Cyber Threat Detection and Countermeasures in Financial Firms

Name: Juliano Alves de Souza Professor: Brendan Carey

CYB_200_Project_Three_Juliano_Alves_De_Souza

Introduction

In the rapidly evolving digital age, financial firms are increasingly vulnerable to cyber threats. Threat actors, motivated by various reasons, pose significant risks to the confidentiality, integrity, and availability of sensitive data. This technical brief addresses a specific incident observed within a financial company and provides a comprehensive analysis of the threat actor, detection methods, ethical considerations, and countermeasures.

Identify your threat actors and characterize their motivations or desired outcomes

The observed threat actor in this scenario is a member of the cleaning crew, seemingly involved in the unauthorized removal of papers from the "destroy" bin. Such individuals can be categorized as "insider threats," as they have physical access to the company's premises. Their motivations could range from personal financial gain, blackmail, or even espionage on behalf of competitors or other malicious entities. Therefore, insider threats, especially those driven by financial motives, are among the most challenging to detect and mitigate due to their inherent access and knowledge of the organization.

Analysis

1. Best practices for detecting threat actors:

1. Complete Mediation: Implement strict access control mechanisms that require authentication and authorization for every access request, ensuring that every action is continually checked.
    - Audit Trails: Implement detailed logging mechanisms that record every access to sensitive areas, such as storage rooms or disposal bins. This would allow for a traceable record of who accessed the area and when.
    - Badge Access Systems: Use electronic badge systems for entry into areas where sensitive documents are stored. This ensures that only authorized personnel can access these areas and any unauthorized attempt can be immediately flagged.
2. Isolation: Segregate sensitive documents and data from general waste, ensuring that critical information is stored and destroyed in a controlled and monitored environment.
    - Secure Document Storage: Use locked cabinets or rooms for storing sensitive documents before they are ready for disposal. Only authorized personnel should have the keys or access codes.
    - Dedicated Disposal Bins: Use dedicated, locked bins for documents awaiting destruction. These bins should be distinct from regular trash, reducing the chance of unauthorized access.

3. Encapsulation: Use secure containers or bins for sensitive documents awaiting destruction, ensuring they are tampering evident.
    - Tamper-Evident Containers: For documents awaiting destruction, use containers that show visible signs if tampered with. This can act as a deterrent and also provide a quick visual check for potential breaches.
    - Document Shredders: Instead of placing documents directly into a "destroy" bin, use shredders to immediately destroy sensitive documents. This reduces the window of opportunity for unauthorized removal.

2. Ethical and legal factors:

From an ethical standpoint, employees and contractors are expected to respect the confidentiality and privacy of the company's information. Taking documents, especially from a "destroy" bin, breaches this ethical code. Legally, such actions could be considered theft or corporate espionage, leading to severe consequences, including termination, legal actions, or even imprisonment. However, The company must also consider its legal obligations to stakeholders, especially if the documents contain personal or financial data, which could lead to breaches of data protection regulations.

3. Tactic for responding to and countering this threat actor:

One effective tactic is the implementation of surveillance systems, such as CCTV cameras, in areas where sensitive documents are stored or disposed of. This not only acts as a deterrent but also provides evidence in case of any suspicious activities. Furthermore, train security personnel to recognize and report unusual behaviors, such as someone spending too much time near disposal bins or attempting to access locked cabinets without authorization.

4. Tactic to reduce the likelihood of recurrence:

To prevent similar incidents in the future, the company can employ a strict document management policy, which includes:

- Minimize Trust Surface (Reluctance to Trust): Limit access to sensitive areas, ensuring only authorized personnel can access places where critical documents are stored or disposed of.
- Implement policies that encourage employees to report suspicious activities without fear of retaliation. This can act as an early warning system for potential insider threats.

Conclusion

While the tactics and methods suggested providing a robust framework for detecting and countering threats, they come with potential ramifications. Surveillance systems, for instance, might raise privacy concerns among employees. Strict access controls could slow down operations or lead to perceived mistrust. However, the protection of sensitive data, especially in a financial firm, is paramount. Balancing security with operational efficiency and ethical considerations is crucial for the company's long-term success and reputation.

References:

1. Anderson, R. (2018). Security Engineering. Wiley.
2. Casey, E. (2019). Digital Evidence and Computer Crime. Academic Press.
3. Stolfo, S. J., & Keromytis, A. D. (2020). Insider Attack and Cyber Security. Springer Science & Business Media.