**Step 1: Measure and set goals.**

The employees of Silvercorp have increasingly used their personal devices to access work email and other communication platforms like Teams or slack. This opens the door for a cybercriminal to attack the company and gather the information that might be useful to sell on cybercriminal platforms. Some of the potential attacks that can be carried out include.

1. Malware: Using personal devices for work can lead to a back door entrance for hackers to delete some crucial files or gather unauthorized access to some applications. Some of the most common malware attacks could include: -: -

* Ransomware: is a form of malware that extracts ransom from users, leaving them with denial of services for some files or applications, making them permanently non-useable.
* Spyware: Installing software without the user's knowledge that record, report, and their activities.(able, N. 2021, October 1).

1. Credentials harvesting: This attack is usually carried out by phishing emails to gather user IDs and passwords by clicking on a link, e.g., creating a fake (replica) website to collect credential information. Once the information is collected, the website shows an error. ( Able, N. 2021, October 1).
2. Lost or stolen devices: Most personal devices lack the first layer of encryption, such as an application like Bitlocker or MFA (Multi-factor Authentication), which protects devices from unauthorized access when it is stolen or lost. Personal laptops are vulnerable since they can be penetrated using techniques like spraying and brute force (Brook, C. ,2023, March 31).

Most of these attacks can be carried out if the user visits unknown websites and download attachments from non-trusted sources, uses public free Wi-Fi, or provides accessibility of the device to an unknown person. Employees comply with the organization's policies and procedures in order to protect the data from threat actors, vectors, and intelligence sources and are expected to behave accordingly; for example:

* **Week Credential security or using repetitive and common password**: Employees are expected to have a password that is 12 characters long that includes alphanumeric, symbol, and both upper and lower case. They must also ensure they do not write down, share or save account credentials on the browser.
* **Employees accessing open Wi-Fi and Sharing is on in public spaces:**  Employees used to use a secure network and avoid using an open wireless network since these networks are often not encrypted and vulnerable to data breaches. Keep sharing off from the system preference or control panel when in public places.
* **Employee opening email and clicking on the link from unrecognized sender:** Employee is expected to delete any suspicious email and report to the local security office as soon as possible.

In order to make sure that employees are following the correct behavior I would test the employees through :-

1. **Quizzes and survey**: Organizing quizzes and surveying to ensure that employees can answer effectively with the possibility of providing real-life case studies. The answers will determine if they are following the security protocols or not.(Mike, 2021)
2. **Security review**: These reviews are conducted to see how an employee can compromise confidential information in the workplace. One of the ways to conduct this review is clean desk policy and physical security to see if employees are following the security standard established by the organization. These checks can be done during office hours by a reviewer. Suppose there is a violation of the policy. In that case, a picture is taken as evidence and kept for future surveys to ensure they are charged with a penalty or some punishment if the same person violates the policy again (Mike, 2021)
3. **Simulating phishing attacks**: Performing a control test to see if the employee follows the security protocols taught during security awareness training. This test includes an email from an anonymous user which contains a link and sees if the employee clicks on it or not.  
   (Mike, 2021)

Since eliminating the security risk entirely is not achievable, SilverCorp is spending $10 million to ensure the company is equipped to deal with any vulnerability. In addition, the company is expected to reduce the loss of intellectual property by 35% by deploying monitoring software on office laptops or computers. The company will also provide employees free access to the premium version of NordVPN, which they can install on their personal devices. Moreover, the company aims to reduce privacy and safety threats by 10% by hiring more security personnel like system and network administrators and penetration testers to deal with vulnerabilities on time.

**Step 2: Involve the right people.**

Companies may have varying organizational structures and policies regarding security. However, in general, five significant departments or employees may be involved in implementing security policy in a company:

1. **Information Technology (IT) department:** This department is typically responsible for managing the company's computer systems and network infrastructure. They may be involved in implementing security policies such as setting up firewalls, monitoring for suspicious network activity, and managing access control to the company's digital assets (Educause, 2023)
2. **Human Resources (HR) department**: The HR department plays a crucial role in ensuring that employees are aware of and compliant with the company's security policies. They may be responsible for training employees on security best practices, conducting background checks on new hires, and ensuring that employees are aware of the consequences of violating security policies (Educause, 2023)
3. **Legal department:** The legal department may develop and enforce security policies that comply with relevant laws and regulations. They may also investigate security breaches and take legal action against individuals or organizations responsible for the breach (Educause, 2023)
4. **Physical Security department:** This department is responsible for ensuring the safety and security of the company's physical assets, such as buildings and equipment. They may be involved in implementing security policies such as monitoring access to the company's premises, installing security cameras, and implementing security protocols for handling sensitive physical documents (Educause, 2023)
5. **Executive leadership:** The company's executive leadership, including the CEO and board of directors, may be responsible for setting the overall tone and direction for the company's security policies. They may also allocate resources to support security initiatives and ensure that the company's security policies align with its strategic goals (Educause, 2023)  
     
   In summary, implementing a comprehensive security policy involves collaboration among multiple departments and employees within a company, each with its own unique roles and responsibilities.

Step3: Training Plan

A security awareness training plan ensures that the employees understands and follows the organization's security policies and procedures. Here are some of the recommendations I will keep in mind to design an effective training plan.

1. Learning: The training will be provided through a learning management system which is an online platform every three months. However, employees can also attend Instructor-led sessions at request. Both modes will have Interactive simulations and quizzes to test the knowledge of employees after the training session. It is also essential to provide refresher training throughout the year to reinforce key concepts and keep employees updated on emerging threats. The training topics will include a wide range of topics relevant to the organization's security policies and procedures. These may include password hygiene, phishing awareness, social engineering tactics, secure email, and physical security practices. In short, training should cover the importance of data protection and privacy (Jennings, 2022).
2. Measurables and reward: One of the best to measure the effectiveness of the training is by using metrics such as employee engagement, feedback, and performance metrics related to security incidents. Assessment can be performed after the training, identifying areas where additional training is required. In addition, the company should recognize and reward employees who demonstrate sound security practices to encourage employees. Some examples would be providing gift cards or generating a point system from which employees can buy a few things from amazon or Walmart etc.; This can help reinforce the importance of security and encourage employees to be more vigilant in their day-to-day activities (Jennings, 2022)
3. Continuous improvement: the company needs to keep the training program up to date, adjust to the latest threats and feedback, and change the organization's policies and procedures accordingly (Jennings, 2022)

*References*

able, N. (2021, October 1). *Top 7 risks of Bring your own device (BYOD) - N-able*. N. Retrieved March 31, 2023, from <https://www.n-able.com/blog/the-top-7-risks-of-bring-your-own-device-msps-should-remember>.

Brook, C. (2023, March 31). *The Ultimate Guide to BYOD security: Definition & more*. Digital Guardian. Retrieved March 31, 2023, from <https://www.digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating>.

Kilgore, M. (2021, May 10). *8 ways to get employees to follow IT security policies*. Global Knowledge. Retrieved March 31, 2023, from <https://www.globalknowledge.com/ca-en/resources/resource-library/articles/8-ways-to-get-employees-to-follow-it-security-policies/>.

*Organizational security awareness*. EDUCAUSE.edu. (n.d.). Retrieved April 1, 2023, from <https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/organizational-security-awareness>.

Jennings, M. (2022, November 9). *8 steps to implement a cyber security awareness training program*. SymQuest Tech Talk. Retrieved April 1, 2023, from <https://blog.symquest.com/steps-to-implement-a-cyber-security-awareness-training-program-at-your-company>.