## **Assessing Security Culture**

### **Step 1: Measure and Set Goals**

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.

|  |
| --- |
| Malware: a lot of apps, even if the user does not realize it, will access your contacts, media, and files. Having work information on your personal devices can allow malicious software to get into work information.  Disgruntled Employee: If an employee gets fired or is upset it only makes that employee have easier access to information for a longer period of time. It is easier to steal the information and expose it.  Stolen Hardware: A person is more likely to just bring their personal phone to a public event. If a phone with work information gets lost or stolen, not only the device is stolen but the data with it. |

1. Based on the previous 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.)

|  |
| --- |
| 1. Malware: users would be more considerate of what they are downloading. They would also run anti-virus software on a regular basis as well as have active firewalls on devices. 2. Disgruntled Employee: agree for the company’s security to wipe all work information off your personal devices and not steal or manipulate any information. 3. Stolen Hardware: limit the amount of devices a person has with work information on it as well as keep it separate from the user's personal devices. |

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.)

|  |
| --- |
| 1. Piggybacking: set up a camera, set up a detection device to compare people walking through compared to number of badge swipes 2. Phishing attacks: calculate how many people open links sent from a suspicious email 3. Private networks: see where people are accessing the network from (are they accessing at home, in the office, or at a Starbucks. 4. Logins: count how many accounts login to particular system (if 20 people have access, are only 20 people logging in and are all keystrokes recorded) 5. Education: conduct a survey to ask basic security questions. Do they know not to Piggyback, use public networks, use personal devices and the risk that poses? |

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.)

|  |
| --- |
| 1. Piggybacking: only allow one person through per sipe of badge. 2. Phishing attacks: reduce the amount of opened suspicious links as possible 3. Private networks: only have employees have access through approved and private networks 4. Logins: only the people that are currently working in an area have access to it. 5. Education: have regular mandatory training especially with new hires to keep the company safe as well as establish guidelines an employee must adhere to when departing the company. |

### **Step 2: Involve the Right People**

1. List at least five employees or departments that should be involved. For each person or department, describe in 2–3 sentences what their role and responsibilities will be.

|  |
| --- |
| 1. Human Resources: They should teach people on basic security measures the company expects. This includes asking any questions people may have. They also have a huge job of onboarding and offboarding and following proper procedures. 2. Accounting/Finance: When it comes to hackers, most of the time it is money what they are after. Keeping finances safe is of the utmost priority. The right people should have access and more than one person should oversee where money is moving to and from. 3. IT/Security: They should help with setting up new devices and develop logins to access certain areas. They should be the backbone when something technology related fails or poses a risk. 4. Marketing: They need to have a firm understanding of what information can be shared and what cannot. Their job is to make the company look good and let people know of the services the company provides without exposing secrets. 5. Operations: They have a hard job of making things more efficient without compromising security. They need to work with the security team on how to reach this goal. |

### **Step 3: Training Plan**

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

|  |
| --- |
| There should be mandatory training for all new hires before they have full access to their area. There should also be a training I would say every 6 months, even if it is just letting people know of the news of what hackers are attempting to do next. Online training is the best training so nothing is missed. I also do think some in-person training is good, especially when it comes to security of one of many buildings, accessing highly secured areas in the office, etc. |

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

|  |
| --- |
| I would cover the importance of piggybacking into the building, how and where to access company information, the importance of passwords, updating login credentials every so often, phishing attempts, downloading or clicking dangerous links, the importance of firewalls, not using work devices for personal use and vice versa, reporting any suspicious activity, strict onboarding and offboarding process, and more! |

1. After you’ve run your training, how will you measure its effectiveness?

|  |
| --- |
| I would use quantitative and qualitative data collecting information that I expressed in Step 1, Question 3: counting people through doors, setting up cameras, fake phishing attempts, conducting surveys, communicating to the employees, encouraging questions, etc. Any reduction of error is a success. The goal is not perfection but as close as we can get to it. |

### **Bonus: Other Solutions**

1. List at least two other potential solutions. For each one, indicate the following:
   1. What type of control is it? Administrative, technical, or physical?
   2. What goal does this control have? Is it preventive, deterrent, detective, corrective, or compensating?
   3. What is one advantage of each solution?
   4. What is one disadvantage of each solution?

|  |
| --- |
| Make sure all devices are up tp date:   1. This is a technical control. 2. This is preventative. 3. This not only makes more devices more efficient but allows another layer of security. 4. It is more work for the security team and can slow down employees because it takes time to update devices. |

|  |
| --- |
| Develop a response plan.   1. It is administrative. 2. It is a corrective and compensating control if compromised. 3. It prevents panic and gives confidence in employees how to combat being hacked. 4. Hopefully you will never have to use a response plan when hacked but with most companies, either you have been hacked or you just do not know it. |