Ronald W. Sudol III

SNHU CYB200

Project Two

08/06/2023

**Incident Analysis Case Study**

The incident in the payroll department underlines several flaws in the execution of our security policy. The result was a number of lost physical files, the loss of trust in the integrity of our data, and periodic losses of access to our payroll application. This incident resulted in a loss in each of the security objective categories. Our payroll data can no longer be considered confidential and due to the periodic outages, its availability has suffered. The greatest overall negative impact, however, is that of integrity. Payroll reports generating inaccuracies are evidence of this. Data is only valuable when it can be trusted. Without integrity, a company and its data cannot be trusted. “Data lacking integrity – that is, data that is not accurate nor valid – is of no use”(Kim & Solomon, 2010).

The negative impact of a loss of integrity affects people, processes, and technologies. “Integrity ensures that no one has changed or deleted data. …Payroll data needs integrity to make sure no one changes a payments after sending it to the printer”(Kim & Solomon, 2010). Employees need to trust the payroll system to maintain morale. Payroll data must be accurate for accounting and finances to remain accurate. The records in the manilla folders that were taken may be irreplaceable and such may leave a hole in future records. In light of these things, we can see the impact of this incident and how this affects the entirety of the organization from the individual employee to the payment methods and recorded data of the organization.

A solution to prevent incidents like this from occurring again in the future would be to establish a back-up database for payroll information that is accessible only to authorized H.R. employees via multifactor authentication. This solution implements the fundamental security design principles of isolation and layering. Isolation is implemented by keeping the back-up database separate from the working database. In the event of data corruption or even a ransomware attack, the back-up database provides a reset point for reestablishing a database with trusted and verifiable data thus preserving data integrity. Layering is implemented by placing an additional authentication layer between the user and the isolated database. This further works to ensure the integrity of the back-up database. “The Best defense is to have multiple layers of control in place, because having multiple layers increases the chances of successfully protecting the system from more attacks than would be possible with just single control”(Kim & Solomon, 2010).

This considers a balance of impacts on people processes and technologies. The back-up database may require more physical space for storing data, but it also creates a reset point for restoring data. The end user may have to go through extra steps to verify and upload data to the back-up database, but in the event of a major incident, the time and effort saved in restoring a database instead of rebuilding it entirely is immeasurable. The use of multifactor authentication keeps the database secure and alleviates some of the responsibility on the part of the end user to secure physical access points by making individual authentication more robust.

The aspect of this solution that is most important to the organization is the idea of isolation. By keeping a back-up of data unavailable through regular access methods, one can ensure that the back-up data is unaffected by any threat actor or incident that can corrupt the integrity of the working database. In today’s data driven world, it can be said that the integrity of a company’s reputation is equivocal to the integrity of that company’s data. A company with a poor reputation for data integrity will find itself struggling to entice new investors. This is detrimental to the success of a business for obvious reasons. “A sound security infrastructure provides the assurance that the organization has employed the necessary controls to comply with all the necessary laws, regulations, and other security requirements. In short, security keeps an organization viable and allows it to conduct business”(Kim & Solomon, 2010).

**CITATIONS:**

Kim, D., & Solomon, M. G. (2010). *Fundamentals of Information Systems Security*. https://openlibrary.org/books/OL25116284M/Fundamentals\_of\_information\_systems\_security

*A Taxonomy of Operational Cyber Security Risks Version 2*. (2014b, May 21). https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=91013