Governance Risk Compliance

By Zabien McKee

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.**

    a. The employee's personal device can be infected with some sort of malware or spyware that has the potential to steal company data.

    b. Due to employees not being able to service their machine with the company IT department, they are vulnerable to social engineering phishing attacks, such as calling a fake tech support company.

    c. The employee's device probably doesn't have the same security software and may be lacking basic important things like an antivirus or a properly setup Firewall

2. **Based on the above scenario, what is the preferred employee behavior?**

    - Employees should have strong passwords that are changed on a regular basis and have Two Factor Authentication set up on all devices that they intend to use for work.

    - Employees should regularly update their devices to ensure they have the latest version of their operating system so they are less susceptible to operating system vulnerabilities.

    - Employees should be careful when downloading suspicious files, knowing that they are not the only ones who have the potential to lose important data in the event of a cyberattack.

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

    - Create a system where if an employee wants to use their device for personal use they need to report every time an account on their device(personal or not) gets breached and track how often certain employees get their accounts compromised for re-education purposes

    - Have a program on the device report the system information that you could then track how often it gets updated. Use that information to inform employees when their device falls too far behind

    - Perform a phishing campaign in your organization to see how many employees download from the suspicious link.

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

    - Every Employee shouldn't have more than 1 breach per 6 months. If any employee exceeds this number, re-education may be in order.

    - 95% of employees should be within a month of the most recent updates

    - Less than 7% of employees should click on the link

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.**

- **Outside Cyber Security Team** - Will send out the phishing email to all of the employees in an attempt to gauge how many people click the link. They will report their findings to Administration and IT directly.

- **IT Department** - They are in charge of either creating or finding the Operating Monitoring software, as well as keeping up the Phishing Email ruse as long as required.

- **Administration** - They will determine the budget for the testing, create the reporting for account compromisation and add a line into the general employee contract saying if you want to use the personal device, you have to use the company operating system tracking software.

- **Human Resources** - They would be in charge of managing any and all complaints put in by disgruntled employees who feel that they have been rudely tricked by the Phishing campaign. They would also deal with employees who are unhappy with the new monitoring policy

- **General Employees** - They would be in charge of implementing all of the information gained from the bi yearly trainings, as well as coping with the new changes to personal device usage in the company

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)**

  Every three months I would run a set of training sessions involving half of the staff, so every year all staff receive Cyber Security trainings twice a year

- **What topics will you cover in your training and why? (This should be the bulk of the deliverable.)**

  Topics would cover:

    - Basic Internet Safety
        - Firewalls
        - Antiviruses
        - Good Internet habits
            - Not clicking suspicious links
            - Only visiting HTTPS sites
        - Two Factor Authentication and Why you need it
    - Phishing
        - What is Phishing? Why is it dangerous?
        - Display Results of phishing campaign targeted against the employees and discuss the results
        - Talk about dangers of downloading suspicious email attachments
    - Malware/spyware
        - Go over basics of what these forms of malicious programs can do and how they get distributed
        - How to protect against malware
    - Ransomware
        - Talk about what exactly ransomware is
        - Perform a live demonstration of a Virtual Machine getting infected by Ransomware
        - Discuss Safeguards to protect against it, frequent local backups to external devices, frequent cloud backups, etc.
    - Operating System Security
        - How OS breaches are found and occur
        - The importance of keeping your device up to date

- **After you've run your training, how will you measure its effectiveness?**

  I would re-run the phishing campaign and see how the employees would fare after new training. I would also check the OS Monitoring software to see how the average last update for devices changes with the training.

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?**
  - **What goal does this control have? Is it preventive, deterrent, detective, corrective, or compensating?**
  - **What is one advantage of each solution?**
  - **What is one disadvantage of each solution?**