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.

According to Yacono (2023), some security risks of allowing employees to access work on their personal devices include:

- Data Leakage: Personal devices used for work can lead to data exposure or loss, especially if devices are misplaced, stolen, or infected with malware.
- Malicious Apps: Employees may download fake or malicious apps that can compromise device security, leading to surveillance, unexpected charges, or loss of personal/work information.
- Device Management Challenges: When devices leave the company's premises, it becomes challenging to control how they are used, exposing them to risks like unsecured Wi-Fi connections or theft.
- Device Infection: Infected smartphones may go unnoticed by users, who can become careless about mobile security due to “app fatigue” and excessive exposure to mobile content. Keeping mobile operating systems up-to-date and using file integrity monitoring is essential to detect and act on device infections.

- Mixing Personal and Business Use: It's inevitable to mix personal and business use when employees work from their personal devices, exposing devices to compromised websites or potential data breaches. Educating employees on security best practices is essential.
- Inability to Control Employees’ Personal Devices: Lack of control around devices is a significant concern when employees work from their personal devices, especially when employees leave the organization or exhibit questionable behaviours. Mobile device management and access governance can help mitigate this risk.
- Lost or Stolen Devices: The loss or theft of employee devices can lead to data breaches. Employees (who are allowed to work remotely) should be trained to protect their devices with passwords or biometric security measures to prevent unauthorized access to data. Employers who are not given remote access should be prohibited from accessing company work on their personal devices.

Potential attacks that can be carried out include:

- Phishing Attacks: Attackers can launch phishing campaigns targeting employees who use personal devices for work. They may send deceptive emails or messages that appear to be from legitimate sources, such as the company's IT department or a well-known app store, requesting login credentials or sensitive information. Unsuspecting users might unknowingly provide their login details, leading to unauthorized access to their work accounts and potentially sensitive data.
- Man-in-the-Middle (MITM) Attacks: In public Wi-Fi networks or compromised networks, attackers can intercept data transmitted between a personal device and the company's servers. Using techniques like packet sniffing or spoofing, the attacker can capture login credentials, personal information, and sensitive business data. This can lead to unauthorized access to corporate systems and data leakage.
- Malware Attacks: Employees may unknowingly download and install malicious apps or software on their personal devices. Malware can include spyware, ransomware, or keyloggers, allowing attackers to monitor user activities, lock devices for ransom, or steal sensitive information. Even legitimate-looking apps may be repackaged with malicious code and distributed through unofficial app stores or phishing links.
- DdoS Attacks: By utilizing multiple compromised computer systems as sources of attack traffic, DDoS attacks can severely affect employees working from personal devices, leading to interruptions in accessing essential services and resources, like an unexpected traffic jam hindering regular traffic flow (What is a DDOS attack?, 2023).

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.)

Employees play a crucial role in helping organizations maintain their security against potential cybersecurity threats. According to Infosec Guide: Dealing with Threats to a BYOD Environment (2017), to reduce the chance of security breaches occurring, employees can take several actions:

- Refrain from accessing company work, accounts and other related applications on personal devices if not given authority from the company to do so:

- Employees must refrain from accessing company work, accounts, and applications on personal devices without proper authorization to avoid potential security breaches and data compromise.

-If authorized to use personal devices for work, employees should strictly adhere to the company's BYOD policies, using strong passwords, enabling security features, and keeping devices and software updated.

-Mixing personal and work activities on the same device should be avoided, and company data should never be stored or shared on personal devices without explicit permission to minimize security risks.

- Keep Passwords Strong and Secure:

- Use complex and unique passwords with a mix of uppercase and lowercase letters, numbers, and special characters.
- Store passwords securely, such as in a password manager, and never share them with others.

- Be Aware of Phishing Scams:

- Be cautious of emails or messages encouraging clicking on links or providing personal data, even if they seem legitimate.
- Verify sender identity and URLs before clicking any links or entering sensitive information online.
- Be wary of emails creating a sense of urgency, as these could be phishing attempts.

- Keep Software and Security Tools Up to Date:

- Regularly update software to address security vulnerabilities and weaknesses.

- Keep security tools like firewalls and antivirus software updated to detect and prevent malicious activity.

- Report Suspicious Activity Immediately:

- Report any suspicious cyber activity immediately to the IT security team.
- Early reporting allows for prompt action and mitigation of potential security breaches.

- Reducing the Risks of Device Loss:

- Remote employees should be required to use security solutions with data encryption.
- Implement secure authentication, such as multifactor authentication, for accessing company data on personal devices.

- Restrict Access to Necessary Information:

- Limit employee access to data by providing only the information they need for their specific roles.
- Ensure departments only have access to relevant files and data that they need to do their jobs.

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.)

Research conducted by Mahyoub et al. (2023), found the following methods can be used to measure employees' preferred behaviour:

- Incident Response Plan Development:

Track and analyze security incident reports related to employees' accessing work-related applications on their personal devices. Look for patterns or trends in incidents that indicate non-compliance with preferred behavior. For example, incidents related to phishing attacks, malware infections, or data breaches might reveal instances of employees not following security protocols. Regular testing and updating of the plan are crucial to address evolving threats and minimize potential damages during cyberattacks.

- Employee Surveys:

Gather anonymous feedback on security practices through employee surveys to ensure compliance with security protocols. This can provide valuable insights into their compliance with security protocols - using safe Wi-Fi networks, encryption, MFA etc. and any challenges they face in adhering to preferred behaviour.

- Compliance Tracking:

Keep track of employees' compliance with security policies and procedures relating to security. This can include monitoring whether employees have enabled security features like encryption or multi-factor authentication on their devices, adhering to safe password policies etc. By sharing information, employees can stay vigilant, make informed decisions, and contribute to the organization's cybersecurity resilience.

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.)

Ideally, the goal for the organization would be 5% or less regarding the following behaviours:

- Employees accessing company work, accounts and other work-related applications on their personal devices
- Clicking phishing emails
- Not using device encryption and MFA
- Downloading and installing malicious apps or software on personal devices

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.

- CISO: The CISO is responsible for leading the development and implementation of security awareness training programs, ensuring they align with the organization's security strategy and empower employees to protect sensitive information. Additionally, the CISO's overall role includes developing security policies, managing security teams, monitoring network activity for threats, overseeing incident response, coordinating breach responses, and reporting to higher-level executives (Watts, 2022).

- CFO: The CFO's role in employee security training is to allocate the necessary budget and resources for comprehensive security awareness training programs and understand the financial impact of cybersecurity breaches. They collaborate with the CISO to assess the ROI of security initiatives, establish metrics, and communicate with the C-suite to prioritize cybersecurity spending and manage increased cybersecurity risk effectively (Bishop, 2022).

- CEO: The CEO's role in employee security training is to actively demonstrate leadership and commitment to cybersecurity by supporting and promoting security awareness initiatives, allocating resources for training, and participating in security training themselves. Their engagement in shaping the organization's security posture fosters a culture of vigilance, accountability, and continuous improvement, safeguarding critical assets and signaling a strong commitment to cybersecurity throughout the company (Dinha, 2023).

- CIO: The CIO is responsible for establishing, implementing, and enforcing an organization-wide information security program, providing expert advice on IT strategic planning, resource prioritization, and maintaining a skilled workforce capable of adapting to technological advancements. Additionally, the CIO ensures the agency maintains a skilled workforce capable of adapting to technological advancements and evolving mission needs (CIO Role at a Glance, n.d.).

- Director of HR: The Director of HR plays a crucial role in overseeing and coordinating employee security training, ensuring all employees receive necessary training and collaborating with the IT security team to reinforce security practices. HR professionals serve as a central repository for personnel information, enabling them to identify patterns and trends to mitigate potential harm to the organization and its employees. They also take charge of developing training plans and schedules to ensure smooth company operations during training sessions (Human Resources Role in Preventing Insider Threats, n.d.).

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 will take place semi-annually to ensure continued compliance with regulations and laws, and to ensure employees are up to date with cybersecurity attacks actors and methods, and policies and procedures. It will be completed over an 8-day period, training 25% of employees for 2 days at a time to ensure productivity is not greatly affected. The training will be in an online interactive environment with short quizzes at the end of each module, and a survey at the end. This will be used to capture any suggestions for improvement that employees may have.

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

The Security Awareness Training will cover various aspects, including:

- Overview of the company’s state of security: Here, we will share the results of the employee survey, incidents response tracking and compliance tracking. We will also reiterate the importance of cybersecurity as a part of the company’s culture.

- Identifying cyberattacks and recognizing cybersecurity threats: Detecting cyberattacks and recognizing cybersecurity threats is crucial in security training because it allows organizations to reduce the damage caused by breaches. Breaches can happen despite efforts to create a safe environment, so being prepared to detect and respond to attacks promptly is essential. Time to discovery and appropriate actions strongly correlate with the impact of a breach and the recovery efforts required. By constantly monitoring network activity and learning to detect anomalies, organizations can minimize damage and isolate intruders, helping protect sensitive data and systems (The Importance of Detecting Cyber Threats Before Operations are Impacted, n.d.).

- Verifying email legitimacy (identifying phishing emails): In security training, verifying email legitimacy (identifying phishing emails) is crucial because malicious emails can be challenging to identify. Employees should check the sender's email address for valid usernames and domains, ensuring it matches known contacts. They should also look for grammatical errors, inconsistencies in tone, and suspicious requests for sensitive information, as legitimate companies maintain professionalism and avoid such practices. Properly identifying phishing emails helps prevent falling victim to cyberattacks and protects sensitive data from unauthorized access (Spotting malicious email messages, 2022).

- The importance of securing home networks: For employees that are allowed to work from home, it is imperative that SilverCorp enables a secure remote workforce for information security due to the rising risks of phishing, malware, and social engineering, especially among remote workers. Providing a VPN connection is crucial to protect company data and resources, as it creates an encrypted private connection from employees' devices to the corporate network, safeguarding against common remote work security threats like phishing attacks, remote desktop account attacks, and data breaches. Securing home networks through VPNs is a vital topic for security training as it ensures employees can work remotely while maintaining the integrity and confidentiality of sensitive information (How to secure your remote workforce and protect your business with a secure VPN, 2023).

- The importance of using safe public Wi-Fi (or avoiding public Wi-Fi): Since some employees at SilverCorp are remote, we will need to educate them on the dangers of using public Wi-Fi. Using public Wi-Fi can lead to potential hacking risks, as cybercriminals can employ various techniques to exploit unsecured networks and steal sensitive information. Attacks such as "evil twin," man-in-the-middle, password cracking, and packet sniffing can compromise user data, including passwords and personal information. Security vulnerabilities and misconfigurations in routers also make it easier for hackers to gain unauthorized access to devices. Therefore, employee security training on the dangers of using unsafe public Wi-Fi is essential to raise awareness and educate them on how to protect themselves and their work-related data while using such networks. Using a virtual private network (VPN) with strong encryption is crucial to protect personal data when connecting to any Wi-Fi hotspot (Zaharia, 2023).

- Data encryption and Multi-Factor Authentication: Data encryption and multi-factor authentication (MFA) are important topics for employee security training as they provide essential protection against cyber threats. Encryption safeguards sensitive data, preventing unauthorized access and potential data leaks. MFA adds an extra layer of security by requiring additional verification beyond passwords, mitigating the risk of malware attacks and unauthorized access. By teaching employees about these security measures, SilverCorp can better safeguard intellectual property, customer information, and other sensitive data, reducing the likelihood of data breaches and potential fines (Why are encryption and MFA essential for your business?, 2020).

- The importance of keeping passwords strong and secure: Teaching SilverCorp’s employees about strong and safe passwords is vital for security training because strong passwords protect electronic accounts and devices from unauthorized access, safeguarding sensitive personal information from cyber threats and hackers. Implementing two-factor authentication (2FA) adds an extra layer of security, requiring more information than just a password. Encouraging the use of complex passwords with numbers, symbols, and a mix of uppercase and lowercase letters, along with making them at least eight characters in length, further enhances security. Advising employees to create passwords from abbreviated phrases or sayings that are memorable to them can help strike a balance between security and usability. Additionally, emphasizing the importance of regularly changing passwords to reduce the risk of compromise and avoiding password recycling ensures a safer digital environment (Cybersecurity 101: Why Choosing a Secure Password Is So Important, 2023).

- The importance of keeping software and security tools up to date: Regularly updating software and security tools is crucial for protecting personal devices from cyber threats. Operating systems are vulnerable targets for hackers, and regular updates help to stay ahead of changing threats. Failing to update leaves devices vulnerable to data loss, compromised access to accounts, and potential financial losses. Employee security training should emphasize the importance of timely software updates to safeguard sensitive information and prevent cyber incidents (Software updates: Why they matter for cyber security Government of Canada, 2020). Remote workers at SilverCorp will be required to keep their devices up to date, along with the rest of the company.

- The importance of reporting suspicious activity immediately upon discovery: Organizations must have measures in place to monitor suspicious network activity as it can have severe implications for their financial security and future. Suspicious network activity encompasses abnormal access patterns, database activities, file changes, and other unusual actions that can indicate an attack or data breach. Recognizing and reporting these activities is crucial as it allows organizations to swiftly respond to security threats, identify the source and nature of the breach, and minimize potential damage. By teaching employees to report suspicious activity immediately, SilverCorp can leverage its workforce as an additional line of defense, helping to detect and address security incidents promptly (Yacono, 2022).

- Access control and authorization: Access control and authorization are essential in security training, emphasizing the principle of least privilege. By implementing this principle, employees are granted access only to the functions and privileges necessary for their specific tasks, minimizing the risk of unauthorized access and data breaches. Teaching employees to have individual log-in credentials and separate administrative accounts with privileged access rights ensures better protection of sensitive information and reinforces a strong security posture within the organization (Choosing the best cyber security solution for your organization, 2022).

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

SilverCorp will measure the effectiveness of their security training program using the following metrics and details (Measuring the effectiveness of security awareness programs: What you need to know, 2023):

• Participation Rates:
- Measure the number of employees who complete the security awareness training.
- Identify the willingness of employees to participate in the training.
- Use the data to make improvements to increase participation rates if engagement is low.

• Completion Rates:
- Calculate the percentage of employees who successfully complete the entire security awareness training program.
- Ensure that all employees have access to and complete the training in its entirety.

• Quiz Scores:
- Track quiz scores to assess employees' knowledge retention from the security awareness training.
- Evaluate how well employees understand the information delivered in the training.

• Phishing Simulation Results:

- Conduct quarterly phishing simulations to measure employees' susceptibility to phishing attacks.
- Analyze the percentage of employees who fall for the phishing attack to identify vulnerabilities to social engineering.
- Use the results to determine areas of improvement and adjust training content accordingly.

• Frequency of Training for Vulnerable Employees:
- Identify employees who repeatedly fall for phishing simulations or demonstrate inadequate knowledge retention.
- Provide these vulnerable employees with additional quarterly training instead of the standard semi-annual training to address their specific needs.

• Security Incident Reports:
- Monitor the number of security incident reports before and after the training program implementation.
- Analyze if there is a decrease in security incidents as employees become more aware of potential threats.

• Employee Feedback and Surveys:
- Gather feedback from employees through surveys to gauge their perception of the training program's effectiveness.
- Use feedback to identify strengths and weaknesses in the training content and delivery.

• Time to Detect Phishing Attempts:
- Measure the average time it takes employees to recognize and report phishing attempts.
- Aim to reduce this time through regular training and reinforcement.

By employing these metrics and continually adjusting the training program based on the data collected, SilverCorp can enhance the effectiveness of their security awareness training and better protect their organization from potential cyber threats (Measuring the effectiveness of security awareness programs: What you need to know, 2023).

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?

- Regular communication/Continuous reinforcement: As an alternative to the training program, SilverCorp could prioritize cybersecurity awareness through continuous reinforcement of security best practices. Regular reminders, posters, emails, and short video clips would be used to keep key cybersecurity messages at the forefront of employees' minds. Clear and concise security policies would be developed and made readily accessible to all employees, and policy updates would be regularly communicated through various channels to ensure that the principles of cybersecurity become ingrained in the collective workforce consciousness (The Security Company (International) Limited, 2023).

  (a) Administrative control
  (b) The goal of this control would be preventative.
  (c) Advantage: By combining culture initiatives and consistent communication, SilverCorp would aim to create a security-aware workforce that can effectively mitigate potential cyber threats.
  (d) Disadvantage: Continuous reinforcement of cybersecurity messages through various channels may lead to communication fatigue or desensitization among employees. Information overload can cause employees to become indifferent or less attentive to the messages over time, potentially diminishing the effectiveness of the awareness program and challenging the sustainability of employees' engagement and vigilance. Striking a balance between reinforcement and avoiding overwhelming employees with redundant messages is crucial to ensure continued effectiveness.

- Develop a secure culture: SilverCorp would aim to foster cybersecurity awareness through the development of a strong security culture. This would be achieved by embedding cybersecurity into the organization's core values and encouraging employees to promptly report any suspicious activities without fear of repercussions. A security advocate/champions program would also be established to recognize and reward individuals who actively contribute to the organization's security, reinforcing the importance of cybersecurity throughout the workplace and promoting desired security behaviours. Further, to ensure comprehensive security, SilverCorp would also collaborate with a trusted cybersecurity partner who would conduct organization-wide behavioural surveys to identify gaps in behaviour, hardware, and policies. Targeted materials would then be provided to address any irregularities, helping to strengthen the overall cybersecurity posture of the organization (The Security Company (International) Limited, 2023).

(a) Administrative control
(b) The goal of this control would be preventative.
(c) Advantage: Developing a strong security culture at SilverCorp would help to create a workforce that is more vigilant and proactive in identifying and reporting potential cybersecurity threats, leading to improved incident response and overall security posture.
(d) Disadvantage: Implementing and maintaining a security advocate/champions program and conducting organization-wide behavioural surveys would require significant time, effort, and resources, potentially impacting other operational priorities and budgets.

References

Bishop, E. (2022). *Why the CFO is crucial to your company's cybersecurity*. Forbes https://www.forbes.com/sites/forbestechcouncil/2022/09/20/why-the-cfo-is-crucial-to-your-companys-cybersecurity/?sh=5777962d11df

Choosing the best cyber security solution for your organization (2022). Government of Canada https://www.cyber.gc.ca/en/guidance/choosing-best-cyber-security-solution-your-organization-itsm10023

CIO Role at a Glance (n.d.). CIO.GOV https://www.cio.gov/handbook/cio-role-at-glance/#:~:text=Information%20security%20and%20privacy%20%E2%80%93%20CIOs,and%20Challenges%20in%20Implementing%20Responsibilities

Cybersecurity 101: Why Choosing a Secure Password Is So Important (2023). Walden University https://www.waldenu.edu/programs/information-technology/resource/cybersecurity-101-why-choosing-a-secure-password-in-so-important#:~:text=They%20protect%20your%20electronic%20accounts,from%20cyber%20threats%20and%20hackers

Dacono, L. (2023). *The 8 top BYOD security risks (and how to mitigate them).* CIMCOR. https://www.cimcor.com/blog/7-scariest-byod-security-risks-how-to-mitigate

Dinha, F. (2023). *Why your CEO needs to be a cybersecurity expert.* Forbes https://www.forbes.com/sites/forbestechcouncil/2023/06/22/why-your-ceo-needs-to-be-a-cybersecurity-expert/?sh=2210d4f04893

How to secure your remote workforce and protect your business with a secure VPN (2023). PaloAlto Networks https://www.paloaltonetworks.com/cyberpedia/how-to-secure-your-remote-workforce

Human Resources Role in Preventing Insider Threats (n.d.). CISA https://www.cisa.gov/sites/default/files/publications/HRs%20Role%20in%20Preventing%20Insider%20Threats%20Fact%20Sheet_508.pdf

Infosec Guide: Dealing with threats to a bring your own device (BYOD) environment. (2017, April 17). Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/-infosec-guide-bring-your-own-device-byod

Ibitoye, O., Isleem, K., Mahyoub, M. & Matrawy, A. (2023). Cybersecurity challenge analysis of work-from-anywhere (WFA) and recommendations based on a user study. *School of Information Technology, Carleton University.* https://carleton.ca/ngn/wp-content/uploads/WFA_Mahyoub.pdf

Measuring the effectiveness of security awareness programs: What you need to know (2023). Cybsafe https://www.cybsafe.com/blog/measuring-the-effectiveness-of-security-awareness-training/

Software updates: Why they matter for cyber security (2020). Government of Canada

Spotting malicious email messages (2022). Government of Canada https://www.getcybersafe.gc.ca/en/blogs/software-updates-why-they-matter-cyber-security https://www.cyber.gc.ca/en/guidance/spotting-malicious-email-messages-itsap00100

The Importance of Detecting Cyber Threats Before Operations are Impacted (n.d.). Truesec. https://www.truesec.com/hub/article/the-importance-of-detecting-cyber-threats-before-operations-are-impacted

The Security Company (International) Limited (2023). *How can you promote cyber security awareness in the workplace*? The Insider https://www.linkedin.com/pulse/how-can-you-promote-cyber-security-awareness-workplace/

Watts, S. (2022). *The CISO role: what does a chief information security officer do?* Splunk. https://www.splunk.com/en_us/blog/learn/chief-information-security-officer-ciso-role.html#:~:text=Primary%20responsibilities%20of%20CISOs&text=This%20includes%3A,and%20preparing%20for%20potential%20threats

What is a DDoS attack? (2023). Cloudflare https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

Why are encryption and MFA essential for your business? (2020). Eset https://digitalsecurityguide.eset.com/en-us/why-are-encryption-and-2fa-essential-for-your-business

Yacono, L. (2022). *Monitoring for suspicious network activity: key tips to secure your network.* CIMCOR *https://www.cimcor.com/blog/monitoring-for-suspicious-network-activity*

Zaharia, A. (2023). The dangers of using public wi-fi (and how to stay safe). Aura https://www.aura.com/learn/dangers-of-public-wi-fi#:~:text=4.-,Snooping%20for%20confidential%20data,you%20use%20public%20Wi%2DFi