Final course project: Security strategy
Introduction

This exercise provides an opportunity to apply your theoretical knowledge in a practical, real-world scenario. By completing this exercise, you will gain hands-on experience in conducting a security analysis, identifying potential threats, assessing their risks, and formulating effective countermeasures.

Scenario

Sam’s Scoops has experienced substantial expansion. Operating across multiple locations, Sam’s Scoops deals with sensitive customer data, including credit card information, addresses, and personal details.

The growing workforce, now over 250 employees, work in diverse departments. An emerging concern is that some of these employees bring their personal computers to the office, potentially introducing new vulnerabilities into the company's network.

Given the rising complexity of cyber threats, Sam’s Scoops is increasingly exposed to potential risks like phishing, ransomware, and DDoS attacks. Furthermore, data breaches are an ever-looming threat that could impact the company's reputation and financial stability.

Objective

Your task is to conduct a comprehensive security analysis and develop a detailed security strategy report for Sam’s Scoops. The strategy should address the evolving threats that the company could encounter and outline suitable solutions for risk mitigation and data protection.

Use the knowledge gained from this course and previous courses to develop this strategy report.

Security Strategy Report for Sam’s Scoops

Introduction

This report presents a comprehensive security strategy for Sam’s Scoops to address the evolving threats in the digital landscape. With the expansion of operations and the increasing complexity of cyber threats, it's imperative for Sam’s Scoops to fortify its security measures to safeguard sensitive customer data and ensure business continuity.

This growth necessitates a robust security strategy to mitigate risks associated with a large workforce and the evolving cyber threat landscape. This report outlines a comprehensive security strategy addressing potential threats, data protection, employee training, and incident response protocols.

Step 2: Identify Potential Threats

Internal Threats:

- *Employee negligence: Accidental data leaks, weak passwords, and lack of cybersecurity awareness can expose data.*
- *Social engineering: Phishing attacks can trick employees into revealing sensitive information or clicking malicious links.*
- *Malware on personal devices: Employees using personal computers with malware can introduce vulnerabilities into the network.*

External Threats:

- *Cyberattacks: Phishing, ransomware, malware attacks, and DDoS attacks can disrupt operations, steal data, or demand ransom.*
- *Data breaches: Hackers can exploit vulnerabilities to gain unauthorized access to customer data.*
- *Zero-day vulnerabilities: Undiscovered software vulnerabilities can be exploited before a patch is available.*

Step 2: Evaluate Risks

Likelihood (Low, Medium, High) and Impact (Low, Medium, High) will be assigned to each threat to determine its overall Risk Level (Low, Medium, High). Here's an example:

Threat	**Likelihood**	**Impact**	**Risk Level**
Phishing attack	High	Medium	High
Malware on personal devices	Medium	Medium	Medium

Step 3: Develop Countermeasures

General Countermeasures:

- *Security awareness training: Train employees on identifying phishing attempts, protecting passwords, and cybersecurity best practices.*
- *Implement endpoint security solutions: Install antivirus, anti-malware, and endpoint detection and response (EDR) software on all devices (company and personal if allowed).*
- *Enforce strong password policies: Require complex passwords with regular changes.*
- *Implement a firewall: Filter incoming and outgoing network traffic.*

Specific Countermeasures:

- *Phishing attacks: Implement email filtering solutions and DMARC to prevent phishing emails from reaching inboxes.*
- *Data breaches: Encrypt sensitive data at rest and in transit.*
- *Zero-day vulnerabilities: Regularly update software and firmware on all devices.*

Step 4: Data Protection Strategy

- *Secure data storage: Store sensitive data on secure servers with encryption.*
- *Data backups: Implement regular backups to a secure offsite location for disaster recovery.*
- *Access controls: Implement access control lists (ACLs) to restrict access to sensitive data based on the principle of least privilege.*
- *Data classification: Classify data based on its sensitivity to determine appropriate security measures.*

Step 5: Phishing Avoidance Strategy

- *Anti-phishing solutions: Implement email filtering solutions that can detect and quarantine phishing emails.*
- *Employee training: Train employees to identify phishing tactics, suspicious email content, and red flags.*
- *Simulated phishing attacks: Conduct regular simulated phishing attacks to assess employee awareness and effectiveness of training.*

Step 6: Personal Device Policy

- *Define acceptable usage: Specify allowed personal device types and activities on the company network.*
- *Require strong passwords and encryption: Mandate strong passwords for personal devices used on the network and require data encryption.*
- *Limit access to sensitive data: Restrict access to sensitive data from personal devices.*
- *Consider Mobile Device Management (MDM): Implement MDM solutions to manage and secure access from mobile devices.*

Step 7: Multi-Factor Authentication (MFA) and Biometrics

- *Implement MFA for all access points to sensitive systems and applications, requiring a secondary verification factor beyond a password.*
- *Consider biometric authentication (fingerprint scanners, facial recognition) for high-security applications.*

Step 8: Incident Response Plan

- *Establish a response team: Identify a team responsible for incident response, with clear roles and responsibilities.*
- *Detection and containment: Define procedures for identifying and containing security breaches to minimize damage.*
- *Investigation and eradication: Develop a process for investigating the source of an incident and eradicating the threat.*
- *Recovery and communication: Establish a plan for restoring systems and data, and communicating effectively with stakeholders during and after an incident.*

Step 9: Continuous Monitoring and Improvement

- *Regularly assess the effectiveness of security measures through penetration testing and vulnerability scans.*
- *Stay updated on emerging threats and adapt security measures accordingly.*
- *Conduct periodic security awareness training to reinforce best practices.*

Conclusion

By implementing this comprehensive security strategy, Sam's Scoops can significantly enhance its cybersecurity posture. A combination of technological solutions, employee training, and well-defined policies creates a layered defense against evolving cyber threats. Regularly monitoring and improving