Homework 2 Assignment
Assessing Security Culture

There are many potential security risks in allowing employees to access work information on their personal devices. A few of those risks include phishing, malware, and having their devices lost or stolen. Phishing is dangerous on their own devices because employees' devices are not always the most secure. If they were to open a suspicious email and then log onto a work account that has confidential information on it, the company could be vulnerable to an attack. Another security risk would be malware. Malware is gaining popularity due to a lot of employees working remotely due to the pandemic. All companies do not provide their employees with proper work equipment so they have to use their devices. Many employees use their personal zoom, slack, and even Facebook messenger to communicate with their team members and this provides hackers with ample opportunities to gain access to confidential information. The third risk is someone having their property stolen or even misplaced. This is dangerous because most people store their passwords and other personal information on their note applications and this can lead to major financial loss if someone were to pick it up and go through it.

The preferred behavior for someone to keep their personal information safe on their devices would require an application backed by Multi-Factor Authentication to make gaining access more difficult for the hacker. Also, for the employee to use different passwords for every account they have, so it will be harder to gain access to the information. The preferred behavior to prevent employees from phishing attacks would be to give the employees proper training on how to identify these types of emails and what to look out for. Preventing lost or stolen devices is rather difficult. Still, we can be sure that the employees have the latest firmware installed and have a strict policy on what applications the employee can have when conducting work-related activities.

I would use a few methods to maintain this by doing routine checks of the employee's social media accounts, and inspecting phones and computers once a month to make sure everything is up to date with the best malware protection software. I would also check to make sure that the latest firmware is installed so that the security features will be up to date as well. The main goal for this is to have at least 90% of people following the guidelines we set in place and keep up to date with new ways that hackers are penetrating systems and hiding information in emails.

The people that should be involved in this are the human resources department, software companies, the management team, the chief information officer, and the chief risk officer. The human resources department would keep a record of all the employees and the devices they are using to keep track of where our data could be accessed. Software companies would give us access to the latest software and updates to keep our data secure. The company would also create a checklist to help employees make install the software properly and how to keep it updated to the latest version. Management of the company would be vital in making sure the proper procedures are being followed. They would also supervise the employees to ensure they are not performing any suspicious activities. Monitoring the company data would be done by the chief information officer. The chief information officer would also keep track if there were

any potential threats throughout the company. Addressing the risks associated with hackers would be done by the chief risk officer. The risk officer would also keep up to date with new ways systems are being penetrated.

Training Plan

Introduction:

We will be learning about the importance of keeping your data safe, how to avoid opening suspicious emails, and also the plan of action when one or more of the devices that are being used come up lost or stolen. The training will consist of both in-person and online with the use of tutorials. This will run the course of the employee's employment and will be updated frequently due to the industry ever-changing.

Learning Objectives:

- Approved devices to use for workplace
    - Any smartphone that can have software installed
    - Laptops or desktop computers with antivirus software and the ability to be updated to have the latest security software.

This is important because the use of personal devices for work-related activities is inevitable and for there to be less chance of data being exploited, the employees must have the most updated devices.

- Latest antivirus software installed, how to install it on different devices, and how to keep everything up to date

This is important because without these items the devices would be unprotected.

- Know what phishing, malware, trojans, and password attacks are.

* This is important to know because if someone doesn't know where it begins then there's no way to prevent it from happening.*

- Learn the different ways hackers try and send suspicious emails, what to be on the lookout for and how to know they are being sent from a trusted source.

It is important to know this because emails are an easy way for hackers to gain access to important information and steal confidential information.

- How to keep passwords safe and what not to do such as sharing them with others and having the accounts be logged in automatically when accessing different sites.

This is important because it's an easy way for hackers to gain access to the accounts.

Training Goals and Outcomes:

Training will be ongoing throughout employment as new ways that hackers are gaining

access to systems are always changing and getting more sophisticated. The goal of this training is to provide all the useful information on how to protect your data as well as confidential company information.

Evaluation:

There will be a short answer quiz following the training course. Every few weeks, we will send out a mandatory checklist to make sure everyone is still in compliance with software updates and knows the different things that have to be done to keep their information secure. We will also send out weekly reports about the new ways hackers are gaining access to devices and what to be on the lookout for.

Other potential solutions:

Providing employees with their own approved devices would be beneficial because this would allow them to separate their personal information and work information and the company will be able to control what is being accessed by them. The employees could also leave the equipment at work. This would be a physical control because we can control what is being accessed and make sure that the proper software is installed and updated. An advantage of this would be our data will be more secure and the chance of confidential information being leaked would greatly be decreased because the employees won't be accessing the information outside the company on unsecured networks. One disadvantage of this would be it would be costly to implement.

We could also create a list of applications that are not permitted to be installed on these devices due to potential security threats. This would be an administrative control. The goal of this would be to deter users from suspicious applications that could leave the device vulnerable. An advantage to this would be all the data and confidential information would be secure but a disadvantage would be an application that the consumer wants could be unavailable to download.

Citations:

"Fake News and Cyber Propaganda: The Use and Abuse of Social Media." *Fake News and Cyber Propaganda: The Use and Abuse of Social Media - Wiadomości Bezpieczeństwa*, https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media.

Gurr, Sarah. "Your Training Agenda Template and When to Use It." *Lunch Rush*, 7 Aug. 2017, https://www.ezcater.com/lunchrush/office/training-agenda-template-use/.

Jones, Dan. “3 BYOD Security Risks and How to Prevent Them.” *SearchMobileComputing*, TechTarget, 4 Jan. 2022, https://www.techtarget.com/searchmobilecomputing/tip/3-BYOD-security-risks-and-how-to-prevent-them.

N-able. “Top 7 Risks of Bring Your Own Device (BYOD) - N-Able.” *N*, 1 Oct. 2021, https://www.n-able.com/blog/the-top-7-risks-of-bring-your-own-device-msps-should-remember.