Cybersecurity Technical Brief

William Pascoe

CYB-200: Cybersecurity Foundations

Robert Brickan

August 16, 2025

Cybersecurity Technical Brief

This technical brief provides an analysis of a significant physical security threat observed at the financial firm. The primary threat actors are identified as contract workers, specifically members of the cleaning crew. Their motivation appears to be information gathering for financial gain, likely through the theft and sale of sensitive client data. This aligns with characteristics of financially-motivated cybercriminals, who often seek to exploit a company's most valuable assets—its data—to turn a profit. The observed behavior, including paying close attention to information on screens and pilfering documents from a "destroy" bin, suggests a reconnaissance and exfiltration tactic aimed at acquiring nonpublic financial or personal information. The analysts in the office didn't seem to be paying attention to what the cleaning crew was doing.

To counter this event and prevent further threats I believe that the analysts in the office need more training to recognize and report suspicious activity. A "See Something, Say Something" policy should be a cornerstone of this training (DHS, 2018). To prevent shoulder surfing. Installing privacy screens on the computers would also help to prevent people from seeing what is on the monitor when they are nearby. Implementing and actively monitoring video surveillance in sensitive areas, such as hallways and common office spaces, can help identify and log unusual behavior.

The company has ethical and legal factors to consider in this situation as well. Ethically, the firm has a duty to protect its clients' data. A breach, even if caused by a third-party contractor, is a failure to uphold this duty. Legally, the company is bound by various data privacy regulations, such as GDPR or CCPA. Unauthorized access or data theft can result in severe financial penalties, lawsuits, and a loss of public trust.

In response to the threat that did occur I would recommend replacing the cleaning company as soon as possible. For the new company I would also recommend they do background checks on their employees to ensure that the people around sensitive data are not trying to steal it. The company should also have the cleaning crew operate in the evening when the data is stored securely and analysts have gone home. They should also make sure that sensitive information that is discarded is shredded immediately or placed in a secure manner that prevents people from going through it and removing it (*Protecting Small Businesses*, 2017).

To prevent future threats to client's data the company should implement several protocols. As previously mentioned, privacy screens are on all monitors. Also, analysts need to make sure that all sensitive information is removed from their desks at the end of each day so when the after-hours cleaning crew comes in there is little chance that they will be able to get information that is lying around.

The implementation of these tactics and methods would significantly strengthen the firm's security posture. By shifting from a reactive stance to a proactive one, the company can mitigate the risk of a data breach. The primary ramifications would be an increased level of physical and procedural security, safeguarding against insider threats. This would lead to enhanced client trust and compliance with legal obligations, ultimately protecting the firm's reputation and financial stability

References:

Kim, D., & Solomon, M. (2023). Fundamentals of information systems security (4th ed.). Jones & Bartlett Learning.

Protecting Small Businesses. (2017, September 6). Federal Trade Commission. https://www.ftc.gov/business-guidance/small-businesses

DHS. (2018, July 13). *Recognize the Signs*. Department of Homeland Security. https://www.dhs.gov/see-something-say-something/recognize-the-signs