| 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.

| Bring-your-own-device (BYOD) delivers a risk of unclear security expectations, compromised data, Unsecure Wi-fi access, and Malware. **Unclear Security Expectations** is the assumption that businesses have no control over the security of inexperienced employees on BYODs. Social Engineering attacks (phishing) target security-unaware employees, ultimately increasing the risk of BYOD attacks. **Compromised Data** occurs when a BYOD of an employee is lost or stolen, providing an opportunity for attackers to gain access to sensitive work information stored on their personal device. Denial of Service attacks adhere to Compromised Data as the BYOD endpoint may be destroyed or permanently damaged resulting in the permanent loss of work information stored on that device. **Unsecure wi-fi** poses an additional risk if BYODs are used by employees. If an employee connects to different networks (work and personal), each with different security settings, the employee introduces a significant threat to inviting snooping and honeypot (Man-in-the-middle) attackers in. Usually public wi-fi’s offer attackers to complete a Man-in-the-middle attack, resulting in an attacker silently capturing data from the employee over the unsecure wi-fi network. Lastly, **Malware** can be intentionally or unintentionally installed on the BYOD device, allowing Trojans, Worms, Ransomware, virus’, etc to attack the network system once the machine or network are at a vulnerable state. |
| --- |

1. 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.)

| Employees of SilverCorp should be discouraged from connecting their BYODs to the SilverCorp internal network and not sign-in to work platforms, like slack, on their personal devices. If employees are required to use their personal phones to complete day-to-day duties, BYODs should be used on their 4G network and secured with necessary Biometrics (fingerprint or FaceID). Additionally, employees of SilverCorp should be encouraged to save work related information into the SilverCorps cloud environment in case anything happens to the BYOD. Slack and any other work related accounts should be set up with Multi-Factor Authentication. |
| --- |

1. 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.)

| In this scenario, I would measure the security awareness of all employees by inviting the affected departments to a **survey**, which evaluates each user’s security levels and practices for using their BYODs. Questions such as “have you connected your devices to the internal work wi-fi before?”, “have you set up Biometrics, passwords, or passcodes on your personal device?” or “have you set up Multi-Factor Identification on your work related platform accounts?”. Based on the results and the backend analytics we can determine which employees/departments have increased risk, and subsequently focus on them first. |
| --- |

1. 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 is to improve BYOD Security competency to 90%. Only the departments reliant on their BYODs (Sales, etc) should be using their BYODs for work related reasons, this should make up the 25%. Other than that, employees should only use their BYODs on 4G for Multi-Factor sign in purposes. |
| --- |

### Step 2: Involve the Right People

1. 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.

| The **Chief Executive Officer (CEO)** will be involved in the research as they solely are responsible for plotting the overall decision to implement the security strategy. The CEO will need to make the executive decision of whether the risk mitigation strategy will go ahead. The **Chief Financial Officer (CFO)** will be involved as they will be the entity in charge of recommending financial decisions to the CEO of SilverCorp. The CFO will be required to ensure that the profitability of the business is not significantly impacted by the risk mitigation strategy. The **Chief Information Security Officer (CISO)** would be involved in the research as they are the executive party which strives to ensure that all systems and networks are secure, and that employee’s of SilverCorp are not left vulnerable. The CISO will be able to recommend necessary decisions to the CEO to fortify the company from employee security unawareness. The **Sales / Marketing department** would be involved as the Sale’s database is full of sensitive sale agreements and contracts. This information is quite valuable to an attacker, and thus BYOD devices will need to be controlled in this space. The same applies to the **Financial department**. The Finance department would be involved as all employees in this department are normally targeted for their valuable sensitive information or for financial gain. Necessary security controls will be needed to improve this department particularly. |
| --- |

### Step 3: Training Plan

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

| Training will be held online using an online module system. This module will be specifically targeted for the Finance and Sales / Marketing employees. Training will be held quarterly. Using the training materials provided in the module, employees will be tasked to successfully pass a BYOD competency quiz. Any unsuccessful quiz attempts will flag the employee as ‘Incompetent’. Any incompetent employee that does not know the necessary BYOD behaviour, will be required to re-complete training so they can re-sit the quiz in order to be ‘Competent’. Any Competent employee will receive a competency badge allowing them to use their BYOD until the next quarter. |
| --- |

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

| The online training platform will include modules focussed on the following. A ‘**Appropriate use of BYOD for Work-Purposes**’ module will predominantly train employees how to appropriately use their BYODs for work related activities only. The ‘**Inappropriate use of BYOD for Work-Purposes**’ will take employees through the inappropriate use of a BYOD in the workplace and the consequences for inappropriate behaviour. This section will speak about not connecting to SilverCorp’s internal wi-fi network (using 4G instead), personal use of BYOD, etc. A ‘**How to Secure your BYOD**’ module will take trainees through practices to secure a BYOD, such as setting up Biometrics, passwords, passcodes, etc. and the risks of using common passphrases. This section will also focus on setting up Multi-Factor Authentication on all work third-party and internal platforms. A ‘**Responses to Irregular Activity on BYOD**’ module will feature in the training which features identifying strange events happening on a BYOD and how to respond to such events appropriately. Lastly the **Competency Quiz** will evaluate whether the training was successful for an employee. |
| --- |

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

| After the training I will measure its effectiveness by sending out **quarterly Competency Quizzes** and reviewing the results and **ratio of Competent:Incompetent**. If staff are coming back with more incompetence, then further training methods will be required to hit the **90:10** Competent:incompetent goal. |
| --- |

### Bonus: Other Solutions

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

| Replacing Work BYOD Devices for Work-Managed Devices.  **Control Type**: Physical / Technical(Security Control Policy Deployment)  **Control**: Preventive and Deterrent  **Advantage**: Full-Control over devices. SilverCorp will be able to deploy only certain apps and security policies onto the devices, deterring employees from downloading and installing malicious programs onto devices. Also forces employees to use required authentication practices.  **Disadvantage**: Zero Trust and Expensive to implement as phones will be 1:1, if 250 employees are affected by this control and one phone is $1000, then that will cost $25000 for implementation, excluding associated security-policy deployment costs. |
| --- |

| Audit Employee Devices for Vulnerabilities  **Control Type:** Technical  **Control:** Detective and Corrective  **Advantage:** The security officers will be able to look into each potential threat per device and act on securing BYOD.  **Disadvantage:** Invasion of privacy. Very Time-consuming. Assuming that SilverCorp has 250 employees in the Sales and Finance departments, each device takes 1 hour to investigate. That’s 250 hours of work. |
| --- |

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