Jessica Sanchez

11/4/20

Week 2 Homework: Assessing Security Culture

Step 1: Measure and set Goals

1. Three examples of potential security risks from allowing employees to access work information on their personal devices (BYOD) are:
    a. Device security & OS updates - Plenty of vulnerabilities are found on devices like cell phones and personal computers and are exploited using techniques like Malware infections, Zero-day attacks, and ransomware attacks. These exploited attacks can all lead to issues like lost or stolen; confidential company data, account information, personal information, and can even lead to server breaches.
    b. Lost or stolen devices - Lost or stolen devices are a major concern, because a user can "jailbreak" or "root" their device, which allows them full access to the system directory, and the ability to make changes to their operating system.
    c. Unsecured wi-fi & internet connections - An unsecured Wi-Fi connection is one that utilizes no security encryption whatsoever. A major risk of connecting to an unsecured Wi-Fi connection comes from using services that require login information. Data transmitted over unsecured Wi-Fi can be intercepted by third parties.
2. The preferred employee behavior when it comes to the listed above scenarios would be:
    a. If employees are using their own personal devices for company business, then they should be required to confirm that the OS & security updates are set to automatically update.
    b. If employees are using their own personal devices for company business and it was lost or stolen, then they should have to report this issue to the company within 24 hours, so that sensitive company information can be remotely deleted.
    c. If employees are using their own personal devices for company business, then they should be following company guidelines when it comes to the use of unsecured wi-fi and internet connections.
3. The methods I would use to measure how often employees are currently not behaving according to the preferred behaviors are; Graphic rating scales - Use of sequential numbers, such as 1 to 5, to rate an employee’s relative performance in specific area, 360-degree feedback - opinions and assessments of an employee from the circle people in the company with whom they work with. Self-Evaluation - ask an employee to evaluate their own performance. Checklists - a simple yes - no.

4. The goals that I would like the organization to reach regarding these behaviors are; a. 100% of employees that have access to company server information, are to turn in an agreement to update their devices regularly, b. Lost or stolen devices are to be reported within 24 hours of the incident, then a three month waiting period for a company issued replacement. In the meantime, they will have access to the company's facilities for work. c. Unsecured internet connections should not be used when accessing company servers. Less than 1% of employees should be accessing company information through unsecure methods.

Step 2 Involve the Right People

Five employees or departments that need to be involved to achieve these goals:

1. Chief Executive Officer (CEO) - is responsible for plotting the overall direction of the company. The CEO reports to the Board of Directors. This group is elected by shareholders and holds the CEO accountable for meeting their demands.
2. Chief Financial Officer (CFO) - charts and monitors the company's financial trajectory. The CFO helps ensure the compacies uses its finances wisely.
3. Chief Operating Officer (COO) - ensures a business is able to function effectively day-t0-day. Typically reports directly to the CEO.
4. Chief Information Security Officer (CISO) - Manages risk to an organization's data throughout its lifecycle.Typically reports directly to the CEO.
5. Chief Information Officer (CIO) - Develops IT systems that support the business. Typically reports to the CEO.

Step 3: Training Plan

Mandatory training is advice for all levels of employment. Frequently training will vary according to departments.

1. Executives Roles: Advice to complete 20 hours of training at hiring and annually thereafter, both in-person and online.
2. Department managers: Advice to complete 20 hours of training at hiring and quartarly, both in-person, and online.
3. Normal employees: Advice to complete 20 hours of training at hiring and quarterly thereafter.
4. All employees will attend 4 hours of soft in-person training focused on company security annually.

The topics that will be covered in training will vary according to employment roles.

1. Executives Role: Training includes, but no limited to;

a. Leading by example in developing a security-focused culture. It will be up to the executives roles to instill natural transition into a safety focus environment, by communicating to all levels, by email or posters, the importance of a diligent secure environment.

b. Empowering employees in making good practices, habits and routines. This training will teach them how to protect the company when using technology so there's no guessing about what security steps should be taken.

c. Expand awareness and get everyone on the same page to reduce threats. These security training sessions are designed to train on real-life threats and employees need to be up-to-date on the cybersecurity dangers they could be exposed to. Security should be cohesive across all departments and no variance in any practice of company policies.

2. Department managers: Training includes, but no limited to;

   a. Leading by example in developing a security-focused culture. It will be up to the executives roles to instill natural transition into a safety focus environment, by communicating to all levels, by email or posters, the importance of a diligent secure environment.

   b. Empowering employees in making good practices, habits and routines. This training will teach them how to protect the company when using technology so there's no guessing about what security steps should be taken.

   c. Expand awareness and get everyone on the same page to reduce threats. These security training sessions are designed to train on real-life threats and employees need to be up-to-date on the cybersecurity dangers they could be exposed to. Security should be cohesive across all departments and no variance in any practice of company policies.

   d. Enabling employees to report problems easily - Empowering employees to become active players in the company security efforts, by removing any barriers to reporting suspicious events.

3. Normal employees: Training includes, but not limited to;

   a. Role-play training on cybersecurity concerns, for example, employees walk through security-related cases and decide how to solve certain problems in alignment with company policies.

   b. Explaining protocols for reporting, and acting behaviors in accordance with company policies.

   c. Encourage good behavior, camaraderie, and diligence in the promotion of security.

After running training the effectiveness would be measured by; evaluating learners reaction to training in completing surveys, use assessment to measure what was learned during training before and after, assess whether or not behavior has changed as a result of training by observations and comparing 360 degree reviews , and evaluate the impact of your program on business results by applying methods like Kirkpatrick's model for good results.