**CYB 200 Project Three**

Douglas Few

Southern New Hampshire University

December 12th, 2020**Introduction**

I will be discussing the second scenario, in which I am a security analyst who has been contracted by a financial company. While touring the building of the financial company, I witnessed a cleaning crew removing documents from a bin labeled “To be destroyed” and hid them on the cleaning cart. In this situation, the cleaning crew is the threat actor as they are stealing assets from company property. Since the financial company deals with high-income accounts, it is safe to assume that the threat actors are looking to profit off of their actions. By stealing documents that are meant to be destroyed, the threat actors could potentially be gaining access to client banking information or social security numbers. With this information, the threat actors could gain access to the clients’ financial accounts.

**Analysis**

The employees at the financial firm all seemed to be ignoring the cleaning crew. This leads me to believe that they either don’t understand the risks involved by letting unauthorized and unqualified individuals view sensitive information, or they’ve developed a misguided level of trust in the cleaning crew. My recommendation for detecting and identifying a threat actor in a situation similar to this is to increase surveillance and supervision. This can be done by hiring a security crew to circulate throughout the facility, or it can be done by installing security cameras throughout the building and hiring several guards to monitor the cameras at all times. Another option, though invasive, would be to check and search every employee as they enter and exit the building.

One big legal concern for the financial company is the liability for financial loss experienced by clients in the event of a threat actor stealing client information. If a threat actor were to steal personal client social security or bank information, the financial company could be held legally accountable by clients affected by the threat act. Depending on the terms of the contracts the analysts have with their clients, it may also be the analysts’ legal responsibility to keep the documents confidential and out of view from any unauthorized individuals. Because of this, they may be responsible for damages resulting from unauthorized sharing of client information. Ethically, it is the company’s responsibility to ensure the safety of their clients and the third-party service providers that enter company property.

In order to counter the threat, the company needs to identify who and what was affected so that those affected can be informed. This way, the affected individuals can be diligent about closing bank accounts and transferring to new accounts. Once informed, the company should also offer assistance in alleviating any potential damage that could happen on account of this threat. For example, the company has an ethical obligation to its clients to offer free credit monitoring (Federal Trade Commission, 2020).

In order to reduce the likelihood of a similar threat happening again, I would utilize the principle of least privilege (CyberArk, 2020). Since access to retired documents is not necessary for the cleaning crew to do its job, the ability to access the documents should never have been made possible in the first place. I would also recommend that retired documents be destroyed immediately, regardless of whether it is convenient for the financial analyst. By leaving documents intact longer than necessary, this opens a window of opportunity for threat actors to steal documents before they are destroyed.

**Conclusion**

One significant ramification of my recommendations comes in the form of consumer trust. According to Hospelhorn (2020), recovering from a loss of reputation resulting from a data breach is most effectively done by being the first to break the news and doing so as quickly as possible. The financial company is going to need to invest in the infrastructure necessary to create a more secure environment. This could include document storage that can be locked, security training for employees, and hardware such as cameras and security monitors. It will also be necessary to replace the cleaning staff with more reliable employees and more vigorously screen future employees. All of this will result in more money being spent by the company in the name of security.

References

CyberArk. (2020). What is Least Privilege Access? PoLP Explained. Retrieved December 12, 2020, from https://www.cyberark.com/what-is/least-privilege/

Federal Trade Commission. (2020). Identity Theft Recovery Steps. Retrieved December 12, 2020, from https://www.identitytheft.gov/info-lost-or-stolen

Hospelhorn, S. (2020, March 30). Analyzing Company Reputation After a Data Breach: Varonis. Retrieved from https://www.varonis.com/blog/company-reputation-after-a-data-breach/