**## GRC Homework: Assessing Security Culture**

This week we learned about security culture and to promote it within their organizations. It’s important that employees are aware of common security risks and treat security seriously. The majority of cyber attacks aim to exploit human weakness via methods like phishing. People are the weakest link in an organization’s security defenses.

For this unit’s homework, you will analyze the following security concern:

- 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 numerous security implications. In this week's assignment, you will research these security risks and develop a plan to mitigate the concerns.

Using the Security Culture Framework, you will develop a plan to combat this concern. Below are the deliverables for this week's assignment.

**### Deliverable 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.

**1. Phishing Attacks  
2. Malware Infiltration**

**3. Device Loss or Theft**

1. Based on the above scenario, what is the behavior that employees should engage in? For example, if the issue was that employees were downloading suspicious email attachments, you would want people to download attachments from only trusted sources.   
  
**- Employee BYOD Access Policy Training  
- Whitelisting and Blacklisting  
- Data Encryption**

1. What methods would you use to measure how often employees are currently not behaving accordingly? For example, if the issue was that employees were downloading suspicious email attachments, you can conduct a survey to see how often people have engaged in this behavior.  
 **- Think through and test your BYOD policy before rolling it out company-wide.  
- Take inventory of every employee device accessing your network.  
- Conduct periodic audits of your BYOD policy.**

1. What is the goal that you would like the organization to reach regarding this behavior? For example, if the issue was that employees were downloading suspicious email attachments, a goal would be to have less than 5% of employees engage in such behavior.   
  
**- The goal is to have less opportunities for Data Theft, Malware Infiltration, and Potential Legal Issues, at the same time increasing productivity and cost savings.**

**### Deliverable 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.   
  
**- CEO, CIO, & CISO informs HR with the BYOD policy and makes sure it’s implemented and being followed accordingly, HR makes all employees sign a legal document ensuring the following departments follow the BYOD policy. The IT department makes sure and keeps track of what needs to be approved and conducts tests, surveys, and training for the company.**

**### Deliverable 3: Training Plan**

Training is often 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 modality will it take? (i.e. In-person, online, a combination of both?)  
  
**- HR will send a corporate email regarding the BYOD access policy and signing.  
- IT department will conduct training for those who keep failing to comply, and will do online and in-person training depending on availability of employees, at least every 6 months, updating them about new Threats, updates to the Policy, Risks and Vulnerabilities the employees might encounter.**

\* What topics will you cover in your training and why? This will be the bulk of the deliverable.   
  
**- Productivity and Freedom if they do choose to work from home.  
- Current or Upcoming Risks and Vulnerabilities.  
- Legal Issues and responsibilities they might face.  
- Penalties for not complying with the BYOD access policy.**

\* After you’ve run your training, how will you measure its effectiveness?  
  
- IT Department will survey and collaborate with a penetration testing company, keep track of those who don’t comply thru logs and have them go through re-evaluation if they are willing to go through re-training, have random checks at random times.

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

**### Deliverable 4: Other Solutions**

Training alone isn’t often the solution to a security concern. Indicate at least two other potential solutions. For each one, indicate the following:  
  
**- Application Installation Control  
- Containerization**

\* What type of control is it? Administrative, technical, or physical?   
 **- Administrative (Application Installation Control), making sure policy is always being followed.  
- Technical (Containerization) , having the IT department setup compartmentalization or segregating portions of the employee’s device.  
- Physical (Application Installation Control & Containerization), have the IT department check if their devices are secure enough and is following the BYOD access policy.**

\* What goal does this control have? Is it preventative, deterrent, detective, corrective, or compensating?   
  
**- Application Installation Control (Preventative, Deterrent)  
- Containerization (Preventative, Deterrent)**

\* What is one advantage of each solution?   
  
**- Application Installation Control (Work Productivity)  
- Containerization (Work Productivity)**

\* What is one disadvantage of each solution?   
  
**- Application Installation Control (Infringement on personal freedoms)  
- Containerization (Doesn’t protect the employees’ personal data)**

**### Submission Guidelines**

Submit this homework assignment in a Google Doc.

- You can submit all four deliverables within this 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 link to BCS.

---

&copy; 2020 Trilogy Education Services