Project One: Stepping Stone One Incident Response Scenarios

Joshua Merren

Southern New Hampshire University

CYB 320: Incident Response and Investigation

Professor Noah Nicholls

6 November 2024

I. Incident Response Scenario One

A. Which computer **assets** are affected by the incident?

The incident in the server room involves crucial computer assets like servers, routers, and network switches. These are essential for the functioning of our network and business operations. Their exposure to water can cause short circuits and permanent damage, potentially leading to significant data loss. Prompt evaluation is necessary to determine the scope of the water damage. Restoring these assets as quickly as possible is crucial to resume normal operations. It is essential to prioritize actions to lower the effects on these critical assets.

B. Are the affected assets critical for **business operations**?

The affected assets are essential for the continuity of our business operations. Servers in the server room manage our data and applications critical for day-to-day business operations. Any disruption to these systems can halt employee tasks and customer transactions, leading to operational and financial setbacks. Understanding the critical nature of these assets helps prioritize our response efforts. Quick response is vital to minimize downtime and maintain business continuity. It is crucial that these systems are protected and quickly restored when incidents occur.

C. What is the **severity** of the impact to business on a scale of low, medium, or high? Justify your response.

The severity of this incident is high because the server room houses our most critical hardware. Water damage may cause prolonged downtime due to necessary repairs or replacements. The potential data loss could be irreversible, affecting our ability to serve customers and manage internal operations. Such an incident not only affects our current operational ability but can also tarnish our reputation with clients. Assessing and addressing this impact quickly is crucial to mitigate further losses. Our response must be prompt and effective to prevent significant business disruption.

D. What is one of the **first actions** you take to respond? Justify your response.

I would first turn off the power to the server room to prevent electrical hazards and further damage. This step is crucial for the safety of the response team and the preservation of undamaged equipment. I would then assess the moisture level to determine which equipment can be saved and which cannot. Prioritizing the safety of personnel and securing the environment are essential before any recovery efforts begin. This approach minimizes additional risks and sets the stage for adequate recovery. Ensuring a methodical and safe response is critical in managing the incident efficiently.

E. What strategies can you propose to **contain** the incident?

To contain the incident, my immediate strategy would be to use industrial dehumidifiers and fans to dry out the affected area quickly. Removing all moisture is critical to prevent further damage to the electronic components. I also arrange for a thorough equipment inspection to assess the need for repairs or replacements. Prioritizing which systems must be restored based on

their business criticality would follow. This approach would help in resuming operations swiftly and effectively. Containment strategies should focus on immediate and long-term actions to secure our assets.

F. What strategies can you recommend to **minimize the possibility** of this type of incident recurring in the future?

To minimize the recurrence of such incidents, I recommend installing water detection systems in the server room to alert us before the situation escalates. Integrate these systems with our building's management system for a quick response. Additionally, it is crucial to reevaluate the placement of critical infrastructure away from potential water hazards. Regular maintenance and checks of the sprinkler system can prevent accidental incidents. Establishing protocols for immediate action upon catching a fault in the sprinkler system would also be vital. These strategies can strengthen our resilience against such unexpected incidents.

II. Incident Response Scenario Two

A. Which computer **assets** are affected by the incident?

The incident likely locked a single workstation with ransomware, affecting the computer asset. This machine is necessary for the daily operations of the employee who reported the issue. If not contained, the infection risks spreading to other network-connected devices. Assessing the network for further infections is crucial to understanding the full impact. Immediate isolation of the affected workstation will help prevent further spread. Identifying and securing any network vulnerabilities the ransomware could exploit is also essential.

B. Are the affected assets critical for **business operations**?

The criticality of the affected workstation depends on its specific use within our organization. The impact could be severe if it contains sensitive information or supports critical business operations. Determining the roles and data access of the infected workstation helps assess the potential broader impact. This evaluation will show our response plan and prioritization of recovery efforts. Protecting assets critical to our operations is a top priority in our incident response plan. Ensuring the tiniest disruption in our business operations is crucial during this process.

C. What is the **severity** of the impact to business on a scale of low, medium, or high? Justify your response.

This incident initially receives a medium severity assessment. However, this could escalate if the infection spreads to other systems or involves critical data loss. Immediate actions to contain the ransomware will determine if the severity increases. The potential for widespread disruption to our network makes it crucial to act swiftly. A thorough investigation will reveal the extent of the compromise and help mitigate the risks. Our response must be strong to protect our assets and maintain business continuity.

D. What is one of the **first actions** you take to respond? Justify your response.

I would first isolate the infected workstation from the network in response to the incident. This would help prevent the ransomware from communicating with its controller and spreading to other systems. Immediate isolation helps contain the threat and provides time for a detailed investigation. Ensuring backups are up-to-date and unaffected is also a priority to boost recovery. This step is critical in minimizing the impact and restoring normal operations. Quick and decisive actions are essential to manage the incident effectively.

E. What strategies can you propose to **contain** the incident?

I would first ensure the infected system is completely isolated to contain the ransomware. Then, running a complete scan using updated anti-malware software will help identify and neutralize the ransomware. Investigating how the ransomware entered the system is essential to prevent similar breaches. Collaboration with IT security experts can provide insights and enhance our defensive strategies. Monitoring network traffic for anomalies and strengthening firewall rules are effective containment strategies. Our goal is to neutralize threats and restore secure operations quickly.

F. What strategies can you recommend to **minimize the possibility** of this type of incident recurring in the future?

Preventing future ransomware incidents involves enhancing our cybersecurity measures and employee training. Implementing strict policies on using external devices and conducting regular security audits will help identify vulnerabilities. Employees should receive training on recognizing and responding to security threats, such as suspicious emails or unauthorized device

usage. Updating our anti-virus and anti-malware software regularly is also critical. Maintaining robust data backups and having a clear incident response plan are also essential. These steps will help us to strengthen our defenses and minimize the risks of future incidents.