4-3 Project One: Stepping Stone Three

Joshua Merren

Southern New Hampshire University

CYB 320: Incident Response and Investigation

Professor Noah Nicholls

20 November 2024

In response to the sprinkler activation incident in the server room, the first step is to replace the damaged universal power supply (UPS) and router to restore basic network functionality. After replacing these pieces, it is critical to reconfigure the router with its original firewall rules and routing tables. Since backups are conducted weekly to the cloud, retrieving the most recent backup is essential for restoring the data and settings lost during the incident. This approach quickly restores the system to its operational state, minimizing downtime and disruption. Enhancing response efficiency, such as maintaining clear disaster recovery procedures, can significantly reduce the time needed to recover from such incidents (Ibm, 2024).

The current weekly backup strategy may leave gaps in recovery, especially for frequently updated configurations such as firewall rules and routing tables. Transitioning to a more frequent backup approach, such as daily incremental or even real-time backups, can improve recovery time objectives (RTOs) and minimize data loss. Regularly test backup integrity to ensure data reliability and full recoverability when needed. Maintaining offline backups alongside cloud-based systems provides an added layer of security against data corruption or cloud service failures (“Best Practices for Cloud Data Backup and Disaster Recovery,” 2024).

To mitigate similar risks in the future, the organization should update its policies to include regular inspections of fire suppression systems to prevent accidental activations. Moreover, incorporating training programs to educate employees on responding to such incidents and implementing stricter access controls to server rooms could reduce risks. These measures enhance organizational preparedness and response capability (Oadesunloro, 2023).

Following the malware infection caused by a personal USB drive, isolating the compromised workstation from the network is the first and most critical step to prevent further spread. Wipe the infected workstation and rebuild it using stored clean system images. Restoring

the most recent backup for the corrupted Excel file on the network drive is essential to recover the lost data. However, changes made since the last backup may be irretrievable, highlighting the importance of implementing more frequent backup intervals ("Best Practices for Cloud Data Backup and Disaster Recovery," 2024).

The existing weekly backup strategy may need to be revised to protect rapidly updated documents or files. Incorporating daily or hourly backups for critical data can significantly enhance data recovery processes and reduce potential losses. Furthermore, employing advanced file versioning techniques could allow the restoration of specific file versions before corruption occurs. This ensures better flexibility in recovery and improved protection against similar incidents (Oadesunloro, 2023).

To prevent similar incidents in the future, the organization should restrict or block the use of personal USB drives on company systems by updating its endpoint security policies. Regular employee training sessions highlighting the risks of unauthorized devices and enforcing strict compliance with these policies are essential. Integrating automated endpoint protection tools to monitor and block potentially malicious devices can further strengthen the organization's security posture (Orszula, 2024).

Incident Response Plans (IRPs), Business Continuity Plans (BCPs), and Disaster Recovery Plans (DRPs) must work in tandem to ensure comprehensive contingency planning. IRPs address an incident's immediate containment and mitigation, while BCPs focus on maintaining critical business operations during disruptions. DRPs, in turn, detail the steps needed to restore IT systems and data following a disaster. These plans form a cohesive strategy to minimize downtime and ensure operational continuity (Ibm, 2024).

Regular training sessions, disaster recovery drills, and the implementation of an effective awareness program actively engage all employees in preparedness. These exercises familiarize staff with their roles during an incident and highlight the importance of adhering to established protocols. Additionally, updating these plans to reflect technological, infrastructure, or organizational structure changes ensures their continued effectiveness. Providing employees with accessible resources such as quick-reference guides and conducting post-incident reviews can improve preparedness (Orszula, 2024).

Reflecting on the cumulative lessons from this project, proactive planning and regular updates to IRPs, BCPs, and DRPs are essential for organizational resilience. Engaging all levels of the organization in developing and testing these plans fosters a culture of preparedness. This approach ensures that organizations can navigate disruptions effectively, safeguarding operational continuity and stakeholder confidence (Oadesunloro, 2023).

References:

Best practices for cloud data backup and disaster recovery. (2024, July 7). *Cross4Cloud*. Retrieved November 20, 2024, from https://cross4cloud.com/cloud-corner/blog/multi-cloud-strategy/best-practices-for-cloud-data-backup-and-disaster-recovery/

Ibm. (2024, August 16). Disaster Recovery Plan. *What is a disaster recovery plan (DRP)?* Retrieved November 20, 2024, from https://www.ibm.com/topics/disaster-recovery-plan

Oadesunloro. (2023, December 1). *How to create a Disaster Recovery Plan (DRP) - CrashPlan*. CrashPlan | Endpoint Backup Solutions for Business. https://www.crashplan.com/resources/guide/how-to-create-a-disaster-recovery-plan/

Orszula, B. (2024, September 3). *A comprehensive guide to managed backup and disaster recovery*. InterVision Systems. Retrieved November 20, 2024, from https://intervision.com/blog-comprehensive-guide-to-managed-backup-and-disaster-recovery/