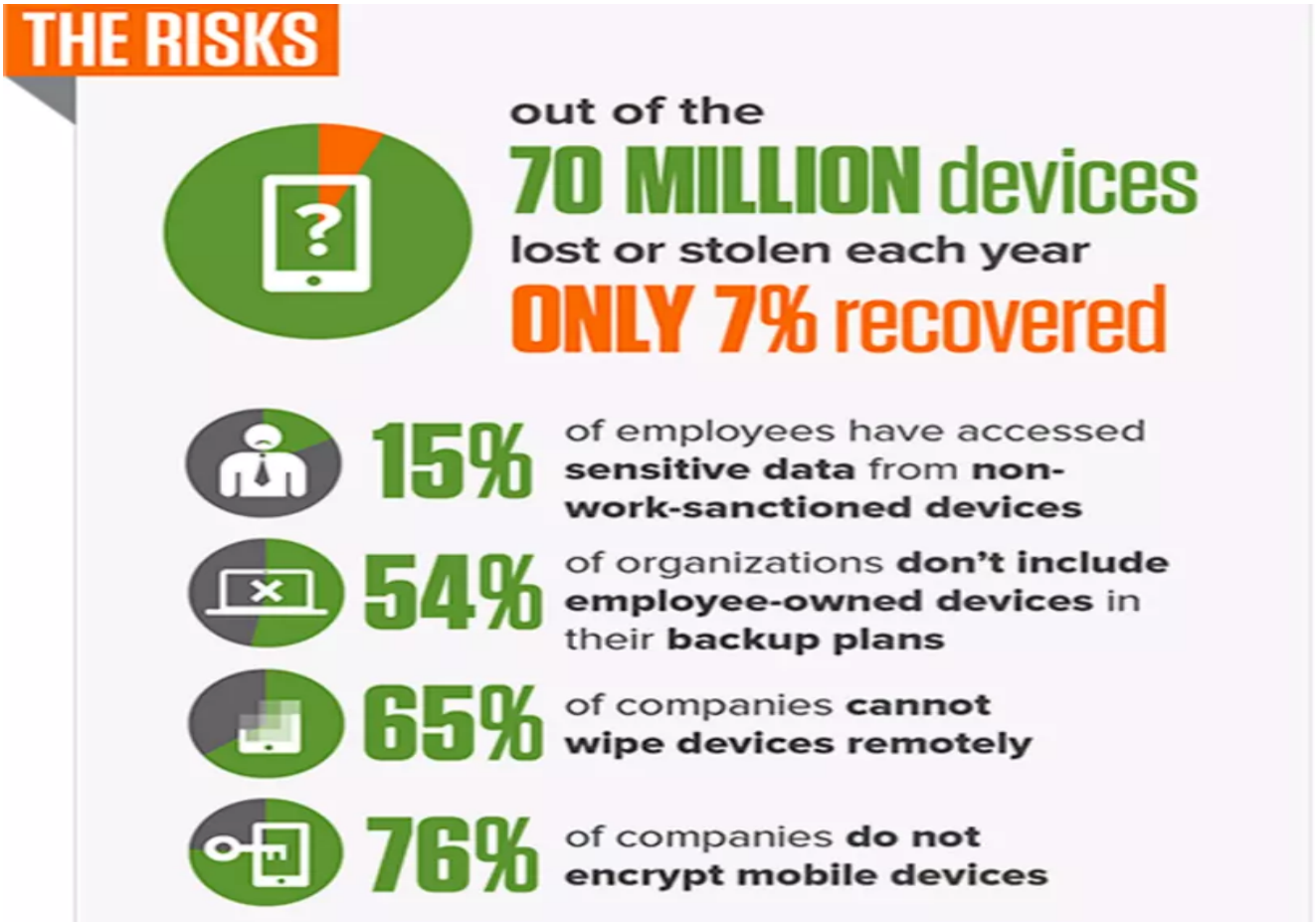
# Assessing Security Culture

**Step 1: Measure and Set Goals**

**Potential Security Risks:**

There are plenty of potential security risks in allowing employees to access work information on their personal devices. Most of them are security related as companies gather exponential amounts of data on their customers and employees. Working on personal devices may seem easier and seem like a more economical choice, however if an employees personal device is compromised, it could cost their company. Let's look at the potential risks associated with using personal devices for work-related tasks.




1) Data Leakage: An employee could physically lose their device or could have malware downloaded on it and all of the company's data is in an attackers hands and they could leak the data collected on the companies servers. Data leakage could tarnish their reputation.
2) Malicious Apps: An employee could have an app on their personal device that is malicious and is sending malware to the company list of employees and customers.

3) Packet sniffing Attacks: The employee could be sitting at a coffee shop conducting a work transaction and an attacker could be sniffing packets through the network connection and could get access to private company data.
4) Logic Bombs: A recent ex-employee could share private company information and data as they have it readily available on their own device.

## Preferred Employee Behaviour:

After looking at the potential risks, if a company does allow employees to continue using their own personal devices, the following should be the preferred employee behaviour in regards to security:

1) Employees' personal devices should be registered with the company and they must use strong passwords on their devices.
2) Employee's should not be using public networks where they could be targeted easily by cybercriminals.
3) Employee's should only open emails from trusted sources and ensure that they are not deceived by emails that look like they have come from authentic sources.
4) Employees should research and only download trusted applications onto their devices in order to avoid downloading malicious applications.
5) They must ensure that all of the data they are using is encrypted.
6) The employee's should ensure that they are constantly updating their devices and firewalls.\
7) The employees should generally understand the reason behind these security protocols and what damages can come out of carelessness.

## Security Checking Methods:

To ensure that all of the employees are following correct behaviour regarding company data security, I would send out surveys which ask whether or not the employee has completed the checklist with all of the tasks from above. I would also send out trick emails and see which employee has opened

the email and also get penetration testing.I would monitor the minor breaches that occur over time by doing security audits so that I could see weather the company's employees are following company protocol.


**Goal:**

The goal regarding the employee's behavior in company data safety is to significantly reduce data theft risk and ransomware risk by at least 35%. 100% of cybersafety assurance is never possible but deterring and prevention is always preferred and is the best mitigation possible.

**Step 2: Involving the Right People**

**Roles and their Responsibilities:**

Essentially, the entire company needs to be involved to ensure that our goal is met in relation to cybersecurity. Although the entire company needs to be involved, it is good to discuss these cybersecurity plans with various employees and departments, so that they could know their role in helping their company become more secure in regards to the employee BYOD policy.

1) **Chief Executive Officer (CEO)**: Their role is to direct the entire company towards success and their responsibility will be to convey the importance of cybersecurity to their employees and communicate the corporate mission of safety while using personal devices throughout the company.
2) **Chief Information Officer (CIO)**: Their role is to oversee the progress of the action plan by setting up a VPN, setting up employee devices, and by helping to check if employees are following the correct cybersecurity protocol placed for them. They will be directly reporting the progress to the CEO.
3) **Chief Information Security Officer (CISO)**: Their role is very relevant to this mission. Their responsibility will be to develop the personal device usage policy and will develop the training methods and oversee them. They will be responsible for coordinating with various departments and the IT department.

4) **Security Operation Center Manager (SOC)**: Their responsibility will be to consistently be checking for data breaches that have occurred or have the potential of occurring and they will be helping the CISO with the personal device usage implications and security training. They will also help in identifying how many employees are not following these policies and preferred behaviours in regards to cybersecurity.
5) **All Employees**: Their responsibility will be to understand the security risks associated with using their own personal devices to conduct company related business. They will participate in the training provided by the company to ensure they are prepared for any possible data breaches and they follow all of the recommended employee behaviour listed in the above section.

**Step 3: Training Plan**

**Training Frequency and Format:**

Training for the new company policies regarding employee personal device usage for work purposes will occur annually and it will be delivered in an online and an in-person format. More than half of employees at Silvercorp use their personal devices to check company messages and about 25% carry work transactions and business through their personal devices. It is possible that 100% of the employees could use their personal devices for work purposes, this means that 100% of the Silvercorp employees will need to be trained. 100% of the employees will receive training in an online format about safety issues regarding personal device usage through modular training sessions and 25% of the employee devices will be pen-tested in each quarter. The employees will need to finish the online safety module course before being approved for randomized pen-testing.

**Topics:**

The main goal for Silvercorp is to maintain security for the company's data and ensure that the servers are not attacked by malicious outside parties. There's an increasing number of Silvercorp employees that are using their personal devices for work purposes. Their personal devices may not be as secure as Silvercorps computing machines which use the highest quality of firewalls and other security implications. The goal for this training is to make the employee's personal devices just as safe as their company's devices. Let us look at the topics that will be covered in the training.

**Malware**: Malware is "hardware, software, or firmware meant to perform an unauthorized process that will compromise the confidentiality, integrity, or availability of a system. Some types of malware are viruses, worms, Trojan horses, or other code-based entities that infect a host". Cybercriminals often send links with downloadable malware in the form of emails, but also can be downloaded through USB sticks. The employees need to understand that malware is easily installed onto devices if they are not careful enough and that it causes considerable damage to their devices and the company's data.

**Ransomware**: Ransomware is a type of malware except with a twist. It is downloaded through malicious links and comprises the system. Once it gets a hold of the systems data, this type of malware encrypts the data and makes it useless. Cybercriminals, then, demand a ransom to decrypt that data. It is easy to understand why ransomware and malware must be avoided at all costs.
**General Data Breaches**: Data holds information which is valuable for any company. Data breaches can result in customers and employee's personal information to be at the hand of malicious attackers. They can release this information which invades the privacy of the attacked parties. Also, company data holds crucial information about their product, services, their financial reports and future plans for the company. This information should not get into the hands of unauthorized parties.
**Implications**: Corporate data is very lucrative and if it gets into the hands of malicious actors, it could be a disaster for Silvercorp. The implications for malware infected devices can ruin the company's server, which could halt any business taking place. Attackers can demand a ransom of millions of dollars, using ransomware, which would be very costly for Silvercorp. If a data breach occurs, the company's reputation would be tarnished and would face multiple lawsuits which could bring Silvercorp to the ground. It is important for the employees to understand these implications which could greatly harm their job security.
**Prevention**: Prevention is key so using strong firewalls, two-factor authentication, strong passwords that are alphanumeric and have symbols will ensure that it is tough for cybercriminals to attack. Other prevention techniques which would ensure cybercrime prevention would be to be aware of one's surroundings, only open emails from trusted sources, not to visit sites starting with http and generally unsecure websites. Malicious apps are to be avoided so employees need to be trained to research the apps that they download onto their devices.

**Results:**

In order to measure the training effectiveness, the information security team will run penetration testing on the employees personal devices. Security audits will also take place at the end of the year. They will also send fake phishing emails and measure how many employees click on them. This will give a good representation of how effective the training was for the employees. In order to ensure that employees fully participate in the training, incentives such as gift cards and longer vacations, will be provided to those who followed the correct security procedures for using their personal devices. This will be a motivating factor to achieve positive results for the training.

**Step 4: Other Solutions**

One solution for this security risk would be to ban employees from using personal devices. This would be a physical control. This kind of solution would have detering qualities. One advantage to this solution would be that it would save financial assets and time from not having training for the new protocols set in place. However, this would cut down on employee productivity because the employees would have to always be physically present to complete assigned work tasks.

Another solution would be to provide corporate owned devices for employees which would have strong firewalls so that the employee does not download unauthorized apps and open unofficial emails. This would be a technical control. This solution would be a preventive one. An advantage of this solution would be that, if an employee is terminated, their personal device would be erased automatically and they would hand back the device to Silvercorp. However this solution would be costly for the company because each employee would have to get a personal device which is equipped with high security software.

# See You In