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 four main attack types; User Attacks, Web Attacks, Server Attacks and Database Attacks. Some are outlined below.

1. **Person-In-The-Middle Attack:** If the employee uses public WIFI or an unsecured network to access the resources, this could be left open to packet sniffing, or a person-in-the-middle attack. With employees using personal devices at work, this could make it easy for data to be misplaced, accidentally shared, or even intercepted.

2. **Malware Attack:** If employees do not adhere to the company security standards, or worse, are not aware of such security controls, they are more likely to be exposed to a malware attack. Infections may come from downloaded material from untrusted sources and unsafe websites. Once a BYOD is infected, it can spread throughout the company network (including but not limited to cloud services and emails) when the employee connects to it.

3. **Phishing Attack:** As mentioned in the malware attack section, if employees are not adhering to security standards set by the company, or are not aware of such controls, they may be susceptible to phishing attacks. Being on their own device means they may not be as vigilant when looking at emails or messages, as they would be on company devices. Especially if the employee's work and personal email address are the same.

4. **Social Engineering Attack:** This type of attack uses human interaction and manipulation to gather sensitive information. A threat actor can ask users for their credentials by pretending to be an administrator. Usually they will disguise themselves and their motives by acting as trusted people.

5. **Physical Attack:** An attacker could simply steal an employee's device and login using the saved credentials. This could happen away from the company site, or even through tailgating to gain unauthorized access to the company building.

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.)

Based on the previous scenarios, we would like to see the employees being trained in best practice cybersecurity standards.
This would include, but not limited to;

- Downloading content from trusted sources.
- Not opening emails and attachments from unknown sources.
- Secure internet connection to company resources. Private connection when onsite, and through VPN when remote access is required.
- Having separate work and personal email addresses. The company could set up their own domain name.
- Data encryption.
- Regular backups, updates, and security scans on devices.
- Creating stronger and individual passwords.
- Setup multi-factor authentication (MFA or 2FA).
- Ignore any requests for passwords or financial information.
- Be vigilant of tailgating when accessing areas at work.

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.)

```
- A survey or questionnaire would be an obvious starting point. The quiz can include how often they receive emails from unknown senders, and can test the employee's knowledge on cybersecurity.
- Hire a penetration testing (pentest) third party to send out a phishing email to the employees with the options of reading it or reporting it.
- Data monitoring and network traffic analysis.
```

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.)

```
I would like to quantify the click-through rate. That is, the percentage of employees that download the malicious attachment. The end goal would be to decrease this number to less than 5%.
```

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.

```
1. CEO (Chief Executive Officer): oversees the whole company, the ultimate decision maker. Reports to the board of directors. Responsible for allocating resources across the various departments. They will need to approve the training plan.

2. CIO (Chief Information Officer): reporting to the CEO, they develop the systems that support the company. They take the lead in ensuring the security of the company. They will help the IT team and other departments understand and combat threats.

3. CISO (Chief Information Security Officer): manages risk to company data throughout its lifecycle. Will implement and oversee the
```

company's security program. They will give reason as to why the employees need the training.

4. **COO (Chief Operating Officer):** oversees the day-to-day operations of the company. Reports to the CEO. Their role is to proactively implement measures to reduce risk, ensuring business continuity and stability. They will justify the need for training as well.

5. **HR (Human Resources):** oversees the hiring and admin of employees. They get involved in enforcing policies and maintain compliance while protecting the company and the employees. Their role is to support and discipline the employees when required. They will advise of the best dates to run the training and the pentests.

6. **SOC (Security Operations Centre) or IR (Incident Response):** manage incident response, is made up of analysts and handlers. This department is necessary in activating the response plan after a breach.

7. **Training Department:** create, implement and monitor the training of the employees. They will build awareness among the employees of how and when to escalate all security-based issues or incidents.

8. **Network Security Team:** in charge of networks, consists of system and network administrators, physical technicians, and may also monitor and manage the help desk. Their responsibility will be to monitor the training and report the results.

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)?

Initially the training will be provided online via email yearly, with smaller modules released quarterly. New team members will do the training with their induction training. Team members that do not pass the training, or record a breach (fail pentest, lose a device) will be enrolled in a supplement training session, that is run quarterly in-person.

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

The training will cover best practices in cybersecurity and the importance of being always vigilant. Specifically covering GRC (Governance, Risk Management, and Compliance), importance of cybersecurity, the different types of attacks, what to look for, and how best to mitigate each threat. The training will include real world scenarios and attacks, along with the response to the incident. By providing these examples in the training, the employees will gain a greater understanding of what could happen and the impact on themselves and the company.

Training will include some categories as outline below;

- **GRC and the employee's role for each aspect.** This will ensure there are clear rules (Governance), identification of threats and how to mitigate these (Risk Management), whilst maintaining regulations and standards (Compliance).
- **Importance of cybersecurity and a great security culture.** Having a team of employees with a cyber-savvy mindset promotes a positive security culture, which in turn will build employee's pride and improve a company's reputation with customers.
- **Roles and responsibilities of departments and employees.** This provides the company's hierarchical structure, who does what and when, which promotes stability and confidence in the team.
- **Types of attacks and how to mitigate them.** This training will identify different threats, and give employees the who, what, when, where and why of cybersecurity. Demonstrates to the employees what to look out for. By educating the team about potential threats and how to recognize them, the company can significantly reduce the likelihood of successful attacks.
- **Appropriate security controls.** Awareness training with the team will minimize the risks stemming from the human element.
- **Reporting an incident.** The team will understand the correct process to report an incident and what happens after an incident has been reported.
- **What happens after a breach.** The team will understand the process the company takes after a breach so that there is no uncertainty amongst the employees.

By going through these sections, the employee will have a full understanding of cybersecurity, and everyone will be on the same page, striving for a positive security culture.

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

```
There are two things we can do to measure the effectiveness.

Firstly, we will send out an email survey to the employees, which will ask
them what they should and shouldn't do with their personal devices. Based on
this feedback we will get an idea of where the employee's security mindset
is.

Secondly, we will have the pentest third party run another phishing
campaign. Will then compare the results from this test to the previous
tests. If the results of this new test have a click-through rate lower than
5%, then we can deem the training has been a success and is effective.
If the result is greater than 5%, then the training has not been effective,
and we will need the Security Framework Team to debrief, to understand what
worked well during the planning and implementation of the training package,
and what didn't work well. Perhaps come up with a new test and reimplement.
```

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?

```
The company can put turnstiles in at the entrance to prevent tailgating.
   a. This is a physical control.
   b. The goal of this control is to stop tailgating. This is a preventive
      control.
   c. An advantage of this solution is it only allows one person through at
      a time. It identifies and logs each person entering and exiting the
      building.
   d. A disadvantage is it can create a bottleneck at peak times, causing
      employee frustration. Also, they can be costly to install and
      maintain, using up company resources.
```

```
The company can implement multi-factor authentication (MFA).
   a. This is a technical control.
   b. The goal of this control is to stop credential stuffing. This is a
      preventive control.
   c. An advantage of this solution is it prevents automated login attempts,
      and will drastically slow down credential stuffing.
   d. A disadvantage of this solution is the increase in management
      complexity for the employee and company. It is also not 100%, as other
      attacks can bypass MFA (such as social engineering, phishing and
      malware).
```

References

edX, UWA 2024, Course content, week 2 pdf presentations.

Jones, S, June 2023, *"6 Cybersecurity Risks of Using Personal Devices for Work"*, url < https://teampassword.com/blog/byod-policies-cybersecurity-risks>, accessed Sat 02/03/2024.

Trend Micro, December 2023, "*What is Social Engineering, How it works, How to stay safe"*, url< https://helpcenter.trendmicro.com/en-us/article/tmka-11340#:~:text=yourself%20against%20scams-,How%20Social%20Engineering%20Works,they%20do%20not%20want%20to>, accessed Sat 02/03/2024.