

## Module 3 Project: Cybersecurity Threat Analysis Report

### Introduction:

TechEase Solutions is a small IT support provider serving local businesses with network configuration, software installation, and troubleshooting services. The company often manages sensitive client information, including access credentials and system logs. Despite steady growth, cybersecurity practices have lagged behind operational needs.

The company operates in a hybrid environment with both on-premises servers and cloud-based platforms such as Microsoft 365. Employees frequently work remotely using personal devices without oversight or security policies, while the office network is protected only by a basic router. Guest Wi-Fi is shared with employees, remote access tools are unvetted, and no incident response or backup recovery plans are in place.

The purpose of this report is to evaluate TechEase Solutions' cybersecurity posture, identify key threats and vulnerabilities, assess associated risks, and provide tailored recommendations. The analysis focuses on three critical areas: phishing attacks, identity and access management (IAM) gaps, and vulnerabilities introduced by remote work.

### Executive Summary:

TechEase Solutions faces significant cybersecurity risks that threaten both its business continuity and its reputation. The company's exposure is heightened by weak network security, the absence of endpoint protection, a lack of employee training, and inadequate risk management strategies.

### Key Findings:

- High-risk phishing: Employees have already clicked on a suspicious email
- Weak Identity controls: No MFA or password security policies
- Endpoint vulnerabilities: Personal devices lack standardized protection
- Network risks: Shared Wi-Fi and an unsecured router invite exploitation
- Operational gaps: No backup or incident response plans

### Recommendations:

1. Implement MFA and enforce strong password policies
2. Deploy endpoint protection and device compliance requirements
3. Provide regular employee security awareness training
4. Segment guests and corporate networks
5. Establish a backup and an incident response protocol

By implementing these recommendations, TechEase Solutions can reduce its exposure to ransomware, phishing, insider threats, and other common cyber risks while strengthening resilience against future threats.

### **Treat Landscape Overview:**

Small businesses like TechEase Solutions are prime targets because they manage sensitive client data but often lack dedicated security resources. Current threats include:

- **Ransomware:** Criminal groups encrypt businesses and demand payment for restoration. According to CISA, ransomware attacks against small U.S. businesses increased sharply in 2024, leaving many unable to recover due to a lack of backups.
- **Phishing:** Email scams remain the most common entry point. Credential-harvesting attacks frequently target Microsoft 365 users, exposing accounts and sensitive data.
- **Insider Threats:** Employees may act maliciously or negligently. Negligence--such as clicking a link or mishandling client data--can be just as damaging as deliberate sabotage.

TechEase Solutions' limited controls make it especially vulnerable to phishing and ransomware, while insider negligence represents a credible ongoing risk.

### **Cybersecurity Domains Analysis:**

1. Network Security
  - a. **Current State:** Guest Wi-Fi is shared with employees, and the router is minimally secured.
  - b. **Impact:** provides attackers with an easy entry point into internal systems.
  - c. **Recommendations:** Segment guests and corporate networks, deploy a firewall, and implement WPA3 encryption
2. Endpoint security
  - a. **Current State:** Employees rely on personal devices without standards
  - b. **Impact:** Malware or unpatched vulnerabilities could compromise client systems.
  - c. **Recommendations:** require antivirus/EDR solutions, enforce updates, and mandate device compliance.
3. Application Security
  - a. **Current State:** Third-party remote access tools are unvetted and inconsistently updated
  - b. **Impact:** Tools could contain vulnerabilities that allow unauthorized access
  - c. **Recommendations:** Approve secure remote access solutions, enforce patches, and monitor usage.
4. Identity and Access Management (IAM)
  - a. **Current State:** Minimal Password practices and no MFA
  - b. **Impact:** increases the likelihood of unauthorized account access through phishing or brute force

- c. Recommendations: Implement MFA, enforce strong password policies, and apply least-privilege access.
5. Risk Management
  - a. Current State: No structured approach to risk assessment, backups, or incident response
  - b. Impact: The company cannot recover efficiently after an attack.
  - c. Recommendations: Establish a risk matrix, conduct regular assessments, and develop backup/incident response plans.

**Threat Actor Profiles:**

1. Cybercriminals
  - a. Motive: Financial gain
  - b. Methods: Phishing, ransomware, and credential theft
  - c. Impact: Client data loss, financial damage, reputational harm.
2. Insider Threats
  - a. Motive: negligence, carelessness, or personal grievances
  - b. Methods: Mishandling of data, unauthorized sharing, or misuse of privileged access.
  - c. Impact: Unintentional leaks or deliberate compromise of sensitive client systems
3. Hacktivists
  - a. Motive: Political or social activism
  - b. Methods: Website defacement, denial-of-service attacks
  - c. Impact: Service disruption and reputational damage

**Risk Analysis:**

High-Priority Risks:

- Phishing emails leading to stolen credentials and ransomware infections.
- Personal devices introducing malware into client environments
- Unsecured Wi-Fi enables unauthorized access.

Risk Matrix Summary:

- Critical (16-20): Phishing → credential theft and ransomware
- High (11-15): Malware via personal devices, unvetted remote access tools.
- Moderate (6-10): Insider negligence, Wi-Fi vulnerabilities
- Low (1-5): Hactivist disruption

**Security Recommendations:**

1. Identity and Access Controls
  - Enforce MFA and complex password requirements
  - Apply least-privileged access across accounts
2. Training and Awareness
  - Conduct quarterly phishing simulations
  - Provide training on secure remote work practices
3. Endpoint Protection
  - Deploy antivirus and EDR to all devices
  - Require device compliance before network access
4. Network Security
  - Implement network segmentation
  - Harden router and firewall configurations
5. Incident Response and Backups
  - Establish offline and cloud-based backups
  - Document a formal incident response playbook

**Lesson Learned:**

This analysis demonstrates that small businesses are vulnerable to the same threats as larger companies but with fewer defenses. Employee awareness, strong IAM, and secured incident response are fundamental to cyber resilience. One of the main challenges is balancing usability with security- especially when employees rely on personal devices.

**Conclusion:**

TechEase Solutions must take immediate steps to strengthen its secure posture. The company can mitigate high-priority risks like phishing and ransomware by implementing IAM controls, enhancing endpoint and network security, and investing in employee training. Establishing a culture of security and preparedness will safeguard sensitive client data, maintain customer trust, and ensure long-term operational stability.