**NAME: MANASSEH DAVID**

**MATRIC NUMBER: 15/ENG02/036**

**1.**

Mobile device security refers to the measures taken to protect sensitive data stored on portable devices. It is also the ability to prevent unauthorized users from using mobile devices to access the enterprise network. Example. smartphones, laptops, tablets e.t.c.

Mobile devices are among the most vulnerable devices around because they're easily exploited and can be quickly compromised by hackers.

It's essential for a company to have a solid security policy in place for mobile devices. So the company data can be well protected. And this can be done by carry out the following;

**Protecting data at rest**

One of the components of any good mobility policy is how it addresses the protection of "data at rest." This includes all data that is stored on mobile devices. The key here is to encrypt all data stored on any mobile device. enterprises must incorporate policies to address any circumstance where corporate data is stored on a mobile device.

A mobile policy should include a statement that mandates the use of strong encryption on all mobile devices that have the capacity to store data. While some companies may have the ability to enforce this mandate using centrally managed encryption solutions, some may have to rely on users to ensure that data is encrypted. There will be more on policy enforcement in the third tip in this series.

Ideally, the protection of corporate data residing on mobile devices will be enforceable using technology that forces data encryption on all devices that do or could contain corporate data

In addition to the policy clauses that address the encryption of data at rest, organizations should have technology to remotely wipe the contents of a device in the event that it is lost or stolen. For this reason, include a policy clause that makes it clear that any lost or stolen devices should be reported to IT immediately.

**Protecting data in flight**

Mobile devices may connect to several networks that are out of the control of the enterprise IT department. For this reason, it is important to define enforceable policies that dictate proper mobile device connectivity practices. In many cases, technology can force compliance with the mobile policy, but if the infrastructure is not in place to force compliance, enterprises must rely on users to understand and adhere to policy.

**Assigning responsibility**

There are so many questions to ask when developing a corporate mobility policy. The most questions arise around who is responsible for what in the policy. For example, policy creators might ask:

Which mobile devices does the IT department support?

* Can employee-owned devices be used for work, or will all mobile devices be assigned by the company?
* If a mobile device is lost, stolen or broken, what is the process to ensure that the data on the device is/was secure, and at that point, is responsibility handed from the user to the company?
* Does the company have the means and infrastructure to ensure that data at rest and data in flight are encrypted and secure, or is the onus on the employee?

 these questions are examples of what the policy will look like and everyone should adhere to the policy.

**Educate users**

Protecting valuable information assets against mobile security threats requires a firm commitment to training all users of mobile technology. The reality is that the consequences of device theft or misuse are too great, potentially including a breach of the corporate network, the loss or corruption of critical data, and the violation of applicable industry compliance regulations. Because a single security breach could very well exceed the cost of staff training -- as seen with greater regularity in recent news coverage -- educating users on mobile security best practices should be viewed as an effective preventive measure and a prudent investment for the organization.

This training for the users should at least cover Protecting the devices , Data encryption and password management.

**Technical controls**

Technology can help ensure mobile policy compliance in four key ways:

* Forcing encryption of data at rest on mobile devices.
* Forcing secure connectivity on unsecured public networks.
* Ensuring that unauthorized mobile devices do not have access to the corporate network or company data.
* Ensuring that mobile user spending is in line with the mobile policy and that additional costs can be recovered.

**IN Summary;** All mobile devices must be protected by a strong password and must not be disclosed to anyone.If you lose your mobile device or it is stolen, it should be reported immediately.User should not download applications from untrusted sources always verify first before making any download.User should Block potentially dangerous applications.Enable the Remote lock and data wipe option on the mobile device just in case the device gets lost.Follow up safe disposal practices when you dispose your mobile device and ensure all sensitive information are erased/removed completely.

**2.**

**Industrial Espionage:**

Industrial espionage is the illegal and unethical theft of business trade secrets for use by a competitor to achieve a competitive advantage. Industrial espionage is conducted by companies for commercial purposes rather than governments for national security purposes. Industrial espionage may also be referred to as "corporate spying or espionage," or "economic espionage."

**Types of Industrial Espionage**

Industrial espionage can be divided into two types. The first and most common is actively seeking to gather intelligence about a company or organization. It may include the theft of intellectual property, such as manufacturing processes, chemical formulas, recipes, techniques or ideas. Industrial espionage may also entail the concealment or denial of access of key information related to pricing, bidding, planning, research and more. Such a practice is meant to create a competitive advantage for the party who has the information.

Industrial espionage tends to involve "inside jobs," in which an employee steals secrets for financial gain or to hurt the company. It may also be conducted by governments as they pursue economic or financial goals. Less frequently, individuals may break into a company facility to steal documents, computer files or pick through trash for valuable information. More likely, an industrial spy will use the internet to hack into a company's network to gain access to trade secrets on work computers and servers. A relatively new area of industrial espionage involves denying a competitor the use of their information, services, or facilities by way of computer malware, spyware, or a distributed denial of service attack (DDoS). Such industrial espionage tools are helpful in exploiting vulnerable systems.

Performing both types of espionage involves similar goals; gaining access in to the rival company’s system, to achieve this the following steps are taken;

**Social Engineering:**

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the attacker moves to gain the victim’s trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.

**Malware:**

After gathering details from the selected weak link of the company and forming a close relationship for cover, the next step would be to infect their devices with malware.

Malware, or malicious software, is any program or file that is harmful to a computer user. Types of malware can include computer viruses, worms, Trojan horses and spyware. These malicious programs can perform a variety of different functions such as stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users' computer activity without their permission.

**HOW TO PREVENT COMPANY ESPIONAGE**

**Identify Your Companies Trade Secrets**

The first step to protecting a company’s trade secrets is to identify exactly what those secrets are. This not only involves looking inward, but looking outward as well. Firms cannot deduce the true value of their trade secrets until they understand how these secrets stack up against the technology and best practices of their competitors. By properly evaluating their intellectual property, firms will be more able to establish priorities and allocate security resources to better protect their most vital secrets.

**Identify the Threats**

Before firms develop strategies to counter industrial espionage, they need to understand what organizations present the largest threat. For instance, a company’s competitors may pose the most obvious danger. However, it should be kept in mind that visitors, customers, business partners, hackers, activist groups, and even foreign national governments are all potential threats and should be considered when building a counterespionage plan.

 **Ensure Physical Security**

The same measures that are effective against run-of-the-mill criminals are also effective at protecting businesses from industrial spies. As such, firms should ensure the physical security of their offices, equipment, and infrastructure. This means setting up surveillance systems, securing entry points, and hiring or contracting specialized personnel. It is particularly important that firms identify the most sensitive information and facilities and ensure that these are given extra layers of protection.

**Establish Policies for Controlling Information**

In many instances, the unwanted disclosure of secrets could have been easily avoided if firms had simply put more thought into controlling the flow of information. Firms should establish policies on what information employees can share inside and outside the workplace. They should also establish procedures for control, reproduction, and storage of sensitive data. Particular attention should be paid to what is disseminated over the Internet and social media sites. Additionally, firms should develop procedures for the proper disposal of paper documents, IT hardware, and other sensitive equipment.

 **Train the Workforce**

While firms may enact policies on the proper storage, control, and dissemination of information, they also need to ensure that their employees are trained to follow these procedures. Firms should conduct periodic training and awareness campaigns to inform employees about the threat from industrial espionage and the importance of information security.  Employees should understand that the threat from espionage is internal as well as external. As such, they should instruct workers on the correct procedures for identifying and reporting suspicious activity.

 **Compartmentalize Information**

Not all information needs to be accessible by every employee in a company. That is why information should be compartmentalized on a need to know basis. Even senior members of a particular corporation may not need to know every technical detail about business operations. As such, firms should put in place policies to segregate which employees have access to which information, with special attention given to those employees who have access to a company’s most vital trade secrets.

 **Conduct Background Checks and Monitoring**

Firms should conduct a background checks on all employees with access to sensitive data. This may even include often-overlooked individuals such as janitors, caterers, and groundkeepers. Specifically, firms should attempt to identify any possible factors that could make a particular worker more prone to illegally disclosing information. Firms should also continue to carry out periodic security evaluations of their employees even after they have initially been vetted.

**Establish Employee Exit Procedures**

It is critical that business develop comprehensive employee exit policies. From day one, an employee needs to understand the firm’s policies on information security.

This means that all employees should be required to sign a nondisclosure agreement, and be reminded of this agreement upon leaving the firm. Moreover, firms should be aware that most cases of intellectual property theft perpetrated by employees occur during their last month of work. This is why it is important to make an employee’s exit as smooth and resentment-free as possible. Companies may also consider limiting the access workers who are expected to leave the organization in the near future.

**Ensure Cyber Security**

Industrial espionage is increasingly becoming the purview of the cyber realm. Therefore, it is important for companies to maintain robust cyber security frameworks. Even while systems should look outward to protect a company from external threats, they should also look inward. Cyber security professionals should monitor their internal networks to uncover suspicious activity and record the transmission, copying, and accessing of sensitive files. Additionally, firms should consider leveraging specialized software to protect critical information, monitor activity, and prevent data loss.

 **Establish Contingency and Crisis Management Plans**

Even the best-laid plans can go wrong. That is why it is important for companies to develop contingency and crisis strategies in the event of intellectual property theft. Firms should attempt to assess the potential damage caused by the theft of trade secrets and develop response plans. They should consider losses to their competitiveness as well as losses to their reputation. Additionally, it is a good idea for firms to have a legal strategy in the wake of an incident of corporate espionage. After all, industrial espionage is illegal in many countries, including the United States, and offenders can face stiff sentences

**3.**

1. 3 HAMLETS - M

1 ORACLE- O

9 MESSENGERS-R

1 SHELL- S

4 RODENTS- E

1 CALABASH- C

3 PROPHECIES- O

1 DESTINY- D

6 COWRIES- E

The result isMORSE CODE

1. **SING THAT RAP FALL**

**Answer:** THINGS FALL APART

**4.**

Encrypted message TSJSFRHGTJQTNZS

1. **Ceasar substitution cipher (key 5)**

ABCDEFGHIJKLMNOPQRSTUVWXYZ

From the English alphabets above Caesar shift of 5 gives:

**VWXYZABCDEFGHIJKLMNOPQRSTU**

Decrypted Caesar cipher- ONENAMCBOELOIUN

1. **Columnar transposition cipher (key 5)**

**Using Key = abcde**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **a** | **b** | **c** | **d** | **e** |
| **1** | **2** | **3** | **4** | **5** |
| **o** | **n** | **c** | **e** | **i** |
| **n** | **a** | **b** | **l** | **u** |
| **e** | **m** | **o** | **o** | **n** |

Plain text = ONCE IN A BLUE MOON