**Week 2 Homework: Assessing Security Culture**

* This week we learned about security culture and how to promote it within organizations.
* It’s important that all employees are aware of common security risks and treat security seriously. The majority of cyberattacks aim to exploit human weaknesses with methods like phishing.
* For this reason, people are most often the weakest link in an organization’s security defences.

**Scenario**

* Employees at SilverCorp are increasingly using their own personal devices for company work.
* Specifically, over half of all employees check their work email and communications via Slack on their personal mobile phones.
* Another 25% of employees are doing other work-related activities using work accounts and work-related applications on their personal phone.
* Allowing sensitive work information to be shared on employees’ personal devices has several security implications.
* You must research these security risks and use the security culture framework to develop a plan to mitigate the concerns.

**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.**

**Improper mobile management** can turn into a potential security risk in the scenario the employee leaves the organisation, and they continue to have access to company data & applications on their personal devices.

**Malware** that infects the network from personal devices by staff downloading various external types of files that is infected with Malware such as applications, emails, PDFs, etc.

**Lost or stolen devices** is a potential security risk in the scenario where the employee has lost their device and has not been following company security protocol by storing data/information on unsecured applications.

1. **Based on the above scenario, what is the preferred employee behaviour?**

**Improper Mobile Management**

The preferred behaviour for improper mobile management would be to ensure that there is policy in place for staff to return company devices or uninstall applications that contain company data if they’re no longer associated with the company. On top of this, there will be systems in place to revoke access, and reset passwords once an employee is no longer associated with Silvercorp.

**Malware**

The preferred behaviour for security breaches via malware is for employees to avoid visiting unsecured webpages and clicking on malicious hyperlinks in emails. Employees will also be required to install the company issued anti-virus software on their personal devices and to ensure that the software is up to date with the latest version installed.

**Lost or Stolen devices**

The preferred behaviour in the scenario of a security risk from a lost or stolen device if employees is to ensure that staff only access and save company data/information via connection to company VPN and to not save company sensitive information on their own personal hard drives.

1. **What methods would you use to measure how often employees are currently *not* behaving according to the preferred behaviour?**

Measures that will be implemented to see if employees are behaving according to the preferred behaviour for ‘Improper Mobile Management & lost and stolen devices’, this will be measured via the training program that will be discussed below as this will be a company policy that employees will need to attend on a quarterly basis. Employees will also be required to complete a mandatory questionnaire that will cover a variety of cyber security topics where staff will be required to achieve a 100% result to pass. The results from the questionnaire will provide insight on what topics & areas requires further investment in future training seminars to ensure employees are up to date on potential security risks with their personal devices.

Regarding ‘Malware’, this will be measured by SilverCorp hiring a penetration testing firm to begin a phishing campaign by sending out emails to their personal/work addresses with links & attachments that contain malware. This will allow the organisation to keep track of how many employees fall for the phishing attempt or clicked on the links/attachments that contained malware and advise the percentage of employees that need to undergo further training if they fall for the phishing attempt.

1. **What is the goal that you would like the organization to reach regarding this behaviour?**

The goal for Silvercorp regarding the training program will be to train 100% of staff by the end of the year. The security training sessions will be hosted quarterly and will aim to train 25% of total employees per quarter until all staff are trained by the end of the year.

For the phishing campaign, the goal for Silvercorp will be to aim for less than 10% of employee participation in phishing attempts, and based on the results achieved, aim to set a goal that less than 5% of employees will engage in the phishing attempts by the start of the financial year.

**Step 2: Involve the Right People**

Chief Executive Officer:

The CEO’s role is to plot the overall direction of the company regarding the corporate mission/goal, and their responsibilities within this is to determine what the company needs to focus on to achieve these goals with the assistance of their core leadership team of the CIO, COO, and CFO.

Chief Information Officer

The CIO role is to have executive responsibility for the execution, administration, and serviceability of computer technologies and information. The responsibilities of the CIO would involve the implementation of technological aspects of the proposed Cyber Security framework such as Anti-Malware software, encryption of personal devices, and revoking access of unauthorised employees.

Chief Operating Officer

The COO role is to administer the company’s day-to-day business operations and administration. The responsibilities of the COO would consist of communicating the changes in policy to the employees and creating the training program to educated staff that use their personal devices on the risks involved (e.g., Malware).

Chief Financial Officer

The CFO is the highest financial position within an organisation and its role is to have executive responsibility of the implementation, management, planning, and running of all financial matters. The responsibilities of the CFO would consist of determining whether the implementation of encrypting all devices or providing anti-malware software is financially feasible for the company.

Cyber Security Department

The role the Cyber Security department is to ensure protection for the company’s information technology infrastructure, and to prevent & monitor data breach attacks. The responsibilities for the Cyber Security department in this scenario would be to monitor, assess the survey/questionnaire & phishing campaign results and identify employees that would need to undertake further training or be issued a company device.

**Step 3: Training Plan**

How frequently will you run training? What format will it take?

* The training program will be issued to employees that have opted to use their own personal devices instead of company issued. The training will be run on a quarterly basis for all those staff involved, and it will be completed online via an eLearning module that requires a 100% result to meet satisfactory requirements

What topics will you cover in your training and why?

The training program will undergo a variety of topics to ensure that staff are up to date and aware on how to mitigate risks in the cyber security landscape. The topics that the program will include are:

* Company statistics outlining the number of breaches has occurred due to staff errors, and what cost are involved in the scenario of a cyber security breach
* Online training for staff to educate on how to install anti-malware software on personal devices and how to keep it up to date with the last software
* An overview of the types of attacks that employees may be at risk of such as phishing attacks, malware, brute-force, keylogging, etc.
* Education on password management on what the minimum requirements are to ensure that staff members are not using a password that would put the company’s information and data at risk (e.g., minimum character length, special characters required, etc)
* General overview on how to access the company VPN while working from home on their personal devices
* Advising staff on how to setup & install the multi-factor authentication (2FA) to access company applications
* Outlining the risks & dangers of utilising external devices such as USBs in personal devices, and what policy is in place if an external device is required (Company issued encrypted USBs)
* General overview of company policies in regards software installations and keeping them up to date, returning devices or uninstalling applications, etc.

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

Methods that will be utilized to measure how often employees are not behaving according to the preferred behaviour will be through surveys/questionnaires of employees that opt to utilise their personal devices to access company information/data. Every quarter, those employees that opt to use their own personal devices will be issued a mandatory eLearning to ensure that they’re up to date with the company policies on how to mitigate potential risks and will need to achieve a 100% score to meet minimum requirements.

The results of the eLearning will provide information of which staff were able to pass the module, how many attempts were required to achieve 100% rating, which topics or questions were staff members having the most issues with. This information will be utilised to improve upon the training that is required to ensure that staff members remain educated and up to date on the potential risks they may encounter of cyber security breaches, and what is the preferred behaviour when utilising personal devices to access company information.

**Bonus: Other Solutions**

Training alone often isn't the entire solution to a security concern.

Indicate at least two other potential solutions. For each one, indicate the following:

**Solution #1: Data Encryption to encode company data**

What type of control is it? Administrative, technical, or physical?

* Technical

What goal does this control have? Is it preventive, deterrent, detective, corrective, or compensating?

* Preventive

What is one advantage of each solution?

* The advantage of utilising data encryption is that it will add a secondary layer of depth of defence in the event of a security breach as the company data will be encoded with encryption which ensures its protection against cyber-attacks without the SSH key.

What is one disadvantage of each solution?

* The disadvantage of implementing data encryption is that it may require Silvercorp to make a large investment in their security as encrypting all company can become quite costly as the systems currently in place will need to have the capacity and upgrades in order to perform such tasks

**Solution #2: Strict Usage Control policies to enforce what applications & websites employees can download/visit on their personal devices**

What type of control is it? Administrative, technical, or physical?

* Administrative

What goal does this control have? Is it preventive, deterrent, detective, corrective, or compensating?

* Deterrent

What is one advantage of each solution?

* By executing strict usages controls for employees using personal devices, this will safeguard employees from accessing unauthorised websites/applications that could contain malware that can potentially infect the company network

What is one disadvantage of each solution?

* Implementing strict usage controls is an added expense for Silvercorp, and it can be a difficult to analyse the cost versus benefit for usage controls over certain applications and websites that employees may regularly visit on their own personal devices

References

N-able, 2021, *The Top 7 Risks of Bring Your Own Device (BYOD) MSPs Should Remember,* Retrieved March 23rd, 2022, <https://www.n-able.com/blog/the-top-7-risks-of-bring-your-own-device-msps-should-remember>

Suzanne Kvilhaug, 2021, *Chief Information Officer*, Retrieved March 24th, 2022, <https://www.investopedia.com/terms/c/cio.asp#:~:text=A%20chief%20information%20officer%20(CIO)%20is%20the%20company%20executive%20responsible,increased%20in%20popularity%20and%20importance>.

Micke Ahola, 2022, *12 Essential Security Awareness Training Topics for 2022,* Retrieved March 25th, 2022, <https://blog.usecure.io/12-security-awareness-topics-you-need-to-know-in-2020>

Melody Bernhardt, 2022, *BYOD: How your business can address the 5 biggest vulnerabilities,* Retrieved March 23rd, 2022, <https://ccbtechnology.com/byod-5-biggest-security-risks/>

Australian Government Business, 2021, *Protect your business from Cyber threats*, Retrieved March 23rd, 2022, <https://business.gov.au/online/cyber-security/protect-your-business-from-cyber-threats>

Spam Laws, 2022, *Data Encryption Pros and Cons,* Retrieved March 26th, 2022, <https://www.spamlaws.com/pros_cons_data_encryption.html>