**Project Title: Cybersecurity Threat Landscape Analysis for a Small Business**

**Student: Oluwaseun Akinola**

**Instructor: Ryan Herron**

**Date: 4/18/2025**

**Introduction**

TechEase Solutions is a small but rapidly growing company that provides IT support services, including software installation, network setup, and troubleshooting for local businesses. As the company grew, its cybersecurity measures didn’t keep up, leaving gaps that could be exploited by cyber threats. With a mix of on-site servers and Microsoft 365 cloud tools, TechEase operates in a hybrid environment. Many employees work remotely and often rely on their personal devices, but there aren’t any strong security policies in place to manage that risk.

**The purpose** of this Cybersecurity Threat Analysis and Risk Assessment is to examine vulnerabilities, assess the risks they pose, and recommend practical solutions to protect TechEase’s systems and client information. This report focuses on three main areas of concern: Identity and Access Management (IAM) gaps, phishing risks, and vulnerabilities linked to remote work.

**Executive Summary**

TechEase Solutions is facing some serious cybersecurity challenges. Some of the biggest weaknesses include employees using unsecured personal devices, shared Wi-Fi networks that aren’t properly separated, a lack of phishing awareness, and the use of remote access tools that haven’t been fully vetted for security. Together, these issues leave the company much more vulnerable to ransomware attacks, stolen credentials, and insider threats.

My threat analysis found major risks tied to both the company’s network security and the way employees handle sensitive information. The risk assessment showed that these vulnerabilities need to be addressed right away.

To fix these problems, I recommend strengthening the company’s network defenses, putting device management policies in place, giving employees regular cybersecurity training, and setting up a formal incident response plan.

By taking these steps, TechEase Solutions can significantly lower its cybersecurity risks and better protect both its business operations and its clients' data.

**Threat Landscape Overview**

Small businesses have increasingly become targets for cybercriminals due to often having weaker security systems than larger organizations.

**Common threats include the following:**

Ransomware attacks: Criminals encrypt a company’s data and demand payment for decryption.

Phishing scams: Attackers deceive employees into revealing sensitive information or downloading malware.

Insider threats: Employees, whether malicious or careless, can expose sensitive data.

Supply chain attacks: Vulnerabilities in third-party software or services are exploited to gain access.

**Recent Cyber Incidents:**

In 2021, a ransomware attack against the IT services company CompuCom disrupted its operations for several weeks, resulting in an estimated $20 million in recovery costs (Whittaker, 2021).

The Verizon 2024 Data Breach Investigations Report states that over 80% of breaches at small businesses started with phishing attacks (Verizon, 2024).

In 2023, an insider incident at Tesla involved a former employee stealing confidential data, leading to legal action and highlighting the serious risks posed by insider threats (Statt, 2023).

These examples show that without strong cybersecurity practices, small businesses like TechEase Solutions face significant risks to their operations, reputation, and client trust.

**Key Vulnerabilities and Gaps**:

|  |  |
| --- | --- |
| Vulnerability | Description |
| Unsecured Personal Devices | Employees use personal laptops/phones with no endpoint protection |
| Weak Network Security | Basic router setup; shared employee/guest Wi-Fi increase risks |
| Lack of Security Vetting | Remote access tools are not consistently vetted or updated |
| No Incident Response Plan | No structured plan to respond to or recover from cyber attacks |
| Low Cybersecurity Awareness | Employees lack training and have interacted with phishing emails |

**Cybersecurity Domains and Applications**

|  |  |
| --- | --- |
| Cybersecurity Domain | How It Applies |
| Network Security | Segregate guest and employee Wi-Fi; upgrade router/firewall security |
| Endpoint Security | Enforce antivirus, encryption, MDM on devices |
| Access Management | Implement strong password policies, MFA and role-based access control |
| Risk Management | Conduct regular vulnerability assessment |
| Incident Response | Develop an incident response and disaster recovery plan |

**Likely Threat Actors**

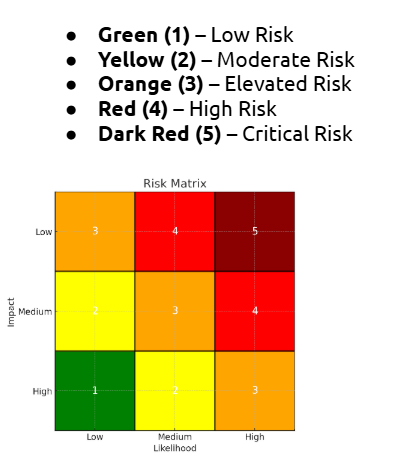
|  |  |  |  |
| --- | --- | --- | --- |
| Threat Actor | Motive | Capability | Potential Impact |
| Cybercriminals | Financial gain (ransomware, data theft) | High | Data loss, ransom demands, reputational damage |
| Insider Threats | Unintentional or malicious actions | Medium | Exposure of sensitive data |
| Hacktivist | Cause disruption for political/social reasons | Medium to Low | Service disruption or data leaks |

**Risk Analysis Table**

**Risk Analysis**

Here is the Risk Matrix categorizing threats by likelihood and impact.

The matrix aligns with the identified risks, providing a visual representation of risk severity using a 5-point color-coded scale:



|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Attack Surface | Vulnerability | Attack Vector | Threat Actor | Risk Statement | Likelihood | Impact | Risk Score | Mitigation Strategy |
| Office Wi-Fi | Shared Wi-Fi network | Unauthorized access | Cybercriminal | Attackers could exploit open network | High | High | Critical | Separate Wi-Fi network, secure with WPA3 encryption |
| Personal Devices | No endpoint protection | Malware infection | Cybercriminal/Insider | Malware on personal devices can spread to company’s data | High | High | Critical | Implement MDM, mandate encryption and antivirus |
| Email Systems | Lack Of phishing training | Phishing attacks | Cybercriminal | Employees may click on malicious links that can spread access to client’s data | High | High | Critical | Provide phishing awareness training and use email filtering tools |
| Remote Access Tools | Not vetted or updated | Remote Exploit | Cybercriminal | Vulnerable third-party tools could allow attackers entry into the company’s network | Moderate | High | High | Standardize and vet remote access tools and update regularly |
| No Incident Response Plan | Lack of preparation | Extended downtime | Cybercriminal/Insider | Failure to respond promptly could worsen damage | Moderate | High | High | Create and practice an incident response plan |

**Recommendations**

Separate Wi-Fi networks: Employee and guest networks must be isolated.

Mandatory device security: Install antivirus, encryption, and MDM for all devices.

Employee cybersecurity training: Regular courses on phishing, safe browsing, and password hygiene.

Remote access policy: Only vetted, updated remote access tools should be allowed.

Incident response plan: Develop, document, and regularly rehearse a full incident response strategy.

Regular risk assessments: Conduct vulnerability scans and risk reviews every 6 months.

**Lessons Learned**

While working on the risk assessment and cybersecurity analysis for TechEase Solutions, I ran into a few challenges that really stood out. One of the biggest was trying to identify risks in a hybrid environment, where personal and company systems overlap. It made it harder than I expected to clearly map out the company's attack surface. Another challenge was the lack of formal cybersecurity policies, which made it tricky to tie certain gaps directly to specific security domains — it took a lot of careful thinking and interpretation.

One key insight I gained from this project is that small businesses often don’t realize how important strong cybersecurity controls are. Many believe they’re too small to be targeted, but in reality, cybercriminals see them as easy opportunities.

Throughout this analysis, I also noticed common risks that kept coming up, like unmanaged personal devices, weak network setups, and a lack of employee training. Even implementing basic cybersecurity practices could make a huge difference for companies like TechEase Solutions.

**Conclusion**

The cybersecurity threat analysis for TechEase Solutions revealed several high-priority vulnerabilities that must be addressed immediately to protect the company’s data and maintain client trust. Risks such as phishing attacks, malware infections on personal devices, and unvetted remote access tools create serious exposure for the business.

Through careful risk assessment, it became clear that small businesses, despite limited resources, must prioritize cybersecurity to remain resilient. Investing in secure network infrastructure, employee training, endpoint protection, and formal incident response planning will significantly reduce TechEase Solutions’ risk profile.

Ultimately, building strong cybersecurity foundations is not just a technical requirement — it is essential for ensuring the long-term survival and success of small businesses in today’s threat landscape.

**Final Thoughts**

Based on everything I found during this project, I believe TechEase Solutions really needs to focus on building a stronger, layered defense strategy that tackles both technical vulnerabilities and human risks.

Some important steps they should take include setting up network segmentation to separate critical systems, putting strict endpoint security measures in place for all employee devices, and using multi-factor authentication (MFA) for anything sensitive, especially remote access tools.

Just as important, I think it’s critical for the company to invest in regular cybersecurity awareness training. Employees need to be able to recognize phishing attempts and other common attacks. Having a formal incident response plan and running regular risk assessments would also help TechEase stay flexible and ready to deal with new threats.

If the company takes these proactive steps, it can move cybersecurity from being just an afterthought to becoming a key part of how they operate — building stronger client trust, keeping their business running smoothly, and protecting their growth in a world where cyber threats are always evolving.

**References:**

Ponemon Institute. (2023). 2023 Cost of Insider Threats Global Report. Ponemon Institute. <https://www.proofpoint.com/us/resources/threat-reports/ponemon-2023-cost-insider-threats>

U.S. Small Business Administration. (2023). Cybersecurity for Small Businesses. <https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats>

Verizon. (2024). 2024 Data Breach Investigations Report. Verizon Enterprise Solutions. <https://www.verizon.com/business/resources/reports/dbir/>

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

National Institute of Standards and Technology. (2022). Small Business Cybersecurity Corner. <https://www.nist.gov/itl/smallbusinesscyber>

Statt, N. (2023, August 21). Tesla sues former employee for insider data theft. The Verge. <https://www.theverge.com/2023/8/21/23840863/tesla-insider-breach-data-lawsuit>

Whittaker, Z. (2021, March 4). IT giant CompuCom hit by ransomware attack. TechCrunch. <https://techcrunch.com/2021/03/04/compucom-ransomware-attack/>

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |