Andree Salvo

Southern New Hampshire University

CYB 420

Instructor: William Mitchell

2-2 Project One Milestone: Security Control Implementation Assessment

---

Introduction

In this scenario, ACME Company is preparing for a future transition to improve its security following weaknesses identified in its people, processes, and technology. The organization relies on multiple departments and critical systems, so issues such as human error, weak procedures, and poor network segmentation can pose significant risks. My project will evaluate those vulnerabilities and apply appropriate controls to help protect ACME's network and daily operations.

Threat Assessment

A. People

Reviewing the Project One Current Organization Infrastructure Diagram, one vulnerability I see is that it lacks physical security at the front, the second door, and the IT equipment closets. **First**, the front door on the first floor is open, meaning personnel at any level can walk straight through it. Next, the second floor has no door; personnel at any level can walk straight through it from the first to the second floor. **Third** is the IT equipment closet. Both closet doors have no locks, allowing any level of personnel and unauthorized individuals to access critical hardware they're not supposed to. After carefully reviewing the infrastructure diagram, it poses a major risk to ACME's network, and anyone could tamper with, steal from, or place unauthorized devices on it.

Next, Employee Awareness Training. Employees might not know the best ways to protect themselves against cyber threats. This makes it more likely they will fall for social engineering tricks. **Phishing, Spear Phishing, Baiting, and tailgating** are four methods attackers use to steal information or gain access to a company's systems or its network.

Process

Lack of documented access-control protocols. The infrastructure diagram shows that the company has not established a structured, documented, or enforced access-control protocol specifying which employees are permitted access to sensitive areas, such as the front/second door, IT closets, Finance, HR, Records, and server areas. Without proper documented procedures, Different departments and individuals might use different security methods. This can lead to unauthorized access, mistakes, or poor handling of important systems. Without clear guidance, it is hard for people, processes, and technology to work together. This increases the company's risk of mistakes and misuse.

Next, there is a Lack of regular security audit monitoring. The diagram specifically shows that there are no signs that ACME conducts regular audits or checks to ensure security controls are maintained. If audits and monitoring are not being maintained, the company could fail to identify, respond to, and recover from a security breach.

Technology

In the diagram, the technology section **lacks network segmentation**. First off, looking at the picture, all departments share a single network (the main switch). Why is this bad? If an attacker compromises one workstation (like in Finance), they could move freely between departments because internal traffic is not properly segmented, allowing attackers to cross from one department to another.

Next, **Poor protection for remote employees**. The remote workers connect to the company's network, but the diagram does not show any secure method for doing so. Without a clear setup, such as a VPN or a firewall, for protecting those connections, there is a higher risk of unauthorized access or interception of their traffic. This makes the remote connection path a weak point for outsiders to try and exploit.

Implementation Approach

People

Installing physical locks, RFID access control readers, and ID Badge access control for both first and second floor doors, and both IT equipment closets. Installing these will only have authorized permission to these floors and doors. And restricting unauthorized personnel from getting inside.

Next, **Employee security awareness training.** A comprehensive guide to security awareness training should be mandated. Deploying this will help employees stay aware of what's coming their way, such as threats they might encounter. Conducting a phishing simulation, clean desk policy, and password hygiene will also help, as it will train new hires and regular employees to be alert.

Process

Implementing **role-based access control (RBAC)** will ensure that employees have the permissions and resources they need for their specific roles. Also, adding the principle of least privilege, as this security practice grants users, applications, and systems only the minimum access and permissions needed to perform their specific tasks within their roles.

Next, set up regular security audits and continuous network monitoring so the system can quickly spot unusual activity or potential breaches, ensuring any security issues are being identified and addressed promptly.

Technology

Applying VLANs and ACLs will help separate ACME's network traffic between departments, preventing devices from being on the same network. VLANs break the network into small, isolated sections, and ACLs filter network traffic by permitting or denying access. Together, they can make it easier to control access, limit broadcast traffic, and protect sensitive areas such as Finance and records.

Lastly, setting up a VPN with multi-factor authentication (MFA) so remote employees can connect to the network safely. Check VPN and MFA logs often to catch any unusual login attempts. Enabling session timeouts so the VPN disconnects when someone is inactive, which helps prevent others from using an open session.