| 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.

| The potential security risks of allowing employees to access work information on their personal devices are as follows:   1. Data leakage-   Sensitive information, such as company files or personal information can be accidentally exposed, shared, or intercepted. Employees may use unsecured or public Wi-Fi networks to access company resources and lack the same security measures as corporate-owned devices. Jones, S. (2023, June 1). 6 Cybersecurity Risks of Using Personal Devices for Work. TeamPassword. Retrieved January 6, 2024, from https://teampassword.com/blog/byod-policies-cybersecurity-risks  Another source from ChatGPT on data leakage indicated a scenario of an employee’s phone being lost or stolen. Without proper security measures, any unauthorized individuals can access confidential data. (ChatGPT (2024, January 6) from https://chat.openai.com/c/e0111c7a-b744-4982-ba9a-ffa779e62a32)   1. Malware and Phishing Attacks-   ChatGPT on malware and phishing attacks indicated a scenario of an employee accidentally installing malware or falling for a phishing attack on their cell phone.Malicious software can compromise sensitive work data, capture login credentials, or allow unauthorized access to the corporate network. (ChatGPT (2024, January 6) from https://chat.openai.com/c/e0111c7a-b744-4982-ba9a-ffa779e62a32)  Also on the topic of malware and phishing attacks, Shanice stated that personal devices are more likely to be infected with malware, stating they would be more likely to not adhere to the security standards of the company as they would on a company device. The malware could easily spread through cloud services, emails, or file-sharing platforms. Jones, S. (2023, June 1). 6 Cybersecurity Risks of Using Personal Devices for Work. TeamPassword. Retrieved January 6, 2024, from https://teampassword.com/blog/byod-policies-cybersecurity-risks   1. Inadequate Device Security-   According to TeamPassword, personal devices often lack the security controls and monitoring capabilities. Companies may find it hard to enforce security policies or remotely manage devices. A personal device may not have the latest security patches installed. This can result in weak or reused passwords, lack of two-factor authentication, or failure to lock devices when not in use, all of which can lead to unauthorized access. Jones, S. (2023, June 1). 6 Cybersecurity Risks of Using Personal Devices for Work. TeamPassword. Retrieved January 6, 2024, from https://teampassword.com/blog/byod-policies-cybersecurity-risks  ChatGPT indicated a scenario similar to TeamPassword, stating personal devices may lack property security measures such as antivirus software, firewalls, or encryption. The lack of security measures on personal phones increase the likelihood of malware infections. (ChatGPT (2024, January 6) from https://chat.openai.com/c/e0111c7a-b744-4982-ba9a-ffa779e62a32)  3 potential attacks that can be carried out on an employee’s personal device:  - “Evil twin” attacks: Hackers set up malicious hotspots with trustworthy names like “Cafe free Wi-Fi” and once connected to the hotspot, they can easily intercept your data. Man-in-the-middle attacks (MitM) that break into a network and eavesdrop on data traveling between connected devices and the Wi-Fi router. Packet sniffing attacks are when malicious hackers capture data units across unsecured Wi-Fi, then they unpack the data to extract login credentials or financial information. Zaharia, A. (2023, January 10). The Dangers of Using Public Wi-Fi (and How To Stay Safe). Retrieved January 7, 2024, from https://www.aura.com/learn/dangers-of-public-wi-fi  -Phishing attacks are a top risk for organizations as attackers can exploit personal information like interests or social media activity to create highly targeted and convincing phishing emails. Jones, S. (2023, June 1). 6 Cybersecurity Risks of Using Personal Devices for Work. TeamPassword. Retrieved January 7, 2024, from https://teampassword.com/blog/byod-policies-cybersecurity-risks  -Code injection attacks. An attacker can add code to a legitimate website, apps, or inject malicious code displaying ads to entice you to click on it. Once clicked, it can install malware or adware. in the form of SQL Injection, Cross-Site Scripting (XSS), or Malvertising to make your device vulnerable to extraction of confidential data  Baker, K. (2023, November 9). 10 MOST COMMON TYPES OF CYBER ATTACKS. Retrieved January 7, 2024, from https://www.aura.com/learn/dangers-of-public-wi-fihttps://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/#6.%20Code%20Injection%20Attacks |
| --- |

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.)

| -For data leakage and unauthorized access, implementing strong encryption on the device, enforcing robust access controls, and enabling remote wipe functionality to erase data in case of loss or theft would be preferred employee behavior. (ChatGPT (2024, January 7) from https://chat.openai.com/c/e0111c7a-b744-4982-ba9a-ffa779e62a32)  Employees adhering to strict security protocols like data encryption and regular software updates, secure boot, and using a VPN to prevent data leakage or unauthorized access. Jones, S. (2023, June 1). 6 Cybersecurity Risks of Using Personal Devices for Work. TeamPassword. Retrieved January 7, 2024, from https://teampassword.com/blog/byod-policies-cybersecurity-risks  -Employee preferred behavior to prevent malware and phishing attacks by regularly updating and patching operating systems and security software, using a firewall, and keeping security settings turned on for security software,internet browsers, and operating systems.  FTC, C. A. (2021, May 1). How To Recognize, Remove, and Avoid Malware. Retrieved January 7, 2024, from https://consumer.ftc.gov/articles/how-recognize-remove-avoid-malware#:~:text=Here%20are%20ways%20to%20avoid%20malware%3A%20%C2%B7%20Install,if%20you%20keep%20your%20browser%E2%80%99s%20default%20security%20settings.  Educating employees about risks of clicking on suspicious links or downloading unknown files. Implementing security software on all personal devices used for work and having automatic and regular updates. (ChatGPT (2024, January 7) from https://chat.openai.com/c/e0111c7a-b744-4982-ba9a-ffa779e62a32)  -Employee preferred behavior for inadequate device security would be to enforce minimum security requirements such as mandatory antivirus software, regular security updates, and strong password policies.(ChatGPT (2024, January 7) from https://chat.openai.com/c/e0111c7a-b744-4982-ba9a-ffa779e62a32)  Employees should have strong security in place to protect unauthorized access inside personal devices such as multi-factor authentication and role-based permissions. Proper utilization of password management can also mitigate core security risks. Jones, S. (2023, June 1). 6 Cybersecurity Risks of Using Personal Devices for Work. TeamPassword. Retrieved January 7, 2024, from https://teampassword.com/blog/byod-policies-cybersecurity-risks |
| --- |

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.)

| -For quantitative data on the frequency of non-compliant behaviors, monitoring tools would be implemented on personal devices with access to confidential data. These tools would track and log employee activities, especially email attachments. (ChatGPT (2024, January 8) from https://chat.openai.com/c/37460d62-d40e-4066-a451-3a2bdfce01a8)  -An email would be sent out by the IT department around every three months that would be a fake malware email enticing employees to click the link inside. The email would be disguised as an internal company email and every time an employee clicks on it, a record or log can be kept to see how many of the total employees fell for the dummy malware email. For employees that have clicked on the email, an automatic email would be sent that includes the incident of clicking on a risky link as well as a training guide on how to protect yourself from emails and telling signs that it is indeed spam.  -Data analysis of existing data sources, such as security logs, to identify patterns of non-compliance. Use data analytic techniques to detect anomalies in employee behavior. (ChatGPT (2024, January 8) from https://chat.openai.com/c/37460d62-d40e-4066-a451-3a2bdfce01a8) |
| --- |

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.)

| To have no more than 5% of employees downloading suspicious email attachments, clicking on suspicious links, or responding to imposters phishing for confidential information. 100% of employees avoid downloading software from insecure sources, 100% of employees have two factor authentication installed, and the use of strong passwords. |
| --- |

### 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.

| 1. Management should be involved first as they would have the ability to coordinate funds and approvals for implementation of company goals. Management would also be the one to structure and communicate the goals so that all staff are on the same page and understand its coming “from the top”. Major updates and progress would be communicated to all staff through the management team. 2. The IT department should be involved in order to monitor employee records and track if the changes are effective. They can also implement the new changes as well as sending out a company wide training email, enticing employees to click on suspicious emails and tracking data on how well trained employees are. They can monitor and track threats that are constantly evolving and keep the rest of the company updated on new threats. They can also tell management how realistic it is to implement new features and how it will impact the company. 3. The finance department should be involved as they would keep records of expenses and funds available for changes. They would also need to budget expenses to be used for the new changes and updates in training materials. The finance department would be able to know and relay how much of the budget can be used for the new processes or if what is being asked for is too much. 4. The HR department should be involved as they deal with new employees directly in the beginning of their employment. They can provide training materials, policies, goals, and expectations to new employees. They can also communicate to current employees with updates on training, policies, goals, and expectations. 5. The employees should be involved as well.Their role would be to accept the new changes and implement them in practice as changes are made. They would report how effective the training and changes are, and how the changes could be improved. |
| --- |

### 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)?

| The training would be immediate for newly hired employees and annually for current employees. The new employees would be given policies, expectations, and training during their new hire orientation including the new training for cyber security. Current employees would be given the training annually in a shortened format with resources to learn more or get refreshers on the training. The training would need to be a combination of in-person, and remotely available depending on the size and nature of the company and its employees. With a local smaller company where employees rarely work remotely, the training would need to be in person. For a larger company with staff working remotely or in a hybrid situation, the training could be completed remotely or in person. Scheduled training would make sure that all those invited to do the training online would be on at a certain time with an instructor giving the information to potentially limitless numbers of staff at once. That way completion of the training can be logged and monitored. |
| --- |

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

| The training will cover these topics for all employees:  Policies and procedures- so that all employees follow the same guidance and understand the expectations of the company.  Reporting incidents- so that employees know what to do incase of a situation. They can report the problem so that it can be resolved and data is collected to keep track of trends or issues.  How to: for security on devices- To make sure that all employees have knowledge and access about the expected software to be installed on all devices accessing company files including two factor authentication, strong passwords, and a VPN.  Recognizing and avoiding threats- This topic would cover how to recognize vulnerabilities including phishing emails, public Wi-Fi, lack of security locks on devices that could be bad if the device is lost or stolen. Also covering avoiding the download of software from unknown sources, using a VPN, and keeping personal files and company files separate so as to not share accidentally with each other.  Examples of different phishing emails, and scenarios that can happen and have happened in the past. Being interactive, there could be a series of emails that the trainees would cast their vote on if the email is safe or not safe and why. What the impact of the scenario and what it could have led to.  Types of attacks that can happen, including data leaks, malware attacks, phishing attacks, man-in-the-middle attacks, adware, etc. and how they happen.  Statistics on the amount of attacks and the impacts of those attacks both internally and externally from other companies. This section would cover how often these threats can happen and who they happen to.  An explanation on how the training can be used in their professional life as well as their personal life. Being secure isn’t just for companies, cyber attacks can happen to individuals as well as companies. It’s a good habit to get into and it’s good practice to use it always.  Additional resources- For those employees who want to take their knowledge of cyber security above and beyond, there are other resources provided in order to encourage employees to learn as much as they can. |
| --- |

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

| The effectiveness will be measured a few ways:   1. Data analysis of employees use of a VPN and two factor authentication while accessing company files. 2. Reports of employees who have clicked on a company wide test email that was sent by the IT department to see how many employees clicked the suspicious link. 3. Company wide survey of training, how good was the training and what the employee may still need training on. 4. Communicating with the IT department on data of current threats that are still impacting the company and if it was included in the training. 5. A small questionnaire is sent to all employees to collect data on how much the employees understood from the training. |
| --- |

### 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?

| Implement network segmentation for BYOD devices.This means it divides the network into smaller, isolated subnetworks based on different criteria like function, location, or device type. It limits access of each subnetwork, reducing attack surface and containing the impact of a breach.  Linkedin (2024). How can you secure your network in a BYOD environment? Retrieved January 8, 2024, from https://www.linkedin.com/advice/0/how-can-you-secure-your-network-byod-environment#:~:text=Network%20segmentation%20can%20help%20you,the%20impact%20of%20a%20breach.  This is a technical control.  The goal of this control is to avoid a breach infecting the entire network. It would only have access to a subnetwork which means attackers can’t hurt the entire network in a single attack.  This control would be preventative  The advantage is that the network would be more secure as a whole having so many subnetworks that it would be impossible to impact the entire system. The problem can then be isolated, contained, and dealt with while keeping the network as a whole up and running.  The disadvantage is that it would require more updates and coordination because the data would be segmented into different departments. This could lead to issues when updating or transferring information. It could also lead to needing more staff in order to smoothly run the subnetworks and monitor them. |
| --- |

| Multi-Factor Authentication implemented for BYOD devices. This means that in order to access programs, etc., you would be required to have more than just a password. Either a temporary code sent to your email or mobile device, or biometric scanners like a face ID, retina scanner, or fingerprint depending on the Multi-Factor Authentication used.  FTC, C. A. (2022, September 1). Use Two-factor Authentication to Protect Your Accounts. Federal Trade Commision Consumer Advice. Retrieved January 8, 2024, from https://consumer.ftc.gov/articles/use-two-factor-authentication-protect-your-accounts  This is a technical control.  The goal of this control is to avoid a breach by requiring the individual to prove that it is indeed them requesting access by more than one type of “key”. It keeps unwanted individuals from accessing your data even if they somehow get your password or figure out your login credentials. The unwanted individual would not be able to replicate your fingerprint for example.  The advantage is it reduces the risk of unauthorized individuals from accessing your data even if they have your phone, or your login credentials. It adds extra security to your accounts and devices.  The disadvantage is it is another step that users have to take in order to access records or programs. Some users would find this to be inconvenient but with the trade off of added security. It also adds a little more time to the accessing process. |
| --- |

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