection relies on having robust logging and monitoring capabilities in place.

**Containment, Eradication, and Recovery** - Once an incident is confirmed, the next step is to contain the incident to prevent further damage. This may involve isolating affected systems or networks. After containment, organizations should eradicate the root cause of the incident, such as removing malware or closing vulnerabilities(Vicente, 2024). Finally, recovery involves restoring systems to normal operations and ensuring that they are secure before bringing them back online.

**Post-Incident Activity** - After the incident has been resolved, organizations should conduct a thorough review of the incident to understand what happened, how it was handled, and what could be improved(Cranford, 2023). This includes documenting lessons learned, updating incident response plans, and making necessary changes to policies and procedures to prevent similar incidents in the future.

**Communication** - Throughout the incident response process, effective communication is vital. This includes internal communication within the incident response team and external communication with stakeholders, customers, and regulatory bodies as necessary. Clear communication helps manage expectations and maintain trust during and after an incident.

**Continuous Improvement** - The final step emphasizes the importance of learning from each incident. Organizations should regularly review and update their incident response plans based on the insights gained from past incidents and ongoing threat intelligence(BlueVoyant, 2024). This continuous improvement process ensures that the organization remains resilient against evolving threats.

References:

bluevoyant. (2024). *NIST Incident Response: Framework and Key Recommendations*. BlueVoyant. https://www.bluevoyant.com/knowledge-center/nist-incident-response-framework-and-key-recommendations

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2025). Computer security incident handling guide. *Computer Security Incident Handling Guide*, *2*(2). https://doi.org/10.6028/nist.sp.800-61r2

Cranford, J. (2023, July 6). *Incident Response Plan: Frameworks and Steps | CrowdStrike*. Crowdstrike.com. https://www.crowdstrike.com/en-us/cybersecurity-101/incident-response/incident-response-steps/

Vicente, V. (2024). *NIST Incident Response: Your Go-To Guide to Handling Cybersecurity Incidents*. Auditboard.com. https://auditboard.com/blog/nist-incident-response