Cybersecurity

Module 2 Challenge Submission File

Assessing Security Culture

Make a copy of this document to work in, and then answer each question below the prompt. Save and submit this completed file as your Challenge deliverable.

Step 1: Measure and Set Goals

1. Using outside research, indicate the potential security risks of allowing employees to access work information on their personal devices. Identify at least three potential attacks that can be carried out.

```
1)Lost or stolen personal device:
Lost or stolen personal devices may compromise sensitive work information.
An attacker gaining physical access can bypass security, potentially
accessing emails, documents, or corporate resources.
2)insecure WI-Fi network
Employees on insecure Wi-Fi risk data interception. An attacker can set up
fake hotspots, intercepting sensitive information when an employee connects,
compromising login credentials or confidential documents. Insider threats
pose additional risks.
3) Malware and Phishing Attacks:
Personal devices, less secure than corporate ones, face malware and phishing
risks. A phishing email can trick an employee into downloading malware,
capturing credentials or allowing remote access.
```

2. Based on the previous scenario, what is the preferred employee behavior? (For example, if employees were downloading suspicious email attachments, the preferred behavior would be that employees only download attachments from trusted sources.)

Prioritize email vigilance: Avoid clicking on links or downloading attachments from unknown sources. Verify emails with known contacts, promote security awareness, use trusted sources, and ensure regular updates to maintain a secure work environment and prevent security breaches.

3. What methods would you use to measure how often employees are currently *not* behaving according to the preferred behavior? (For example, conduct a survey to see how often people download email attachments from unknown senders.)

Regularly audit employee adherence to security protocols, using automated tools for vulnerability scans. Encourage incident reporting and analyze reports to identify non-compliance patterns. Conduct simulated phishing, administer cybersecurity surveys, and monitor network and device activities. Assess training program effectiveness through completion rates and post-training metrics. Monitor file downloads and access logs to detect unusual behavior, investigating unauthorized access. Conduct interviews or focus groups for qualitative insights into employee cybersecurity behavior and perceptions

4. What is the goal that you would like the organization to reach regarding this behavior? (For example, to have less than 5% of employees downloading suspicious email attachments.)

The goal for the organization should be to achieve a high level of cybersecurity adherence,for a significant reduction in risky behaviors. Employees engaging in unsafe practices, such as clicking on suspicious email links or downloading attachments from unknown sources. The goal is to minimize the risk of security breaches and protect sensitive information, fostering a secure work environment. Regular monitoring and proactive measures should be implemented to ensure continuous improvement toward this goal and enhance overall security.

Step 2: Involve the Right People

5. List at least five employees or departments that should be involved. For each person or department, describe in 2–3 sentences what their role and responsibilities will be.

Cybersecurity depends on collaboration among departments and individuals. include the Chief Information Security Officer (CISO), Network Security Team, IT Department, HR, and all employees, actively contributing to a robust defense. This involves heightened awareness, strong practices, and a commitment to promptly report potential threats. Each element works together to fortify the organization, ensuring a comprehensive defense against evolving cyber threats.

The CISO is responsible for overseeing the entire cybersecurity strategy. They develop and implement policies, procedures, and guidelines.

Network Security Team,this team focuses on securing the organization's network infrastructure. Responsibilities include configuring firewalls, monitoring network traffic for anomalies.

The IT department is vital for implementing and maintaining security measures on user devices and servers.

The HR Department is involved in the cybersecurity process by managing employee onboarding and offboarding training.

Every employee is accountable for maintaining strong cybersecurity practices. This encompasses creating robust, individual passwords, exercising caution regarding phishing attempts, and immediately reporting any suspicious activity to the IT or cybersecurity team.

Step 3: Training Plan

6. How frequently will you run training? What format will it take (e.g., in-person, online, a combination of both)?

The frequency of cybersecurity training is contingent upon the specific requirements of the organization. Ideally, consistent training sessions that incorporate a mix of in-person and online methods help employees stay informed about emerging threats and any alterations to the company's guidelines and policies.

7. What topics will you cover in your training, and why? (This should be the bulk of the deliverable.)

In cybersecurity training, vital topics include phishing awareness, password and data security, device security, social engineering, incident response, compliance, software updates, secure communication, and physical security. This comprehensive foundation cultivates a resilient, security-conscious organizational culture by enhancing awareness and skills.

Educating employees on recognizing and avoiding phishing attacks, stressing strong password practices, and explaining data protection significance are crucial steps. Furthermore, covering incident response strategies, compliance adherence, and emphasizing the importance of secure communication and physical security contribute to a holistic understanding. Overall, these topics collectively fortify employees against various cyber threats, ensuring a robust defense within the organizational framework.

8. After you’ve run your training, how will you measure its effectiveness?

Training effectiveness involves analyzing phishing simulation results, conducting knowledge assessments, evaluating incident response performance, monitoring security compliance, gathering employee feedback, and tracking security incidents. Combining all their results, organizations can comprehensively assess the impact of cybersecurity training on employee, and the overall security.

Bonus: Other Solutions

9. List at least two other potential solutions. For each one, indicate the following:
   a. What type of control is it? Administrative, technical, or physical?
   b. What goal does this control have? Is it preventive, deterrent, detective, corrective, or compensating?
   c. What is one advantage of each solution?
   d. What is one disadvantage of each solution?

In cybersecurity, controls fall into three categories: administrative, technical, and physical. Administrative controls involve policies and training, technical controls use technology like firewalls, and physical controls include access safeguards. The control's goal aligns with its objective:

Preventive Controls: Stop accidents before they occur, e.g., firewalls.

Deterrent Controls: Discourage attackers, e.g., surveillance cameras.

Detective Controls: Identify incidents, e.g., intrusion detection systems.

Corrective Controls: Mitigate impact post-incident, e.g., patching.

Compensating Controls: Address weaknesses, e.g., additional security measures.

```
Solution 1: Multi-Factor Authentication (MFA)
Technical control.
Preventive. Enhances access control by requiring multiple forms of verification.
Increases the security of user authentication, particularly against unauthorized access due to compromised passwords.
Some users may find it slightly inconvenient, and implementation costs could be a consideration for organizations.
Solution 2: Surveillance Cameras and Access Control Systems
Physical control.
Preventive and deterrent. Monitors and restricts physical access to facilities.
Provides real-time monitoring and acts as a visible deterrent against unauthorized entry.
Limited in addressing virtual threats, and maintenance costs can be significant.
```