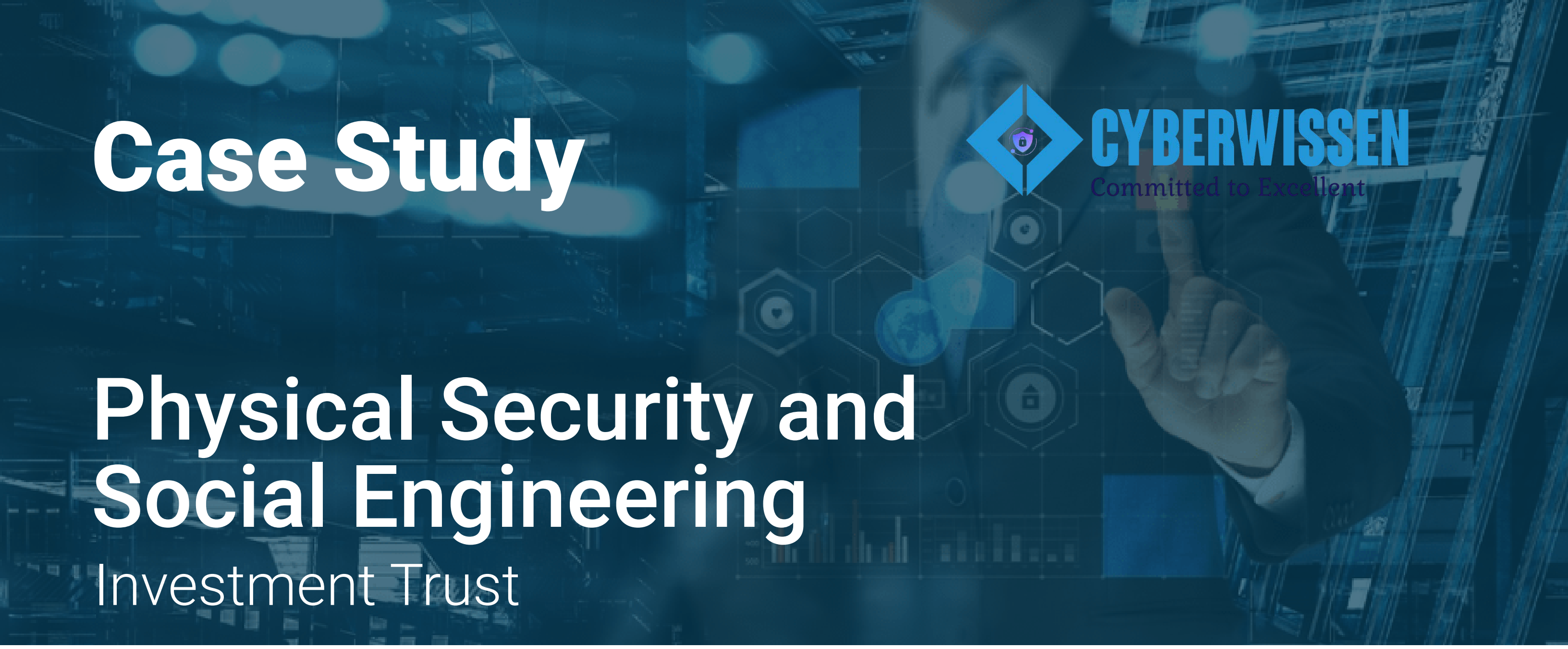

Case Study

CYBERWISSEN
Committed to Excellent

Physical Security and Social Engineering

Investment Trust

Business Challenges

- Easy to gain access to employee secured area
- Data is protected but accessible through an unprotected system

Business Opportunities

- Test physical security of location to ensure all security controls are in place and system is protected
- Verify that staff follows all security protocols
- Provide derailed reports of security testing and solutions

CyberWissen Solutions

- Social engineering
- Physical security penetration testing

Background

A prominent private investment and trust institution understands how critical every aspect of security is to protect the company and their clients. While they perform ongoing testing of their cybersecurity controls both internally and by CyberWissen, they had never tested the physical security of their locations throughout the Netherlands to confirm that not only are the physical security controls in place, but that the staff at each location is following the security protocol as mandated by the internal security team.

Objectives

- Test physical controls that should prevent unauthorized access at each of their locations
- Verify that the security staff at each location follows the company's mandated process for access to data centers/offices where sensitive data is stored
- Obtain detailed report of any vulnerabilities found and recommendations to correct them

Solution

We coordinated with the company's Head of Security to plan our attempts to gain unauthorized access at each location. The results varied greatly by location, from "Very Secure" where controls prevented access and process was followed that kept us from getting near the Data Center to "Weak" where our consultant easily gained access by tailgating an employee into a secured area, and was able to log on to an unprotected system and access protected data. What was most valuable for the client was the extreme detail we provided in their reports that showed exactly how each attempt was made, what prevented access, and which staff needed additional training and supervision to ensure they followed the protocol in the future when it might not be a test.

Fully Secured

Proactive physical security penetration testing