6-1 Project One: Incident Response and Recovery Recommendations

Joshua Merren

Southern New Hampshire University

CYB 320: Incident Response and Investigation

Professor Noah Nicholls

4 December 2024

The ransomware incident primarily affects several critical assets, beginning with the Finance department workstation where the infection was first detected. This device is central to the employee's daily tasks and contains crucial financial files. Additionally, shared drives and networked resources used by the Finance department are likely affected, as ransomware typically spreads laterally across the network. Other departments, especially those not adequately segmented from the network, are also at risk due to the discovered segmentation gaps. Moreover, the organization's backup system, which performs monthly cumulative backups, could be compromised if ransomware accessed the locally stored backups. These interconnected assets form a system vulnerable to further disruption, emphasizing the need for immediate action. Any databases shared across departments may also face encryption risks, causing delays in key business functions. Shared data reliance in critical software systems likely impacts their performance, reducing overall productivity. Identifying and mapping the scope of affected assets ensures a targeted and effective response (Mancuso, 2024).

Containing the ransomware begins with isolating the infected workstation by disconnecting it from the network. This action prevents the malware from propagating to other devices. Next, all shared drives and network resources should be temporarily disabled to limit access and stop the spread of encrypted files. Enforce network segmentation immediately to isolate compromised departments from unaffected ones. Using endpoint detection and response (EDR) tools can help identify and isolate other potentially infected systems automatically. Additionally, firewall rules must be updated to block suspicious traffic, including communication with any command-and-control servers used by the ransomware. Communicating with employees is essential; they must stay informed to avoid interacting with suspicious files or emails. Physical access to systems should also be restricted to prevent further tampering while containment is underway. The organization should actively enforce a freeze on new software downloads to limit additional vulnerabilities. These measures work together to quickly limit the ransomware's spread and protect unaffected areas of the network (Blanchard, 2023).

Remediation begins with eradicating the ransomware from affected systems using advanced anti-malware software. IT teams must wipe and rebuild infected devices using clean system images and verify that backups are uninfected before restoring critical files. Given the monthly backup schedule, some data may be unrecoverable, highlighting the importance of implementing more frequent backup strategies. After restoring systems, it is essential to apply patch management to close the vulnerabilities exploited by the ransomware. Reset the passwords for impacted accounts to prevent unauthorized access. IT should review logs to identify how the ransomware infiltrated the network and implement measures to block similar entry methods in the future. Collaborating with external cybersecurity experts for deeper forensic analysis can further strengthen the organization's defenses. Any temporary containment measures should be gradually removed after remediation to restore normal functionality. Managers should brief employees on lessons learned from the incident to prevent its recurrence actively. These steps ensure a comprehensive cleanup and help fortify systems against future attacks (Dansimp, 2024).

To prevent future ransomware attacks, the organization should implement multiple strategies. First, frequent data backups—performed daily or hourly—should be stored in secure, offsite locations to ensure quick recovery without paying ransoms. Second, train employees to identify phishing attempts and other common ransomware vectors. Third, organizations should actively use endpoint protection tools to monitor and block unauthorized devices like personal USB drives. Fourth, regular software updates and patches are necessary to address vulnerabilities. Email filtering solutions must also be enhanced to prevent malicious links or attachments from reaching users. Lastly, a detailed incident response plan for ransomware should be established and regularly tested through drills to ensure rapid and coordinated responses during incidents. Conduct periodic audits of IT systems to identify and address potential vulnerabilities. Encouraging employees to report suspicious activity promptly can further bolster defense mechanisms. These proactive measures ensure that the organization remains prepared and less susceptible to ransomware attacks (Antal, 2024).

Maintaining business continuity during recovery involves enabling unaffected employees to work from alternate setups. Secure remote work should be supported through virtual private networks (VPNs) and virtual desktop infrastructure (VDI). Employees should have access to cloud-based tools, ensuring they can collaborate and access necessary resources remotely. For critical tasks like financial reporting, alternate devices can be provided to affected users, preconfigured with secure software to ensure productivity. By prioritizing tasks based on their importance to business operations, organizations actively direct resources to maintain essential services, temporarily delaying secondary processes. Clear communication is vital; inform employees and customers about the recovery timeline and interim processes. Transparent communication builds trust and keeps productivity levels as high as possible. Providing temporary office spaces for employees who require in-person work ensures minimal disruption to key processes. Partnering with third-party IT service providers can supplement internal efforts to maintain operations. These strategies provide the organization's resilience during recovery (Blanchard, 2023).

A failover system ensures operational continuity by automatically switching to a secondary system when the primary one fails. For this organization, implementing failover solutions, such as redundant servers with real-time replication, can minimize downtime caused by ransomware. Train employees to understand how failover activation impacts their workflows, ensuring they can continue tasks seamlessly. Processes must include regular testing of failover systems through drills to confirm that they work as intended during an emergency. On the technology side, investments in robust failover solutions, such as cloud-based redundancy, will be necessary. These systems must be integrated with existing infrastructure to allow smooth transitions without data loss. Overall, failover systems increase organizational resilience and reduce disruption during ransomware attacks (Antal, 2024).

The organization must revise the current monthly cumulative backup strategy to improve recoverability. Updating to a daily or hourly incremental backup schedule stored in secure, offsite locations or cloud environments will enhance data availability. Employees need training to access and restore files from these updated backups actively. Routine backup integrity testing should confirm that processes can be used effectively during emergencies. Technologically, adopting advanced backup solutions with file versioning ensures that organizations can recover specific file versions unaffected by ransomware. This update reduces data loss risk, increases recovery speed, and ensures critical operations can resume quickly after an incident. Additionally, implementing automation for backups reduces human error and ensures consistency in data protection. Regularly reviewing and updating the backup strategy ensures it evolves with emerging threats and organizational needs. Finally, integrating backup solutions with a real-time monitoring system will help detect and address potential issues before they escalate (Findling, 2024).

References

Antal, G. (2024, November 26). *The Road to Redemption: Ransomware Recovery Strategies for businesses*. Heimdal Security Blog. Retrieved December 4, 2024, from https://heimdalsecurity.com/blog/ransomware-recovery-strategies/

Blanchard, A. (2023, November 15). How to maintain business continuity in the age of ransomware. *Ransomware.org*. Retrieved December 4, 2024, from https://ransomware.org/blog/how-to-maintain-business-continuity-in-the-age-of-ransomware/

Dansimp. (2024, October 16). *Prepare for ransomware attacks with a backup and recovery plan*. Microsoft Learn. Retrieved December 4, 2024, from https://learn.microsoft.com/en-us/security/ransomware/protect-against-ransomware-phase1

Findling, I. (2024, December 2). *5 Strategies to combat ransomware and ensure data security in Microsoft 365*. The Hacker News. Retrieved December 4, 2024, from https://thehackernews.com/expert-insights/2024/12/5-strategies-to-combat-ransomware-and.html

Mancuso, P. (2024, September 15). Building a Resilient Business Continuity Plan for Ransomware Attacks. *Vitalintegrators*. Retrieved December 4, 2024, from https://www.vitalintegrators.com/blog/business-continuity-plan-for-ransomeware