1-2 Journal: Incident Playbooks

Joshua Merren

Southern New Hampshire University

CYB 320: Incident Response and Investigation

Professor Noah Nicholls

29 October 2024

Incident playbooks are crucial for managing and mitigating cybersecurity threats effectively. They assist organizations in preparing for, responding to, and recovering from security incidents by classifying incidents into high, medium, and low levels, helping prioritize responses accordingly. For example, a High-level incident, such as a severe network breach that threatens sensitive data, demands immediate and thorough action involving multiple teams and often external partners. Medium-level incidents, such as unauthorized access that does not compromise sensitive data, still require thorough investigation. In contrast, low-level incidents may only require routine checks to confirm that no further action is needed. By utilizing such classifications, organizations can efficiently manage resources and ensure that their responses are proportionate to the threat level, thus enhancing their cybersecurity posture and response efficiency (Nelson et al., 2024).

When severe incidents like a lightning storm hindering an organization's primary data center occur, business continuity and disaster recovery plans are triggered. The business continuity plan ensures that essential business functions can continue by transitioning operations to a secondary site or employing scalable cloud-based technologies to handle increased loads. Concurrently, the disaster recovery plan focuses on restoring critical systems, potentially using backup generators to restore power or retrieving data from backups to reboot essential services. These plans may include rerouting network traffic through secondary data centers and leveraging cloud services to manage client requests, minimizing service disruption, and maintaining customer trust during critical periods (Nelson et al., 2024).

Effective incident response extends beyond addressing immediate threats and includes planning for long-term recovery and prevention. After managing an incident, organizations should review what occurred and update their playbooks based on the lessons learned. This

continuous improvement process typically involves examining the attack vectors used, the effectiveness of the response, and any exploited protocol gaps. Updates to the incident playbook include refining communication protocols, enhancing security measures, and implementing new technical solutions to prevent similar incidents. This preparation, response, recovery, and improvement cycle keeps security practices robust and ensures that the organization is better prepared to handle future threats (Nelson et al., 2024).

Reference

Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2024). *Incident Response Recommendations and Considerations for cybersecurity Risk Management:* https://doi.org/10.6028/nist.sp.800-61r3.ipd