Cybersecurity Awareness & Security Hardening Project

Overview

This project focused on assessing common cybersecurity risks within a small-to-medium business environment and developing a comprehensive set of best practices, standard operating procedures (SOPs), and software recommendations. The assessment identified several high-risk areas—including weak passwords, phishing exposure, unsecured devices, improper data handling, remote-work vulnerabilities, and delayed incident reporting. I conducted research, analyzed real-world attack patterns, and created a structured security improvement plan designed to strengthen organizational resilience.

Objectives

- **Identify critical security gaps across user behavior, devices, and networks**
- **Develop clear best practices and SOPs for employees**
- **Recommend effective security tools for password management, endpoint protection, and training**
- **Improve overall cybersecurity posture through awareness and policy enforcement**

Findings

The assessment revealed that many common threats stem from human error, weak authentication practices, and insufficient device/network protections. Key risks included:

- **Weak or reused passwords**, increasing the likelihood of unauthorized access
- **High susceptibility to phishing attacks**, which could lead to credential theft or malware infections
- **Unsecured devices and networks**, especially in remote-work environments
- **Improper handling of sensitive data**, risking compliance violations
- **Delayed incident reporting**, allowing threats to spread
- **Lack of ongoing cybersecurity training**, leaving employees unprepared for evolving threats

These gaps significantly increase the risk of breaches, data loss, and operational disruption.

Solution

To address these vulnerabilities, I developed a multi-layered security improvement plan. The solution includes best practices, SOPs, and recommended tools across seven key areas:

1. Password Security

- Strong, unique passwords (12+ characters, mixed complexity)
- 90-day rotation policy
- No password sharing
- **Recommended Tools:** Bitwarden, 1Password, Microsoft Authenticator

Phishing Awareness

- Verification of sender identity
- Hover-to-inspect link behavior
- Avoiding unexpected attachments
- **Recommended Tools:** Proofpoint, Mimecast, KnowBe4

3. Device & Network Security

- Automatic updates enabled
- Antivirus and firewall protection
- VPN usage on untrusted networks
- **Recommended Tools:** CrowdStrike, Sophos, NordLayer

Data Protection & Privacy

- Access only what is required for the role
- Encrypted storage for sensitive files
- Secure file-sharing platforms
- **Recommended Tools:** BitLocker, VeraCrypt, OneDrive Business

5. Remote Work Security

- Company-approved devices
- Secure home Wi-Fi with strong encryption
- VPN for all remote access
- **Recommended Tools:** Intune, TeamViewer, OpenVPN

Incident Reporting

- Immediate reporting of suspicious activity
- Clear documentation of incident details
- No self-remediation without IT guidance
- **Recommended Tools:** Jira Service Management, Slack, Microsoft Teams

7. Ongoing Training & Awareness

- Quarterly cybersecurity training
- Real-world examples and simulations
- Regular updates to training materials
- **Recommended Tools:** KnowBe4, Infosec IQ, TalentLMS

This layered approach ensures protection across people, processes, and technology.

Outcome

The project resulted in a **comprehensive cybersecurity enhancement plan** that organizations can implement immediately. Deliverables included:

- A structured set of best practices and SOPs
- Software recommendations tailored for small-business environments
- A clear explanation of how each measure reduces risk
- A roadmap for ongoing training and policy improvement

Overall, the project significantly strengthens organizational defenses, reduces human-driven vulnerabilities, and promotes a culture of cybersecurity awareness.