**VxLEARN Networks**

Networking & Cybersecurity Track
Simulated Employment Program

# Lab Report:
# Recommend Threat Mitigation Measures

Prepared by:
Kudzaishe Majeza
Junior Network Engineer – VxLEARN Networks

Mentor:
Titus Majeza
Senior Network Engineer

Date: 16 January 2026

## Table of Contents

## Objectives

The purpose of this lab is to analyze two cybersecurity incident scenarios and recommend practical threat mitigation measures that could have prevented or reduced the impact of each incident. Additionally, research current cybersecurity threats to small and medium-sized businesses (SMBs) and recommend mitigation strategies for the top threats.

## Part 1: Incident at All Time Video Inc. (Video Production Company)

### Step 1: Analyze the Attack

**Conditions that led to the incident:**

1. **Use of infected removable media:** Malware was introduced into the network from free USB drives obtained at a trade fair.
2. **Lack of malware defenses on endpoints:** Malware was able to infect multiple hosts without being detected.
3. **Unpatched software:** Content management servers were running outdated software with known vulnerabilities, which the malware exploited.
4. **Exfiltration via covert channel:** DNS tunneling was used to bypass detection and send large amounts of data out over months.

## Step 2: Recommend Mitigation Techniques

| **Event in Incident** | **Mitigation Measures** |
|---|---|
| Infection via USB drives | • Implement a USB usage policy (disable or restrict USB ports).<br>• Use endpoint malware protection with removable media scanning.<br>• User training on safe handling of external media. |
| Malware spread across network | • Deploy endpoint detection and response (EDR) systems.<br>• Apply network segmentation to limit lateral movement.<br>• Use host-based firewalls and intrusion detection systems (IDS). |
| Exploitation of unpatched CMS software | • Implement regular patch management and vulnerability scanning.<br>• Maintain an up-to-date inventory of software and versions.<br>• Use automated update services where possible. |
| Data exfiltration via DNS tunneling | • Monitor and filter unusual DNS traffic.<br>• Use DNS security solutions to detect and block tunneling behavior.<br>• Implement Data Loss Prevention (DLP) controls. |

## Part 2: Incident at Retail Company

### Step 1: Analyze the Attack

**Steps in the attack:**

1. Threat actors exploited weak security at supplier's network access point.
2. The attackers gained network entry through compromised supplier infrastructure.
3. From that point, attackers located and accessed the customer payment server.
4. They used weak credentials (weak password) to access the database.
5. Sensitive customer data was copied and subsequently uploaded to public hacker servers.

| **Event in Incident** | **Mitigation Measures** |
|---|---|
| Weak security at supplier connection | • Enforce strict vendor security agreements with minimum requirements.<br>• Perform security assessments and audits of third-party connections.<br>• Use network segmentation and firewalls between supplier systems and internal assets. |
| Attackers gaining entry | • Implement Zero Trust principles (verify all devices/users before access).<br>• Use VPNs or secure tunnels with strong authentication.<br>• Monitor and log all third-party traffic. |

| | |
|---|---|
| Weak password compromise | • Deploy strong password policies and enforce complexity.<br>• Implement multi-factor authentication (MFA).<br>• Use account lockout policies after failed login attempts. |
| Sensitive file not protected | • Encrypt customer database data at rest and in transit.<br>• Restrict database access to the minimum necessary users (least privilege).<br>• Perform regular security configuration reviews and audits. |

## Reflection

### 1. Resources Used from the Web

I researched the latest cybersecurity threat reports and mitigation techniques from reputable cybersecurity organizations. These resources helped identify common threats and effective mitigation practices, such as MFA, employee training, network segmentation, regular patching, and monitoring.

## 2. Top 5 Cybersecurity Threats & Mitigation for SMBs

**a. URL of Source Used:**
https://www.jpert.com/blog-resources/top-cybersecurity-threats-small-medium-businesses-face

**b. Organization Name:** JPert
**c. Nature of Organization:** Cybersecurity awareness and educational resource provider that publishes research and insights on security trends.

Threat Table

| **Threat** | **Mitigation Recommendation** |
|---|---|
| Ransomware / Ransomware-as-a-Service | • Regular encrypted backups off the network.<br>• Endpoint detection & response (EDR).<br>• Keep systems patched |
| Phishing & AI-enhanced social engineering | • Employee awareness training.<br>• Email filters and threat detection.<br>• MFA. |
| Business Email Compromise (BEC) | • Strong email authentication (DMARC, SPF).<br>• Avoid shared credentials.<br>• Enable MFA. |
| Supply Chain Attacks | • Security assessments of vendors.<br>• Network segmentation.<br>• Continuous monitoring of third-party access. |
| AI-Driven Malware & Deepfake Attacks | • User training about deepfakes/phishing.<br>• Advanced threat detection tools.<br>• Zero Trust access model. |

## Conclusion

This lab illustrated how multi-layered defenses including strong policies, regular patching, network monitoring, and user education are essential to mitigating modern cyber threats. Proactive measures reduce risk by limiting entry points and exposure to attackers.