### 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.

According to Nightfall.ai - Hacking such as man in the middle attacks, malware attacks, and data leakage due to unprotected devices are the biggest security risks when it comes to employees using their personal devices. Hackers can take advantage of the unsecured devices, networks and malicious apps to mine for company information.

2. 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.

Employees should only download email attachments from trusted source and always confirm with someone if they feel like the file may be malicious.

Employees should also avoid using open wireless networks such as cafe wifi if they intend to access any company information.

Employees should always use company provided hardware (if provided) to access any work information or use the company VPN network to access the information.

Employees should never download sensetive company information to their personal devices.

If employees do use their personal devices they must have the most up to date security for OS and an up to date anti virus.

3. 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.

Keep an IP log of when a file was accessed and where it was accessed from

Keep a log of what kind of devices were used to access the files or servers.

Conduct a test to see how many employees download email attachments without looking it over.

4. 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.

The goal is to have no employees using personal devices to access company information. Employee's must use company provided hardware to access work related material. Another goal is to have less than 5% of employees downloading email attachments from unknown sources.

The company will aim to host training seminars to inform employees of how to prevent hackers from getting company information.

#### 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.

1. CEO:

There are 3 main roles and responsibilities for a CEO to cover off, first off its:

Governance:

The CEO would hire the CISO or appoint someone into that role. The CEO would work with the CISO to maintain a strategy to the company's cyber risks using industry standards and guidelines

The CEO would ensure that the CISO has a direct line of communication to relay threats to the board.

Lastly, The CEO would make sure the security policies, standards, and behaviour enforcement and procedures are consistent with all departments and businesses

Risk Assessment and Management:

The CEO would need to establish a risk assessment within the company's risk management and governance processess and would need to work with the CISO on a plan.

Moreover, the CEO would need to analyze the results of the risk assessment for oversight with key stakeholders and the board of directors. In addition, they would overlook the performance of monitoring to stay on top of evolving cyber attacks.

2. CSO:

The CSO would be in-charge of laying down the groundwork of what the training material should include. In addition to, what kind of test will be conducted to determine employee behaviours to certain attacks.

3. CISO:

CISO is responsible for the company's information and data security. The CISO role would be to evaluate the IT threat and create an interface for the program the department would use to analyze threats and KPI's

4. Human Resources: The HR Department's role would be to conduct the required training with all business departments of the organization and to ensure that all employees have received the mandatory training of the new cyber security policies put in place.

5. IT Department:

The role of the IT department would be to work with the CISO to improve the company's security and to make sure that all company hardware is secured to be able to access company information safely. They would also make sure all computers are fully updated and operational with the most up to date security and anti virus features.

#### 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)

Training will take place in-person during company time to ensure all employees are attentive during the training process.

Training will take place once every 2 weeks and we aim to have 25% of employees trained every 3 months.

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

1. The importance of security and using your personal device

Employees should know the risks the company faces when personal devices are used to access company information.

2. Most common Cyber security threats

To inform the employees of the threats and what to look out for to try to avoid being a victim to an attack and to protect their and the company's data

3. How to secure personal device

Its very important for employees to know how to properly secure their device if they are going to use it to access company information.

4. How to maintain company devices and personal devices

Employees should be aware of any new security updates or software needed to keep their devices up to date and safe from threats

5. New Company policies and rules

The new company polices and rules that the employees will have to adhere - The organization's goals is to lower the threat of cyber attacks thus new rules and policies are put in place that the employees will have to follow.

\* After you’ve run your training, how will you measure its effectiveness?

To start we would monitor the number of security indcidents the organization has experienced after the training to see if employees are following proccesses and procedures they were taught. We would follow this up with an email test to see how many employees download the email attachment and reference that with previous data. We would then conduct a survey to gain insight on what the employees thought about the training and if they would like to add anything or change anything about the training. Lastly, We would have open discussions with the employees if anyone had any concerns about the new policies and procedures put in place.

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:

1. Vulnerability management program

2. Restrict end user access to systems

What type of control is it? Administrative, technical, or physical?

1. Technical

2. Technical

What goal does this control have? Is it preventive, deterrent, detective, corrective, or compensating?

1. Deterrent/Preventive

2. Preventive

What is one advantage of each solution?

1. Be able to identify new vulnerabilities in a system and priotize them based on impact to the business. It allows the business to construct a plan to manage the vulnerabilities.

2. If a user has a virus, limiting his access would also limit the virus's access since most virus can run only as the user that is logged in giving them the same permissions the user does.

\* What is one disadvantage of each solution?

1. Consumes alot of resources for up keep

2. Could slow down users productivity waiting for authorization to access files.