**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 defenses.

**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 a number of security implications.
* You must research these security risks and use the security culture framework to develop a plan to mitigate the concerns.

**Instructions**

Compose the answers to the following four steps in a Google Doc.

**Step 1: Measure and Set Goals**

Answer the following questions:

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.

Employees not following the company’s BYOD security policy and the potential consequences. Lost or stolen devices. Unsecure Networks being accessed (Wifi Hotspots). Potential malicious Apps installed on employee devices unknowingly. Unsecure data transfers.

Malware – attackers can use malicious apps to infect the system with something as serious as ransomware.

Physical Attack – with the theft of an employee’s personal device the company’s intranet can be accessed even if the employee followed proper procedures with passwords.

Hacking – personal devices often lack strong data encryption capable of keeping determined outside actors from snooping on your device when connected to an open WiFi hotspot potentially compromising the users web activity, usernames, and passwords. Man in the middle, snooping, etc.

1. Based on the above 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.

Preferred behavior is that employees follow the companies BYOD guidelines such as installing a Mobile Device Management program to allow the company to protect the company’s security and by refraining from accessing the internet from public or open WiFi hot spots.

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.

You could conduct a survey to determine how many employees connect to the internet by using Open or public WiFi hot spots. The MDM program should allow you to verify additional information as well as checking to see who has accessed the system on personal devices without having the MDM program installed.

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.

100% compliance for anybody using a personal device connecting to the companies network must have a MDM program installed onto that device to be granted access.

**Step 2: Involve the Right People**

Now that you have a goal in mind, who needs to be involved?

* Indicate at least five employees or departments that need to be involved. For each person or department, indicate in 2-3 sentences what their role and responsibilities will be.

**Chief Executive Officer (CEO)**

* The CEO is responsible for plotting the overall direction of the company and conceiving and communicating a corporate mission or ultimate goal, determining what the business should focus on in order to meet those goals, assessing risks, and setting standards of social responsibility for the organization.

 **Chief Operating Officer (COO)**

* The COO is responsible for ensuring business functions operate effectively day-to-day, monitor day-to-day operations, keeps the CEO aware of significant achievements and setbacks, and oversees people management (hiring, promotion, firing).

 **Chief Financial Officer (CFO)**

* The CFO is responsible for charting and monitoring the company's financial trajectory, in other words, they are ultimately responsible for budgeting, which helps ensure that the company uses its funds wisely.

 **Chief Information Officer (CIO)**

* The CIO is responsible for developing IT systems that support the business including setting up corporate networks, provisioning services like VPN, setting up and recycling employee devices, and ceasing servers for data storage and internal application development.

 **Chief Information Security Officer (CISO):**

* The CISO is responsible for managing risk to an organization's data throughout its lifecycle. This means they are responsible for ensuring that the company's data is safe from the time it's collected to the time it's stored and retrieved.
  + Other responsibilities include: overseeing a security operations organization, which identifies, contains, and responds to threats, developing and disseminating information security policies, developing and disseminating training to personnel, working with the CIO to coordinate implementation of security policies by IT teams.

**Step 3: Training Plan**

Training is part of any security culture framework plan. How will you train your employees on this security concern? In one page, indicate the following:

* How frequently will you run training? What format will it take? (i.e. in-person, online, a combination of both)

Conduct a mandatory online training that must be completed before an employee can use their own personal device. Training is mandatory any time they choose to change which personal device they use (ie new phone etc). Also make the training mandatory bi-annually so that if any new challenges to security arise those can be covered.

* What topics will you cover in your training and why? (This should be the bulk of the deliverable.)
* Acceptable use: what applications and assets are employees permitted to access from their personal devices?
* Minimum required security controls for devices
* Company-provided components, such as SSL certificates for device authentication
* Company rights for altering the device, such as remote wiping for lost or stolen devices
* **1. Outline appropriate uses**
* Specify when and how employees can use their devices. List which programs they can use to access and work on company documents. Detail any programs or uses that are not permitted in the office.
* **2. Detail acceptable devices**
* State which devices are permitted for BYOD use. Perhaps you will allow personal smartphone use but require employees to work on company computers. You could also give the option of using their own device but provide company-owned technology if they prefer it. Outline which operating systems and device models are compatible with the programs and apps that you require employees to work with.

## **3. Registration**

After adding the mobile devices to an inventory and deciding which of them are eligible to access the enterprise network, there must be a registration procedure. The enterprise IT department may choose to develop this software in-house, though most will find a it easier to use a [Mobile Device Manager (MDM)](http://searchmobilecomputing.techtarget.com/definition/mobile-device-management) package to support this process.

Since guests will have devices that missed the inventory portion, they will have a much shorter registration process and much more restricted access. Many organizations will require a signed Acceptable Use Policy (AUP), grant them access to a designated wireless LAN (WLAN) and direct all traffic to a proxy server to limit access and bandwidth.

Using the inventory information and following steps in the procedure, the remaining users should be able to complete the tasks required to begin access. Those steps will include:

* Login
* Password
* Authentication code
* VPN setup

## **6. Tracking**

* Keeping track of mobile device uses and usage improves the accuracy of traffic estimates as well as bandwidth planning. With the tools already in use above, enterprise IT staff will be able to track the activity of individuals, groups of users, applications, classes of applications, and also provide security input similar to Intrusion Detection Systems (IDS).
* Knowing where mobile users are going and what they are doing in the enterprise network makes proactive network troubleshooting, network planning, and infrastructure adjustment more accurate and effective.

## **12. Revocation**

* There will come a time that the mobile device (or the user) will need to have access revoked. In the case of the user, it could come from an AUP violation or departure from the enterprise or changing jobs in the organization. With the monitoring, tracking, and logging of each device, it is much easier to know if data may be stored on the device and to what extent so a limited wipe of enterprise data and configurations may be all that is required before user departure.
* With the mobile device, there could be major damage, or it may have been stolen, or even just lost. A full remote wipe of the device, with confirmation, is the best solution, and it should happen as soon as it can be done.
* After you’ve run your training, how will you measure its effectiveness?

Monitor access to your Intranet and ensure that only devices with proper security qualifications and that are registered with the company are in use. Make MRM mandatory for BYOD use.

This portion will require additional outside research on the topic so that you can lay out a clear and thorough training agenda.

**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:
  + What type of control is it? Administrative, technical, or physical?
  + MRM technical, dual authentication
  + What goal does this control have? Is it preventive, deterrent, detective, corrective, or compensating?
  + Deterrent/corrective, preventitive
  + What is one advantage of each solution? Physical loss of property or termination of employee can be easily addressed. More secure log in access.
  + What is one disadvantage of each solution?
  + Employee satisfaction, time requirement to log in.

**Submission Guidelines**

Submit this homework assignment in a Google Doc.

* You can submit all four steps in the same document. Make sure that anyone can view and comment on your document.
* Title your document with the following format: [Your Name] Unit 2 Homework
* Submit the URL of the Google Doc in Bootcamp Spot.

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.