Southern New Hampshire University

Project Two: “Incident Analysis Brief”

Written By: Max Navarrette

Course: CYB-200-J9875 Cybersecurity Foundations 24EW4

Professor: Robert Brickan

Southern New Hampshire University

Financial Organization Incident Analysis Brief

To: Payroll Administrator

From: Max Navarrette

Subject: Incident Analysis and Security Enhancement Recommendations

Date: 04/08/2024

1. **Executive Summary:**

This brief analyzes a critical security incident involving unauthorized physical and network access at our financial institution. A suspicious individual (The Perpetrator) was observed leaving the payroll administrator's office with potentially stolen documents and an electronic device. This breach coincided with unauthorized foreign network activity on the administrator's account, inaccuracies in payroll reports, and intermittent outages of the payroll application. These events have raised serious concerns about the "integrity" and security of sensitive financial data and internal systems. Our response and the subsequent recommendations aim to address these vulnerabilities and prevent future occurrences, strengthening the financial organization's overall security posture.

2. **Security Objective: "Integrity"**

   A. **Impact of Security Objective Loss:**

The breach in our financial system's "integrity," evidenced by unauthorized access and document theft, has grave implications. This deliberate attack has put immediate transactions at

risk and threatens our institution's long-term trust (Kim & Solomon, 2023, pp. 169-213). Incorrect payroll data could lead to employee disputes and financial inaccuracies (Kral, 2011). The breach, likely by someone with system knowledge, calls for an immediate overhaul of our security protocols and a strengthened culture of awareness (Siponen, 2000). To safeguard against such vulnerabilities, we must implement a robust security framework, enforce strict access controls, and foster persistent vigilance among our team (Benzel et al., n.d.). Addressing these issues holistically is pivotal for restoring confidence and ensuring the resilience of financial operations (University, S.N.H., n.d.; Design Principles, 2001).

B. Negative Impacts on People, Process, and Technologies:

The security breach at our financial institution has profoundly impacted people, processes, and technology, highlighting critical vulnerabilities in our security measures. The breach, involving physical theft and unauthorized network access, has compromised the integrity of our payroll system, a cornerstone of our operational integrity, leading to inaccuracies in payroll reports and causing system outages (Kim & Solomon, 2023, pp.169-213; Kral, 2011). The resulting erosion of employee trust and potential damage to client relationships underscores the necessity of a security-aware organizational culture and stringent access control measures (Siponen, 2000). Our current security protocols must be scrutinized and realigned with industry-standard design principles for security to ensure the confidentiality, integrity, and availability of our systems, as per the C.I.A. Triad (Benzel et al., n.d.; Levin et al., 2007; University, S.N.H., n.d.). In response to this incident, implementing a cybersecurity playbook becomes essential to guide the organization in reinforcing its security posture, thereby restoring stakeholder trust and safeguarding against future threats (Navarrette, n.d.; Design Principles, 2001).

3. **Recommendations:**

- **Fundamental Security Design Principles Selected:**
  - Layering (Defense in Depth), Least Privilege

A. Implementation of Security Design Principles

To reinforce our defense, we should implement multiple layers of security (defense in depth), including physical security measures, network segmentation, and strict access controls. Additionally, applying the principles of least privilege will ensure that users have only the access necessary to perform their job functions, reducing the risk of unauthorized data manipulation (Levin et al., 2007). Defense in depth, a multi-layered defense strategy, would encompass enhanced physical security to thwart unauthorized entry, robust network segmentation to protect critical systems, and comprehensive access controls to verify and limit user access in alignment with their job requirements (Benzel et al., n.d.). This strategy is particularly pertinent given the incident's indication of insufficient physical and logical access control measures, which allowed the theft of sensitive data and misuse of the payroll administrator's account (Kim & Solomon, 2023, pp.169-213). Concurrently, the principle of least privilege must be rigorously applied to ensure that individuals are granted access only to the information and resources essential for their duties, thereby minimizing the risk of unauthorized access or data manipulation (Levin et al., 2007). According to the C.I.A. Triad, these measures would safeguard the confidentiality, integrity, and availability of our information systems, which is imperative in restoring trust and upholding the organization's reputation (University, S.N.H., n.d.). By integrating these fundamental security design principles into our cybersecurity playbook, we will address the vulnerabilities revealed by this incident and establish a resilient and adaptive security framework to deter and withstand future cyber threats.

B. Balancing Impacts:

We must strategically implement in-depth defense principles and least privilege to mitigate the security breach's impact and strengthen our financial institution's cybersecurity posture. By embedding multiple security controls, such as enhanced physical barriers, network segmentation, and multifactor authentication, we create a robust multi-layered defense that minimizes the risk of a single point of failure (University, S.N.H., n.d.; Benzel et al., n.d.). Concurrently, by applying the least privilege principle, we limit user access rights to the bare minimum required to fulfill job duties, thus curtailing the potential for unauthorized data access (Kim & Solomon, 2023, pp-169-213). This security enhancement will be balanced with operational efficiency by integrating comprehensive security awareness training for employees, which is critical for ensuring staff adherence to new protocols without impeding their work (Siponen, 2000). The training will be supported by streamlined processes and advanced technologies designed to facilitate the adoption of security measures, ensuring that our organization maintains a productive yet secure environment. Regular reviews and updates of these security measures will be essential to adapt to evolving cyber threats and maintaining an adequate defense without compromising operational workflows (Kral, 2011). Through this integrated approach, the institution aims to safeguard its assets and maintain trust among stakeholders, ensuring long-term resilience against cyber threats.

C. The most important aspect of the solution:

Implementing defense in depth stands out as the most critical recommendation for our organization, and I strongly advocate it to our manager. This principle is essential in constructing a security architecture with redundant layers that collectively provide robust protection against diverse threats (University, S.N.H., n.d.). The recent security incident revealed considerable

gaps, including the physical theft of sensitive documents and unauthorized access to the network, highlighting the need for a comprehensive approach that spans physical, technical, and administrative domains (Levin et al., 2007). By incorporating defense in depth, we would deploy a combination of physical security enhancements, advanced network defenses like firewalls and intrusion detection systems, and stringent administrative controls, all of which are crucial for safeguarding the confidentiality, integrity, and availability of our financial systems (Benzel et al., n.d.; Kim & Solomon, 2023, pp.169-213). Such a multi-layer strategy mitigates a wide range of risks and ensures operational resilience, aligning with the security objectives essential to maintaining trust and continuity in our institution's operations (Kral, 2011). Therefore, the most critical step toward bolstering our institution's security framework is prioritizing defense implementation in depth.

Results:

The security incident that the financial institution experienced serves as a crucial wake-up call, emphasizing the need for immediate action to address the stark vulnerabilities exposed. Implementing the recommendations for an in-depth strategy for multi-layered defense and enforcing the principle of least privilege will improve our security posture and create a robust framework capable of withstanding similar incidents. These measures are intended to create a resilient security environment that can detect, prevent, and respond to potential breaches more effectively, reducing the likelihood of future occurrences. By acting promptly to integrate these enhancements, we can safeguard our critical assets and maintain the trust of our stakeholders, which is essential for the institution's reputation, business, and operational integrity.

References:

University, S. N. H. (n.d.). *C.I.A. Triad and Fundamental Security Design Principles* (pp. 1–3). SNHU. Retrieved March 14, 2024, from https://learn.snhu.edu/d2l/lor/viewer/viewFile.d2lfile/1546049/22533,-1/

Benzel, T. V., Irvine, C. E., Levin, T. E., Bhaskara, G., Nguyen, T. D., & Clark, P. C. (n.d.). *Design principles for security* (pp. 1–28). Secure Core. https://learn.snhu.edu/d2l/lor/viewer/viewFile.d2lfile/1546049/21566. Secure Core Technical Report | ISI-TR-605 | NPS-CS-05-010 .

Levin, T. E., Irvine, C. E., Benzel, T. V., Bhaskara, G., Clark, P. C., & Nguyen, T. D. (2007). *Design principles and guidelines for security* (pp. 1–34). NAVAL POSTGRADUATE SCHOOL . https://learn.snhu.edu/d2l/lor/viewer/viewFile.d2lfile/1546049/21566. Technical Report: NPS-CS-0 7-0 14, ISI-TR-6 48.

Navarrette, M. A. (n.d.). *Cybersecurity Playbook* (SNHU Edition, pp. 1–17). Template Provided by: Sothern New Hampshire University Professor: Robert Brickan Course: CYB-200-J9875 Cybersecurity Foundations 24EW4.

Benzel, T. V., Irvine, C. E., Levin, T. E., Bhaskara, G., Nguyen, T. D., & Clark, P. C. (n.d.). *Design principles for security* (pp. 1–28). Secure Core. https://learn.snhu.edu/d2l/lor/viewer/viewFile.d2lfile/1546049/21566. Secure Core Technical Report | ISI-TR-605 | NPS-CS-05-010 .

Design Principles. (2001). *Apress/Authoring*, 83–102. Southern New Hampshire University. https://learn.snhu.edu/d2l/lor/viewer/viewFile.d2lfile/1546049/21425,1/. Chapter 6: Design Principles pp.101-102.

Kim, D., & Solomon, M. (2023c). *Fundamentals of information systems security* (4th ed., pp. 1–574). Jones & Bartlett Learning. Chapter 6: Access Control pp.169-213.

Kral, P. (2011). *Incident Handler's Handbook* (pp. 1–19). https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

Siponen, M. T. (2000, March 1). *A conceptual foundation for organizational information security awareness*. Emerald Insight; M.C.B. IP Ltd. https://www.emerald.com/insight/content/doi/10.1108/09685220010371394/full/html. Vol. 8 No. 1, pp. 31-41.