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.

There are too many potential security risks of allowing employees to access work information on their personal devices. The most important one is that the organization can’t control and monitor what their employees do with their personal devices. There is always a risk that employees can access public Wi-Fi, download an unsafe app that can compromise corporate data.

Here are some potential attacks:

1) Phishing and social engineering attacks which can lead to data leakage and access to sensitive and confidential information.
2) Malicious apps
3) Infected devices
4) Stolen device (or loss - even if loss is not an attack but it’s a high potential security risk)
5) Shoulder surfing

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.)

1. Employees should be able to recognize phishing emails and avoid clicking on suspicious links and download suspicious attachments.
2. Employees should not connect to public Wi-Fi if they are using personal devices for work-related activities, using work accounts and work-related applications.
3. Employees should increase protection from malware by installing anti-malware on their personal devices.
4. Employees should change their passwords frequently, use a strong password in conjunction with Multi-Factor Authentication.
5. Bea aware of their surrounding when accessing company data in public (avoid shoulder surfing)
6. Use encrypted devices or encrypt data (in case the personal device is stolen or lost).

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.)

1. Test employees (simulate phishing attacks)

Best is to simulate phishing attacks within the company - using software such as phishing simulators that can help to gather more information like open rates, click rates etc and decide which employees require further training.
Also better is to target specific audiences like finance, IT, senior managers or high-level employees.

2. Check company’s security culture (Surveys)
   Check if employees understand common security risks and the security implications of their decisions, how they approach security issues, how employees react when observing and reporting cyber-security incidents.
3. Security teams must test their efficiency as well, through penetration testing, simulating realistic cyber attacks, and other vulnerability assessments.
4. Keep track of all devices connected to the office network, run routine network scans.

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.)

1. Click rate goal of the phishing emails should be under 5%.
2. The number of employees using personal devices (to check their work email and communications via Slack or doing other work-related activities) should be reduced by 50% in the first year. Eventually reduced to a rate of less than 5%.
3. Aim for a 85% employee pass rate in security risk assessments.

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.

In order to establish a strong security risk culture within an organization it's essential to involve diverse individuals and departments:

1. **The chief executive officer (CEO)**
   The CEO is responsible for plotting the overall direction of the company. In this case the CEO allocates resources, integrates security into the business strategy, and reports to the board of directors about what security precautions are put in place.

2. **Chief information security officer (CISO) and Security Team**
   They are responsible for the security program, create, implement and enforce security policies to protect critical data, conduct risk assessments, promote security awareness, and manage security incidents.
   Also, they are responsible for surveys for the assessment of security culture, also conducting quality control for repeat assessment (if necessary).

3. **Chief information officer (CIO)**
   CIO manages an organization’s IT systems, and also reacts to the information security concerns. Also manages network implementations such as scanning the network, updating patches (can execute the technical components of the security strategy).

4. **Department Heads**
   Department heads play a crucial role in promoting a strong cybersecurity culture within an organization. They can help to identify and address security risks within their department. They can improve communication and collaboration between departments on security initiatives. By setting a strong security example, department heads can inspire their teams to take security seriously this leads to a more security-conscious workforce.

5. **Human Resources (HR)**
   HR can integrate and oversee the planning and scheduling of security training sessions, manage training resources, track employee participation and also track completion rates.

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)?

With cyber attacks posing a significant threat to businesses the importance of regular cyber security awareness training is evident.

Training frequency is based on the data we collect from the previous trainings: training effectiveness, evolving threats, results after phishing simulations etc

Security training should be run every 4-6 months, training format can be in-person and online with mandatory attendance (but in-person training is preferred).

To address specific vulnerabilities, targeted security training is recommended for different departments and roles. Regular phishing simulations are recommended too, this will help employees identify and avoid phishing attempts. Employees who fail a simulated test should be encouraged to revisit the security training.

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

Phishing attacks and social engineering - attackers are using this technique to trick employees into compromising sensitive data. Employees need regular training on how to identify phishing attacks as well as how to report it.
Public Wi-Fi - employees should be aware of how unsafe the public Wi-Fis are, and learn how to use VPN.
Ransomware - employees should be aware that ransomware is one of the most popular threats targeting businesses across the world.
Removable media - employees should be aware of how quickly plugging an USB into a computer system can impact security, and how to protect sensitive information when using removable media.
Passwords and authentication - Employees should learn why having a strong password is important, how to keep it safe and also learn about multi-factor authentication.
Physical security - keeping sensitive physical documents secured is vital to the integrity of a company's security system. Also, employees should learn about tailgating.
Mobile device security - Mobile phones are becoming a popular target for cyber crimes, that's why employees should learn what is acceptable use of personal mobile devices for work related tasks.
Working remotely and security at home - While working from home, employees need to become more aware of the potential risks of a cyber attack.
Social Media Use - employees should learn about the risks of social media, share sensitive information through various channels.
Incident reporting - employees should learn to identify and know how to quickly alert security team about potential threats or security gaps.

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

1. **Quizzes** - We will use post-training assessments to evaluate knowledge retention among participants.
2. **Simulate phishing attacks** - simulate phishing attacks to see if employees can avoid malicious emails following security training.
3. **Ask Employee's Feedback** - Surveys can help us understand if the training was engaging, relevant, and easy to understand.
4. **Monitor employees behavior** regarding security protocols like password complexity or data handling procedures after training.
5. **Track reported security incidents** like phishing attempts, malware infections etc. A decline might indicate improved awareness.

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?

```
identification and authentication mechanisms
```

```
biometric access control systems
```

a) What type of control is it? Administrative, technical, or physical?
   - identification and authentication mechanisms is a technical control
   - biometric access control systems is a physical control

b) What goal does this control have? Is it preventive, deterrent, detective, corrective, or compensating?
   - **identification and authentication mechanism** is a preventive control, these mechanisms act as a barrier to entry, preventing unauthorized individuals or devices from gaining access.
   - **biometric access control system** is a preventive control, act as a barrier to entry, using unique biological characteristics of a person (fingerprints, iris scans etc) for identification and authentication.

c) What is one advantage of each solution?
   - **identification and authentication mechanism -** enhance security by minimizing the risk of unauthorized access to sensitive information
   - **biometric access control system** - significantly reduces the risk of unauthorized access compared to traditional methods like passwords or keycards, which can be stolen or shared.

d) What is one disadvantage of each solution?
   - **identification and authentication mechanism -** some methods, like multi-factor authentication, can add extra steps to the login process, potentially impacting user experience.

- `biometric access control system` - Implementation and maintenance of biometric systems can be expensive.