**YB 200 Project Two**

Douglas Few

Southern New Hampshire University

December 5th, 2020

**Scenario Analysis**

Since integrity is the idea that only authorized users can change information (Kim & Solomon, 2013), I believe the security objective most affected by this scenario is integrity. The report mentions that payroll reports generated the day after the incident occured contained “inaccuracies,” which would signify an unauthorized change. Based on the evidence provided in the report, it is likely that these “inaccuracies” could have been caused by the suspicious-

looking person with the backpack seen by the payroll administrator. This reflects the greatest overall negative impact on the organization because this could mean extra pay being given to an individual, or it could mean one or more people’s pay being shorted. Depending on company policy, this could mean a loss for the organization if the extra pay given to individuals cannot be revoked.

The loss of integrity is also made apparent by the missing manilla folders. While the contents of these folders are currently unknown, the fact that they are missing is a change made by an unauthorized individual. Depending on the contents of the paperwork in the manilla folders, this could negatively impact the organization in a number of ways. For one, this is information that the organization is now forced to invest resources into reobtaining. Since the paperwork is missing from a payroll administrator’s office, it is safe to assume that the paperwork is regarding employee pay. Depending on the contents of the paperwork, the loss of the manilla folders could impact employee pay. For example, if the paperwork was regarding recent terminations, this could result in recently discharged individuals receiving pay that they are no longer entitled to.

Finally, the unexpected outages being experienced by the payroll application is another example of integrity being lost in the organization. While the payroll application is unavailable, employees who are working and should be receiving pay are not being tracked by the application. This could result in employees not receiving pay that they are entitled to.

**Recommendations**

My recommendation is primarily based on the fail-safe fundamental security design principle (Bishop, 2003). By following this principle, each incident mentioned in the incident report could have been stopped. For example, if the file cabinet that contained the missing manilla folders was protected via a lock, then only authorized keyholders would be able to access the folders without using some level of force. Likewise, if the payroll administrator made sure that she locked her computer upon leaving her workspace, no one other than her would be able to log back in and tamper with the payroll application. In this instance, the payroll administrator would be the only one with the password because she’s the only employee that needs that privilege in order to perform her duties. Using the fundamental security design principle of layering, the payroll administrator could make it even more difficult for a threat actor to enact a similar event in the future (Tjaden, 2015). For example, on top of locking her computer when she leaves her workspace, she could also lock her office so that only those employees with a key to the office have the ability to enter it. While both of these methods constitute a fail-safe, doing them together is an act of layering.

One way my solution will impact the corporation is by making payroll more secure. This ensures that employees can feel confident that their pay is correct and frees the company from having to correct potential issues regarding payroll. This solution also helps to prevent sabotage to company technologies by reducing the likelihood that a potential saboteur will be able to access company computers (US Legal, 2020). The issue regarding the payroll application suffering from unexplained outages is likely a result of sabotage, so barring individuals access to company computers prevents them from tampering with them. These solutions can also be applied to people across the entire organization, not just the payroll administration office, thereby improving security across the entire company. Even though payroll administration was affected this time, a threat actor could choose to target client information. By following the recommendations of keeping unattended computers and unoccupied offices locked at all times, client bank account and social security information stays safe and inaccessible to those who do not have authorization to view it.

The solution I would likely recommend as the most important aspect is the principle of fail-safes. Many potential threats can be preemptively avoided by creating barriers that stop unauthorized action from occurring. If the payroll administrator had locked her computer upon walking away from it, the locked computer would have acted as a fail-safe from the threat actor, thereby stopping them from tampering with it. The same applies to if she had locked her door upon leaving her office. Unless someone has a key to the door, they would not be permitted access to the office, thereby protecting everything inside the room. By implementing fail-safes across the organization, any sensitive information can be protected from those who should not be viewing or making changes to it. I would assert to my manager that by implementing fail-safes, they would be taking the most important step in my incident analysis brief.

References

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

Kim, D., & Solomon, M. G. (2013). Fundamentals of information systems security (2nd ed.). Burlington, MA: Jones & Bartlett Publishers.

Tjaden, B. C. (2015). Appendix 1: Cybersecurity first principles. Retrieved from

https://users.cs.jmu.edu/tjadenbc/Bootcamp/0-GenCyber-First-Principles.pdf

US Legal (2020). Sabotage Law and Legal Definition. Retrieved December 09, 2020, from https://definitions.uslegal.com/s/sabotage/