**Project Two:**

**Incident Analysis Brief**

Matthew A Keaton

Southern New Hampshire University

CYB 200: Cybersecurity Foundations

Professor Linda Hamons

April 14, 2024

**Scenario Analysis**: Using your work in the case study analyses (Modules Two through Four) and other course resources as reference, select the security objective you think is most relevant to the organization in the case.

* 1. Describe why the loss of your selected security objective (confidentiality, integrity, or availability) reflects the **greatest overall negative impact**on the organization. Use evidence from the scenario and your coursework to support your selection.

The loss of confidentiality reflects the greatest overall negative impact on the financial organization. Confidentiality means “guarding information from everyone except those with rights to it” (Kim & Solomon, 2023, pg. 14). The payroll administrator broke the tenet of confidentiality because she left her workspace unattended without securing the office by locking the door, logging off her computer, and locking the file cabinet. This would help prevent the unauthorized access of the person to confidential information. According to Kim and Solomon (2023, pg. 14) confidential information is considered private data of individuals, intellectual property of the business, and national security for countries and governments. At a large financial organization, any of this confidential information could have been on the manila folders that were taken, employee personal payroll information from the computer, and other businesses payroll information. The loss of confidentiality poses the greatest risk to the large financial company because it damages trust and reputation, can cause major financial losses, lead to identity theft, and other legal actions.

* 1. Summarize the **negative impacts** on people, processes, and technologies associated with the loss of your selected security objective.

The loss of confidentiality has a negative impact on people across the organization because it increases the fear that their personal information has been stolen, potentially putting their families and finances in danger. Also affecting customers losing trust in the organization’s ability to keep their sensitive data safe causing a decrease in valued customers and profits. The incident disrupted the company’s payroll leading to the organization changing the process which can cause delays or errors in employee’s paychecks. Some people would not be able to afford this change of process and could negatively impact their personal lives. The unauthorized access to the network using the payroll administrator's account highlights vulnerabilities in the organization's technology and may need to change their authentication and access control systems.

**Recommendations**: Select two Fundamental Security Design Principles as criteria and recommend solutions to remedy the loss of the selected security objective based on your assessment of the incident.

1. Explain how your solution **implements the selected Fundamental Security Design Principles**. Provide evidence from the scenario and your coursework to support your selections.

A solution to remedy the loss of confidentiality in the large financial organization is to implement fail safe defaults/fail secure. Fail safe defaults/fail secure is the “theory that unless a subject is given explicit access to an object, it should be denied access to that object” (Bishop, 2003). This would prevent the unauthorized user from accessing the information on the computer by adding encryption to the payroll data stored. This would also minimize access to physical work locations such as the office or filing cabinet by adding secure locks. Another fundamental security design to help remedy the loss of confidentiality is layering. Layering is “having multiple forms of security and involves a series of checks and balances to make sure the entire system is secured from multiple perspectives” (Tjaden, 2015). For example, another “layer” of defense that can be implemented to the finance organization, is a system that automatically logs out after a certain amount of time of inactivity. This would prevent sensitive information being left on the screen while the employee takes a coffee break. The same idea can be added to hardware that has automatic locks any time a door or filing cabinet is closed. This would prevent unauthorized access to users who are not issued a key and prevent human error when employees forget to lock the door behind them.

1. Describe how your solution **balances impacts**on people, processes, and technologies.

The solution provided would help people feel more comfortable that their data is safe. Even after a potential threat is identified people will know that their data is still encrypted making it much more difficult to obtain. Also, making people feel safer knowing human error has been minimized by adding extra safeguards such as automatic locks when people forget to lock-up after leaving. Although people should always try their best and remember to lock their office or log out of their computers when they leave, mistakes happen and we tend to forget, having these security solutions makes the process easier instead of having someone check each office in the building or the busy payroll administrator needing to remember one more thing.

1. Explain which aspect of your solution you would recommend to your manager as the **most important to the organization**. Support your response with evidence from the coursework or scenario.

The aspect of my solution that I would recommend to the manager as the most important to the organization is implementing a layered defense. By implementing a layered defense strategy, organizations can enhance their security posture, mitigate risks, and protect against security threats and vulnerabilities. Cybercriminals often target entry points and end users, so having multi-layered security such as monitoring, network, internet, users, devices, firewall and intrusion prevention, patch management, and data protection, is the best approach so that your critical data remains safe from cyberattacks and user error (AMDH Services Limited, 2021). Implementing this security design will not only help the payroll administrator, but every employee, in feeling more comfortable when leaving the office knowing there are multiple defenses protecting sensitive information. This security design will help restore the trust from employees, customers, and business partners that may have been lost from the incident. This solution will also strengthen the overall security defenses for the entire financial organization, not just the payroll department, making it the most important aspect of security.

**References**

AMDH Services Limited. (2021 March, 02). *The Importance of Multi Layered Security*. <https://www.amdhservicesltd.com/the-importance-of-multi-layered-security>

Bishop, M. (2003). Computer security: Art and science. Boston, MA: Addison-Wesley Professional.

Kim, D. & Solomon, M.G. (2023). *Fundamentals of Information Systems Security, 4th Edition*. Jones and Bartlett Publishers. https://openpage ebooks.jblearning.com/wr/viewer.html?skipLastRead=true&oneTimePasscode=ST3209 3eb-26474c27-bdd9-9653b52d36ee&launchOrgCode=jbl&language=en-US#//HTML-1

Tjaden, B. C. (2015). Appendix 1: Cybersecurity first principles. Retrieved from https://users.cs.jmu.edu/tjadenbc/Bootcamp/0-GenCyber-First-Principles.pdf