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.

- Company data may be more susceptible to **phishing Attacks**.Companies have less control over what an employee can access on personal devices. If an employee uses their phone to access company data, and becomes the victim to a phishing attack, they have the potential to have their personal data and company data compromised.
- **Malware**, while having the same implications and vulnerabilities as the previous point, is its own separate issue. Whether it's a personal phone or computer, Malware could leak company data if it’s installed onto these devices.
- An **Insider Attack** may be easier for an employee to accomplish on their own device. Something as simple as a screenshot could allow a bad actor to leak sensitive company data for their own gain. Most personal devices, when used in a workplace environment, are not configured to be monitored by the employee’s company. The reduced control and visibility personal devices engender are a serious threat to consider.

2. Based on the previous scenario, what is the preferred employee behavior? (For example, if employees were downloading suspicious email attachments, the

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

preferred behavior would be that employees only download attachments from trusted sources.)

```
As stated in the example above, employees would be less susceptible to
Phishing attempts and Malware if they were to only download and/or click on
links from sources that they trust. However, there are some instances where
social-engineering could trick employees into trusting a malicious source.
As for insider attacks, it may be worthwhile for companies to create a
culture of loyalty and confidentiality to mitigate this threat. It is also
the responsibility of management to monitor employee behavior to mitigate
insider threats.
```

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.)

```
I used to work as a teller in a bank. The method they used to train
employees, and monitor preferred behavior, is applicable to this question.
In the email client that the bank used, they had a button on the GUI where
you could report a suspicious email as phishing. Occasionally, the company
would send me fake phishing emails to see if I would download the
attachments and/or click on the links in these emails. This was not only a
form of training, but it could be used by the company to monitor how likely
employees were to click on a malicious link.
Personally, I would emulate this type of monitoring, as it would show who is
the biggest liability to company data.
```

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 ideal goal would be 0% of employees to download malware and click
phishing links. However, this goal is unrealistic, and does not account for
human error.
Let's say our hypothetical company has 100 employees. A more reasonable goal
of Less Than 7% (of employees trusting malicious sources) would be
attainable. The percentage of employees that trust malicious sources would
fluctuate depending on the company’s size and their goals.
```

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

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.

- Upper-Management
    - Having the highest level of management involved, or conscious, in a security mindset has a trickle-down effect to the rest of the company. If this individual or individuals value Cybersecurity, it will help allocate funding to these aforementioned security projects.
- Enterprise chief security officer
    - Similarly to upper management, having this individual focus on Cybersecurity's best practices affects how the company values and prioritizes securing company data. They direct many different departments, and could help to orchestrate Cyber Security trainings.
- Chief information security officer
    - This individual is more directly involved with Cybersecurity, and the company's data security than the previous two examples. This individual would help create data security standards for the departments under their command. They may also design training programs for the employees within the company.
- IT Security Team
    - Being under the CISO, The IT Team is directly responsible for implementing the plans enacted by the CISO. Monitoring employee activity, following up on security breaches, developing more secured work-portals, etc.
- Average Employee
    - If the average employee is security conscious, the company would be less likely to incur data-breaches. These employees need to be trained on Cybersecurity standards, and need to be comfortable talking about mistakes they make and correct their future actions.

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)?

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

```
This answer depends on the needs, and the situation, of each individual
company. A baseline standard that I would implement would be to email,
monthly, mandatory video-trainings. They could cover a range of best
practices in a short amount of time. A follow-up quiz would help bolster
information retention.
```

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

```
Considering that most (if not all) employees will be using their personal
devices for work-related purposes, it would include short and comprehensive
information on email attacks and malicious links. It would encourage
employees to exercise caution when using their emails or accessing the
internet. I would also make sure that they know the resources they can use
to report suspicious sources, or to receive further information on
data-security.
```

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

```
As previously mentioned, a short quiz will help to ensure information
retention. Also, sending out benign phishing emails to test employees in
their normal work environment.
```

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?

```
Provide Devices for work purposes
   A. Physical & Technical
   B. Preventative and detective
   C. This solution gives much more control to the company for monitoring
      data-access, controlling what the devices can be used for, and even
```

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

allow the company to wipe the device in cases where it is lost or stolen

D. The biggest disadvantage is the expenses that providing devices would incur. It may be in the companies best interest to selectively give out these devices to certain employees.

Ban the use of personal devices for work-related purposes

A. Administrative, Physical, and (possibly) technical.

B. Deterrent and corrective

C. Whether it’s not allowing non-trusted devices to access certain work-related data, or just implementing a culture for management to enforce, this solution helps prevent sensitive data from being accessed on a device that the company has less control over.

D. It may be more costly and less convenient for the company to pursue this option.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.