Southern New Hampshire University

Project Three: “Technical Brief”

Written By: Max Navarrette

Course: CYB-200-J9875 Cybersecurity Foundations 24EW4

Professor: Robert Brickan

Southern New Hampshire University

CYB 200 Project Three Scenario Two

You are a security analyst at a local IT firm who has been contracted as a helpdesk for a financial company. (In this situation, your director would be writing a plan for the company.) While on-site, you learn that the company is made up of financial analysts who handle high-income accounts. You learn that analysts are responsible for their own clients, and that they are contracted to not share the personal information of their accounts with anyone outside the company. While you are helping the administrative assistant for this company with an issue around securing the printer, you observe the cleaning crew going from office to office and cubicle to cubicle. They appear to be taking great notice of the information on the analysts' screens. You observe one of the cleaning-crew workers take what appears to be papers out of the "destroy" bin, then move them to try to hide them on their cleaning cart. The other people in the office seem to be ignoring the cleaning crew as they go about their business.

Introduction:

The threat actors in this scenario are the cleaning crew members who are observed taking undue interest in the information displayed on the analysts' screens and even attempting to steal documents from the "destroy" bin. A variety of factors could drive their motivations. For instance, they could be gathering sensitive information for financial gain or acting on behalf of a competitor or a malicious entity seeking to undermine the financial company's operations. According to Kim & Solomon (2023a), threat actors can be motivated by various factors, including monetary gain, competition, or ideological beliefs. In this case, the cleaning crew's actions suggest a motivation rooted in financial gain or competition, as they target a financial company handling high-income accounts (Kim & Solomon, 2023a, pp. 73–113).

Analysis:

Detecting threat actors like the cleaning crew in this scenario requires a multi-faceted approach. One effective method is implementing a robust access control system that restricts unauthorized access to sensitive information. This could involve screen privacy filters to prevent shoulder surfing and secure disposal methods for sensitive documents. According to Kim & Solomon (2023c, pp. 169-213), access control systems are crucial in preventing unauthorized access to information systems. Additionally, employee awareness programs can be beneficial. Employees should be trained to recognize suspicious behavior and report it promptly. As Siponen (2000) suggests, a well-informed workforce can act as an effective first line of defense against internal threats.

In dealing with this threat, it is crucial to consider ethical and legal factors. Ethically, it is essential to respect the privacy of all individuals involved, including the suspected threat actors. Any investigation should be conducted discreetly and professionally, avoiding unnecessary harm or embarrassment. The company must comply with all relevant data protection and privacy laws. Unauthorized access to client information could lead to legal repercussions for the company. According to Kim & Solomon (2023b, pp 414-430), organizations must adhere to various information security standards to ensure information confidentiality, integrity, and availability. In this scenario, the company must ensure that it is not only protecting its clients' information but also operating within the bounds of the law.

Implementing an incident response plan is one effective tactic in responding to and countering this threat. This plan should outline the steps to be taken when a security incident is detected, including the roles and responsibilities of all involved parties. According to Kral (2011), an incident response plan is crucial in minimizing the impact of a security incident and ensuring a swift and effective response. In this scenario, the plan could involve immediate actions such as securing the "destroy" bin and alerting the security team, followed by a thorough investigation. The incident response plan should also include measures to preserve evidence for potential legal proceedings.

The company could implement stricter access control measures to reduce the likelihood of a similar situation occurring in the future. This could include limiting the cleaning crew's access to certain areas during working hours or implementing a clean desk policy where all sensitive information is secured before leaving the workspace. Additionally, the company could invest in secure disposal methods for sensitive documents, such as cross-cut shredders or secure disposal services. As suggested by Kim & Solomon (2023c, pp 169-213), effective access control measures can significantly reduce the risk of internal threats.

Conclusion:

The tactics and methods suggested in this technical brief could have several ramifications. On the positive side, they could significantly enhance the company's security posture, reducing the risk of internal threats and data breaches. This could lead to increased client trust and a more substantial reputation in the industry. However, these measures could also have some negative impacts. For instance, employees could see stricter access control measures as intrusive or inconvenient, potentially affecting morale. Furthermore, implementing these measures could involve significant costs. However, as Johnson et al. (2016) argue, the cost of implementing effective cybersecurity measures is often far less than the potential losses from a data breach or other security incident, as it usually requires much effort.

References:

Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). *Guide to Cyber Threat Information Sharing* (pp. 1–43). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-150.pdf. NIST Special Publication 800-150.

Kim, D., & Solomon, M. (2023a). *Fundamentals of information systems security* (4th ed., pp. 1–574). Jones & Bartlett Learning. Chapter 3: Risks, Threats, and Vulnerabilities pp.72-113.

Kim, D., & Solomon, M. (2023b). *Fundamentals of information systems security* (4th ed., pp. 1–574). Jones & Bartlett Learning. Chapter 13: Information Security Standards pp. 414-430.

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

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.

Navarrette, M. A. (2024). *CYB 200 project two milestone: “Decision aid”* (pp. 1–15). Southern New Hampshire University. Course: CYB-200-J9875 Cybersecurity Foundations 24EW4 Professor: Robert Brickan.

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