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.

```
[
   A. Unauthorized access to database- Personal devices used for
      work-related tasks often have a lot of personal and professional data
      (for example, access to systems, networks, and databases). If such
      devices get lost or fall into wrong hands, it can become a significant
      threat for both personal and professional data exposure, leakage, or
      theft.
   B. Malware infections and phishing attacks- Personal devices usually have
      lower levels of security, and are often used outside the business
      secure-network environment. This introduces a risk of being exposed to
      malware infections and phishing attacks, which can compromise
      corporate database and network systems, and most importantly business
      reputation.
   C. System security - Multiple personal devices exploit the system and
      network, and also pose a threat of infecting corporate systems with
      malicious apps installed/available on the devices.
]
```

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.)

```
[
Preferred employee behaviors: while using personal devices, All employee
would:
   A. Use VPN,
   B. Strong password protection - MFA, SSH cryptographic keys
   C. End to End Encryption
]
```

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.)

```
[
The methods to measure the employees non compliances:
   A. CCTV Monitoring
   B. Monitor user activity logs,
   C. Monitor user access management/control,
]
```

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 business goal would be:
   A. To have 100% of employees using VPN
   B. To have 100% of employees using Strong password protection
   C. To have 100% of employees using End to End Data Encryption while on
      and accessing corporate networks.
]
```

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.

```
[
Chief Executive Office
Chief financial officer (financial department)
Chief operating office
Chief information security officer
Chief information officer

]
```

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 training should be run every three months. The training should be
      delivered in a combined mode of online training and face-to-face
      training.
]
```

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

```
[
   -  For improving security culture at SilverCorp, the training mainly
      focuses on the recent security challenges due to personal devices used
      at work. This will outline main challenges that business is currently
      experiencing due to Personal Devices on Network and their possible
      remedies. Finally, the training will provide the awareness as well as
      explicit guidance on the procedure set up to rectify such issues going
      forward. This will in turn, facilitate the implementation process.
]
```

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

```
[
   -  For measuring the effectiveness of the training, the measures of non
      compliances will be reviewed and compared with the previous trend. If
      such a comparative study postulates a positive change in employee
      preferred behavior, then it can be said that the training became
      effective. The rate of effectiveness can be measured on the rate of
      adoption of positive behaviors by employees, for example - after first
      online training, 95% of employees adopted all three preferred
      behaviors, then further 3% increase after second training and finally,
      100% employ follow the security behaviors after third training, or so
      on.

]
```

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?

```
[
- Complete restriction of personal devices at work (need to be kept in a
secure vault) and no remote network access via Personal device (no work from
home)
 - Physical and administrative
 - Preventive
 - No personal devices can be able to access the data and network, hence no
exposure to any risks and vulnerabilities via such devices
 - Extremely difficult to police and uncomfortable for employees to leave
their personal devices out
]
```

```
[
- Provide all the mobile hardwares (Laptops, mobile phones, scanners etc.)
that are built up at company specifications (with all necessary software and
```

```
security tools) to all relevant employees, so that there is no need to use
personal devices at work.
- Physical, Administrative
- Preventive, corrective and compensative
- No need for personal devices at work, all devices were secure - built up
at company specifications, no threats posed to network and database from
such personal devices.
- Cost involved with the procurement and management of such personal
devices.
]
```