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:

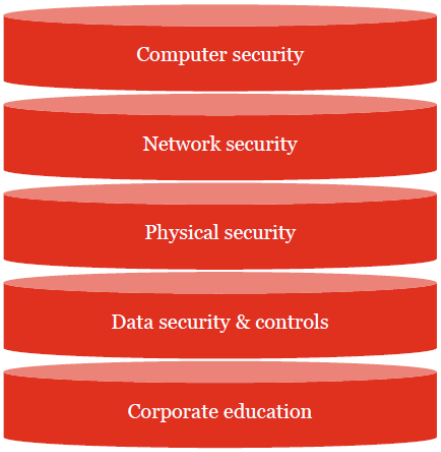
For the given scenario, identify and explain the type of Attack?

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:

SECURITY MEASURE/ CONTROLS: