CYS401: Fundamentals of Cybersecurity

Class Activity 3

SCENARIO:

Two "encrypted" laptops containing Protected Health Information (PHI) were stolen from a locked conference room at a client location. These laptops were assigned to IT employees working on a data migration project.

FINDINGS:

A law enforcement investigation determined a security guard responsible for securing the incident location had stolen the two laptops, one of which was recovered by the company. After a thorough investigation and analysis of the recovered computer, no evidence was found indicating unauthorized network intrusion or that PHI was accessed after the computer was stolen. Computer analysis determined that IT employees had stored PHI on an unencrypted partition on the local hard drive. The investigation team determined that over a million members data may have been breached.

ATTACK:

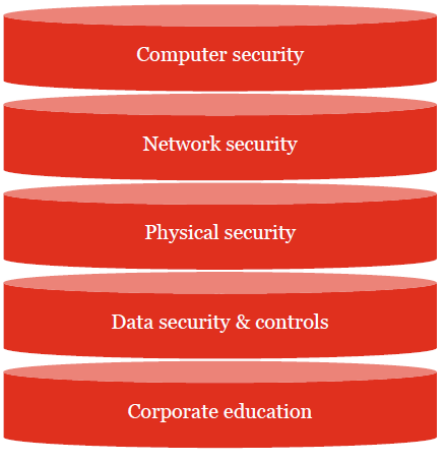
For the given scenario, identify and explain the type of Attack?

IMPACT:

What could be the operational/ financial/ security impact of above attack on the organization.

SECURITY MEASURE/ CONTROLS:

By applying layering approach as shown in figure, how you can help the company to implement a series of policy, technical and corporate culture changes, coupled with employee education, to help prevent the risk of future data breaches. (write **THREE** security control for each layer)



Solution:

ATTACK:

The attack is an intended insider physical theft that led to a confidentiality compromise.

The security guard is the insider threat who carried out a theft of two company laptops. Even though the two laptops were supposed to have been encrypted, the found laptop revealed that employees used to store Protected Health Information (PHI) in the unencrypted partition of the laptop. This implies that there was exposure of sensitive information to a breach.

This constitutes an interception/ confidentiality threat since the sensitive information would have been intercepted by an unauthorized party. The vulnerability is the use of the unencrypted partition to store the PHI while the threat is the insider who committed the theft of the laptops. Confidentiality entails protection of secrecy of data.

Attack classification:

- Threat source: **Human – Internal**
- Threat intent: **Malicious / Intentional**
- Attack method: **Physical theft**
- Main security property affected: **Confidentiality**
- Threat damage type: **Interception**
- Vulnerability exploited: **Unencrypted PHI stored locally**

IMPACT:

Operational Impact

A complete investigation will have to be conducted by the organization in order to assess the type of information that was available on the laptops, and if the information was accessed or not. There will be considerable expenditure of time on investigation, recovery, checking of security procedures, and rectifying the mistakes.

Financial Impact

There could be considerable financial implications for the organization as a result of the cost incurred through the process of investigation, forensic analysis, the acquisition of new equipment, security measures, and training. With more than a million members' information at stake, the financial implications could be substantial.

Impact on Security

First, there is a breach of confidentiality. This is because the PHI data was not encrypted on the device, and therefore any unauthorized individual who acquired the laptop could be able to view the personal details of the members. Although during the investigation it was established that there was no access to PHI data in the recovered laptop, the organization was not sure whether the confidentiality of the data on the stolen devices was intact.

SECURITY MEASURE/ CONTROLS:

Layer 1: People

1. **Security awareness and training:** Provide mandatory training explaining how employees must handle PHI and other sensitive information, including the risks of storing sensitive information locally.
2. **Employee responsibility and accountability:** Employees who work with PHI should understand that they are responsible for following data-protection requirements and reporting violations or suspicious activity.
3. **Security screening and awareness:** Conduct appropriate security checks for employees and personnel who have physical access to sensitive areas, and train staff to recognize and report suspicious behavior.

Layer 2: Policies

1. **Data classification and handling policy:** Classify PHI as sensitive information and establish clear rules governing where it may be stored, processed, and transferred.
2. **Encryption policy:** Require all PHI and other sensitive information stored on laptops to be encrypted. Employees must not store PHI on unencrypted partitions.
3. **Physical access and device-security policy:** Establish procedures governing access to rooms containing company equipment. Laptops containing sensitive information should not be left unattended without additional physical protection, even inside locked rooms.

Layer 3: Technology

1. **Full-disk encryption:** Require encryption of the entire laptop drive and all partitions, preventing employees from accidentally storing PHI on an unencrypted partition. Encryption is specifically identified in the slides as a method for ensuring confidentiality.
2. **Strong authentication and access control:** Require strong user authentication, preferably **two-factor authentication**, and restrict PHI access according to authorized user roles and privileges.
3. **Auditing and monitoring:** Maintain logs of access to sensitive information and monitor company devices so suspicious activity can be detected and investigated. This supports the course's AAA concepts of **auditing and accountability.**