Fictional Business: TechEase Solutions

Industry: Small IT Support Company

Size: 15 employees

Business Type: Provides IT support and troubleshooting services to small businesses.

IT Infrastructure:

Asset	Description
Website	Clients submit IT support tickets via an online portal.
Database Server	Stores client information and support request logs.
Employee Workstations	Employees use Windows computers to handle support tickets.
Firewall & Network	Basic router and firewall protecting the internal network.
Email System	Employees use company email for communication with clients.

Security Concerns:

- **Weak passwords** used by employees.
- **Unpatched software** on employee computers.
- **Potential phishing attacks** targeting employees via email.
- **Exposed database vulnerabilities** that may leak client data.

TechEase Solutions

Introduction

The purpose of this cybersecurity audit is to assess the current security posture of **TechEase Solutions**, a small IT support company, and identify potential risks and vulnerabilities within its IT infrastructure. This audit covers critical assets such as the company website, database server, employee workstations, network, firewall, and email systems. By conducting a thorough risk assessment, identifying threats, and evaluating existing security controls, this audit aims to recommend effective mitigation strategies that will enhance the company's security, ensure regulatory compliance, and protect sensitive client data. The audit's goals are to provide clear, actionable recommendations to strengthen TechEase Solutions' cybersecurity measures and to maintain a secure and resilient operational environment.

Scope and goal of the audit

Scope: The scope of this audit is defined as the entire security program at TechEase Solutions. This includes their assets like website, database server, employee workstations, firewall and network, etc. I will need to review the assets TechEase Solutions has and the controls and compliance practices they have in place.

Goals: Assess existing assets and complete the controls and compliance checklist to determine which controls and compliance best practices need to be implemented to improve TechEase Solutions' security posture.

Risk Assessment

1. Identifying Assets:

TechEase Solutions, a small IT support company, relies on several critical IT assets:

- **Website**: Used for client support ticket submissions.
- **Database Server**: Stores client data and support history.
- **Employee Workstations**: Windows-based computers used for client interactions.
- **Network & Firewall**: Protects internal systems from external threats.
- **Email System**: Used by employees for client communication.

2. Identifying threats and vulnerabilities:

Several security threats exist that could impact the business. The key threats and vulnerabilities include:

- **Phishing Attacks**: Employees may fall for malicious emails, leading to data breaches or malware infections.
- **Weak Passwords**: Employees might use easily guessed or reused passwords, making systems vulnerable to unauthorized access.
- **Malware Attacks**: Workstations without proper antivirus protection could be compromised, leading to data loss or system downtime.
- **Unpatched Systems**: If software updates are not applied regularly, attackers could exploit known vulnerabilities.

3. Assess impact and likelihood:

Each identified threat is evaluated based on its potential impact and likelihood:

- **Phishing Attacks**: High impact and high likelihood. A successful attack could lead to data breaches, financial losses, and reputational damage.
- **Weak Passwords**: Medium impact and high likelihood. Unauthorized access could result in data leaks and account takeovers.
- **Malware Attacks**: High impact and medium likelihood. Malware could lead to system downtime and financial losses.
- **Unpatched Systems**: Medium impact and medium likelihood. Exploited vulnerabilities could disrupt business operations.

4. Risk Score:

Each risk is scored based on **impact (1-5)** and **likelihood (1-5)**. The final risk score is calculated as **Impact × Likelihood**.

- **Phishing Attacks**: 25 (**Critical**)
- **Weak Passwords**: 16 (**High**)
- **Malware Attacks**: 15 (**High**)
- **Unpatched Systems**: 9 (**Moderate**)

5. Recommended Security Controls:

To mitigate the identified risks, the following security measures should be implemented:

- **Phishing Awareness Training**: Educate employees on identifying phishing emails and enforce email filtering to reduce spam and malicious messages.
- **Strong Password Policies**: Require employees to use complex passwords and enable multi-factor authentication (MFA) for all critical systems.
- **Malware Protection**: Install and regularly update antivirus software on all employee workstations.
- **Regular Patching and Updates**: Implement a patch management strategy to ensure all systems and applications receive timely security updates.

Additional comments

The most critical risks for TechEase Solutions are **phishing attacks**, followed by **weak passwords and malware threats**. By implementing the recommended security controls, the company can significantly reduce its exposure to cyber threats and improve overall security.

Control best practices

The first function of the **NIST Cybersecurity Framework (CSF)** is **Identify**. TechEase Solutions must dedicate resources to identifying and managing critical assets to ensure business continuity. This includes classifying existing assets, assessing their importance, and evaluating the potential impact of asset loss on operations. By maintaining an up-to-date asset inventory and risk assessment process, the company can implement effective security controls to mitigate threats proactively.

Compliance considerations

To ensure regulatory adherence, TechEase Solutions must comply with relevant **cybersecurity laws, industry standards, and best practices**. This includes frameworks like **NIST CSF, ISO 27001, and CIS Controls**, which provide structured guidelines for securing IT systems. Additionally, if handling customer data, compliance with **privacy regulations such as GDPR, PIPEDA, or CCPA** is crucial. Regular **compliance audits, policy reviews, and employee training** will help maintain adherence to these standards. By integrating compliance into security operations, the company can **reduce legal risks, enhance customer trust, and improve overall cybersecurity resilience**.

Evaluation of Existing Security Controls

Before implementing new mitigation measures, TechEase Solutions must evaluate its **current security controls** to identify strengths and gaps. This includes reviewing **existing policies, network configurations, and security tools** to assess their effectiveness against identified threats. Regular **security audits, vulnerability scans, and penetration tests** should be conducted to measure the resilience of current defenses. Additionally, monitoring **incident response logs and employee security practices** will help determine whether existing controls are being followed. If weaknesses are found, adjustments should be made to **enhance security policies, improve user training, and upgrade outdated technologies**.

Detailed Mitigation Plan

This mitigation plan outlines security measures to reduce the risks identified in the risk assessment. The goal is to **strengthen TechEase Solutions' cybersecurity posture** by addressing vulnerabilities and implementing best practices.

Phishing Attacks (Critical – Score: 25)

Mitigation Measures:

- Conduct **mandatory phishing awareness training** for all employees.
- Implement **email filtering solutions** to block suspicious emails.
- Enable **multi-factor authentication (MFA)** for all business accounts.
- Regularly perform **simulated phishing exercises** to test employee awareness.

Weak Passwords (High – Score: 16)

Mitigation Measures:

- Enforce a **strong password policy** requiring at least 12-character passwords with uppercase, lowercase, numbers, and special characters.
- Implement **multi-factor authentication (MFA)** for critical systems.
- Use a **password manager** to store and generate strong passwords securely.
- Require **password expiration and regular updates** (e.g., every 90 days).

Malware Attacks (High – Score: 15)

Mitigation Measures:

- Install **endpoint protection software** (antivirus, anti-malware) on all workstations.
- Enable **automatic updates** for all security software.

- Restrict **admin privileges** to prevent unauthorized software installation.
- Train employees on **safe browsing and email attachment handling**.

Unpatched Systems (Moderate – Score: 9)

Mitigation Measures:

- Implement a **patch management policy** to ensure all software, operating systems, and firmware are regularly updated.
- Enable **automatic updates** where possible.
- Conduct **regular vulnerability scans** to identify outdated software.
- Assign a **dedicated IT resource** to track security patches.

Conclusion

In conclusion, the audit of **TechEase Solutions** has identified several critical risks, including phishing attacks, weak passwords, malware threats, and unpatched systems. These risks pose significant threats to the company's cybersecurity resilience and can lead to data breaches, system downtime, and financial losses. By implementing the recommended security controls, such as phishing awareness training, strong password policies, endpoint protection, and regular patching, TechEase Solutions can significantly reduce its exposure to cyber threats. Furthermore, aligning with industry standards and maintaining compliance with relevant regulations will ensure that the company remains secure, trusted, and resilient. Ongoing evaluation and improvement of security measures will be essential to adapt to emerging threats and maintain a robust defense system.