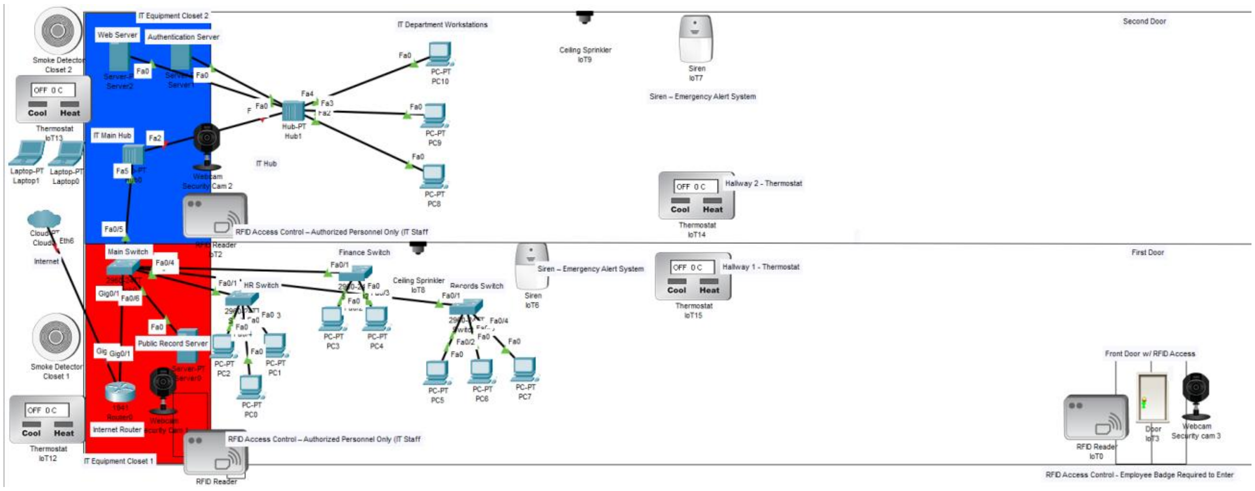
Andree Salvo

Southern New Hampshire University

CYB 420 – 17439

Instructor: William Mitchell

4-2 Project One Submission: Multi-Level Approach to Enterprise Security



Threat Assessment

People

One key problem on the people side is unauthorized access to restricted areas, like the IT equipment closets and the room where the Public Records Server, Web Server, and Authentication Server are located. If someone gets in, they could unplug devices, steal equipment, or plug in an infected USB drive. Another issue is human error. Employees in HR, Finance, Records, or IT might click on phishing links, share passwords, or leave their workstations unlocked. Since these users access sensitive data on their department workstations, a single mistake could give an attacker access to ACME's internal network. According to SpringerNature, ***"Human behaviour has emerged as a major vulnerability, frequently exploited in sophisticated cyberattacks like social engineering and phishing,"*** meaning that it

“demonstrates how attackers can bypass advanced technological safeguards by targeting human vulnerabilities.”

Process

For the process, inconsistent security routines create gaps. Suppose ACME doesn’t have a regular schedule for updating policies, reviewing access to systems like the Public Records Server, or removing accounts for employees who leave. In that case, it can leave active accounts or permissions open to attackers' abuse. Another risk involves physical and environmental safety. If there is no straightforward process for checking thermostats, smoke detectors, or sprinklers in areas where network equipment and servers are located, overheating or fire could damage the Internet Router, Main Switch, and departmental switches. That would cause downtime and possibly data loss.

Technology

As for technology, a major issue is poor network segmentation. All department switches—HR, Finance, Records—and the IT Hub connect back to the Main Switch and Internet Router. If VLANs and ACLs are not correctly configured, an attacker who compromises one workstation in HR could move freely to Finance, Records, or even the Web Server and Authentication Server. According to the AlgoSec website, ***“by segmenting a larger network into smaller chunks, it becomes much more manageable to secure the entire network.”*** Another risk is outdated systems and missing patches on servers and workstations. Crowdstrike states, ***“Patch management is the process of identifying and deploying software updates, or “patches,” to a variety of endpoints, including computers, mobile devices, and servers.”*** If ACME’s endpoints and servers are not kept up to date, known vulnerabilities in the operating systems or applications could be exploited by malware or remote attackers.

Adversarial Mindset

People:

To use an adversarial mindset in the people's domain, I imagine how an attacker would try to exploit ACME's employees through both social engineering and physical access. For example, an attacker would likely target HR, Finance, or Records staff with phishing emails, fake login pages, or phone call scams to trick them into revealing credentials or clicking malicious links. They might also try tailgating through the front door or following someone into the IT closet where the core equipment is kept. Thinking this helps reveal weaknesses such as poor security awareness, unlocked workstations, and inconsistent badge use, showing exactly where people-based vulnerabilities exist.

Process:

For process domain, I think about how an attacker would take advantage of ACME's weak or inconsistent procedures. If things like account removal, policy updates, or system maintenance aren't done regularly, an attacker would see that as an easy opening. Attackers might try using old credentials that haven't been disabled or targeting systems that haven't been patched because the update process isn't well-managed. By looking at ACME's processes the way an attacker would, it becomes easier to spot where unclear steps or missing routines could turn into real security risks.

Technology:

For **technology**, I would first look at ACME's network the way an attacker would, identifying the easiest technical entry points. I think about weak spots like outdated systems, missing patches, open ports, or poorly configured devices such as the Main Switch or departmental workstations. An attacker would scan the network, look for unsecured traffic between VLANs, or target servers like the Web Server or Authentication Server that might not be fully locked down. Seeing the environment through that helps reveal where technical gaps exist and how they could be exploited if ACME doesn't strengthen those areas.

Infrastructure Diagram:

People:

My diagram shows RFID readers at the front door and in the IT closets to ensure only authorized personnel can enter. Security cameras are installed near entry points and equipment areas to monitor who comes in and out. These controls help keep unauthorized people out and add another layer of safety for everyone inside.

Process:

For the process, thermostats, smoke detectors, and sprinklers are installed throughout the building to prevent systems from overheating or being damaged. Emergency sirens are also set up in both hallways to quickly alert everyone to an issue so people can evacuate safely. These controls help ACME stay safe and avoid downtime during emergencies.

Technology:

For Technology, my diagram includes stronger network segmentation and traffic control. I implemented VLANs on the Main Switch to separate HR, Finance, Records, and IT, and I configured ACLs to limit which VLANs can reach critical servers like the Web Server, Public Records Server, and Authentication Server. I also assume that endpoints and servers are regularly updated to reduce known vulnerabilities. These changes help prevent lateral movement and make it harder for attackers to use one compromised device to reach the rest of the network.

Organizational Protection:

People:

For my implemented controls, the RFID readers and security cameras protect ACME by controlling and monitoring access to sensitive areas. Only employees with valid badges can open the front door or IT closets, reducing the risk of unauthorized individuals or staff physically accessing routers, switches, and servers. Cameras are used to record who accesses these areas and when, discouraging insider threats and creating investigations if something happens. Together, these controls protect ACME's physical assets and enhance the network's overall security.

Process:

For process, Thermostats, smoke detectors, sprinklers, and sirens help prevent damage or downtime. If there is heat, smoke, or fire, these monitoring devices act fast to keep people and data safe. They ensure operations continue and protect equipment from loss or destruction during emergencies.

Technology:

On the technology side, VLANs and ACLs protect ACME's assets by limiting traffic flow between each department and servers. If an attacker compromises a workstation in the HR VLAN, ACLs make it much harder for them to reach Finance, Records, or the IT administration systems. Proper router configuration shapes internal and external IP traffic so that only necessary connections from the internet reach the Web Server or other public-facing services. Regular updates and endpoint protection on devices further reduce the chance that malware or known exploits can take over servers and workstations.

Balancing Controls:

When it comes to balancing, controls mean keeping ACME secure without making things more complicated for employees or wasting money on tools the company doesn't really need. Simple fixes like training employees, using strong passwords, and keeping systems up to date and patched go a long way without slowing anyone down. Significant changes, such as adding new equipment or implementing stricter access rules, require more planning but can affect how people work. Finding the right balance can help ACME stay protected while keeping things practical and running smoothly every day.

References

Khadka, K., & Ullah, A. B. (2025). ***Human factors in cybersecurity: An interdisciplinary review and framework proposal.*** **Information and Computer Security. https://link.springer.com/article/10.1007/s10207-025-01032-0**

AlgoSec. (2023, August 9). ***Network segmentation vs. VLAN explained.*** **https://www.algosec.com/blog/network-segmentation-vs-vlan**

Roeckl, A. (2024, February 27). ***What is Patch Management?*****. CrowdStrike. https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/patch-management/**