3-2 Project One Stepping Stone Two: Business Continuity Scenarios

Joshua Merren

Southern New Hampshire University

CYB 320: Incident Response and Investigation

Professor Noah Nicholls

12 November 2024

I. Business Continuity Scenario One: Sprinkler System in Server Room

A. Short-term solutions for displacement of employees:

In response to the sprinkler activation, employees can relocate to a designated recovery site equipped with necessary workstations and resources, ensuring minimal disruption. If a physical relocation is not feasible, implementing a comprehensive remote work policy can be an effective alternative. This policy should include issuing company laptops, ensuring secure access through VPNs, and providing support for remote collaboration tools like Microsoft Teams or Slack. This setup supports continuity and allows employees to maintain productivity from home or any remote location, duplicating their office environment virtually.

B. Short-term solutions for processes and hardware:

If water damage compromises hardware, deploying temporary hardware and utilizing cloud services can keep critical applications running. For instance, renting servers or using Infrastructure as a Service (IaaS) options like Amazon Web Services or Microsoft Azure can replace damaged Infrastructure. Activating business continuity provisions in service-level agreements (SLAs) with cloud providers complements this by ensuring rapid resource provisioning. Portable IT equipment such as laptops and mobile hotspots can also be distributed to critical staff to maintain operational capabilities.

C. Failover solution:

A geographically diverse disaster recovery site would be the leading failover solution, with real-time data replication from the primary server room. For instance, a VMware Site Recovery Manager service can automate the failover and failback processes, reducing downtime and operational risk. Such a setup would require strong data communication links and regular drills to ensure employees are familiar with emergency operations, enhancing the organization's resilience to physical incidents affecting IT infrastructure.

D. CIA triad importance ranking:

In this scenario, Availability is paramount because the physical damage to the server room poses an immediate threat to business operations. The next priority, Integrity, ensures that no data has been corrupted by the incident; regular checksum verifications and backups can aid in this. Confidentiality remains a lower priority here, as the incident does not inherently involve unauthorized data access. However, measures such as encrypted backups and secure data transfer protocols should still be in place to protect data during recovery operations.

II. Business Continuity Scenario Two: Workstation Locked by Malware

A. Short-term solutions for displacement of employees:

In the face of a malware attack, quickly setting up unaffected workstations in a clean environment is crucial. Employers could also facilitate remote work setups by ensuring that employees have secure, remote access to necessary systems through VPNs and by accelerating the deployment of virtual desktop infrastructure (VDI). This would allow employees to work from home using virtual desktops that mirror their office setup, ensuring continuity and security. We could also use temporary office spaces with pre-configured laptops to accommodate displaced staff.

B. Short-term solutions for processes and hardware:

Immediate response to a malware incident on a workstation should include isolating the affected device to prevent network spread. Utilizing advanced endpoint protection solutions, such as those offered by Symantec or McAfee, which can detect and quarantine ransomware, is essential. Simultaneously, IT teams should initiate a forensic analysis to determine the malware's entry point and patch vulnerabilities. Rapid deployment of updates and patches to all other systems in the network can prevent further infections.

C. Failover solution:

Implementing an EDR system would automatically detect abnormal activities and could shut down compromised systems while alerting administrators. Automated processes for backing up and restoring data from unaffected backups, combined with such systems, ensure minimal downtime. Additionally, network segmentation can prevent the spread of malware to critical parts of the network, thereby maintaining essential services and business functions even during an attack.

D. CIA triad importance ranking:

For this malware incident, Integrity takes precedence because the malware could alter or damage files and systems. Availability follows closely, as the primary goal is to ensure that all employees can continue their work without interruption. Confidentiality is crucial to prevent any potential data leaks caused by the malware, mainly if the malware variant includes data exfiltration abilities. Safeguarding against such threats involves proactive monitoring and deploying intrusion detection systems (IDS).