NAME: COLE EMMANUEL ROTIMI

MATRIC NUMBER: 15/ENG02/016

COURSE CODE: COE 510

COURSE TITLE: COMPUTER SECURITY TECHNIQUES

LEVEL: 500L

Question 1

The main aim of this policy is to protect the integrity and confidential data that resides within company XYZ’s technology infrastructure. This policy aims to prevent this data from being deliberately or accidentally stored insecurely on a mobile device or carried over an insecure network where it can potentially be compromised. A breach of this type could result in loss of information, damage to critical applications, financial loss, and damage to the company’s public image. Therefore, all users employing a mobile device connected to an unmanaged network outside of XYZ’s direct control to backup, store, and otherwise access company data of any type must follow the defined protocols of company XYZ.

### ****Acceptable Use****

* Company XYZ defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing.
* Employees are going to be blocked/disallowed from accessing certain websites during work hours/while connected to the company’s network at the discretion of the company. Such websites include, but are not limited to…
* During work hours or when connected to the office network devices’ camera and/or video capabilities are/are not disabled while on-site in order to monutor activities.
* Devices may not be used at any time to store or transfer illicit materials nor store or transmit proprietary information belonging to another company, Harass others, Engage in outside business activities .
* There would be permitted apps which includes; detailed list of apps, such as weather, productivity apps, Facebook, etc.
* Applications not downloaded from a reliable source such as iTunes or Google play are prohibited
* Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, documents, etc.

### ****Devices and Support****

* Smart phones including iPhone, Android and Windows phones are allowed
* Tablets including iPad and Android are allowed
* Connectivity issues will be supported by the IT department; employees should/should not contact the device manufacturer or their carrier for operating system or hardware-related issues.
* New devices must always be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

### ****Reimbursement****

* The company will/will not reimburse the employee for a percentage of the cost of the device (include the amount of the company’s contribution), or The company will contribute X amount of money toward the cost of the device.
* The company will/will not reimburse the employee for the following charges: roaming, plan overages, etc.

### ****Security****

* In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the company network.
* Company XYZ’s [strong password policy](http://www.itmanagerdaily.com/network-security-fundamentals/" \o "Network Security: Top 5 Fundamentals) is: Passwords must be at least six characters and a combination of upper- and lower-case letters, numbers and symbols. Passwords will be rotated every 60 days and the new password can’t be one of the previous passwords.
* After three failed login attempts, the device will be locked temporarily. Employees would have to contact IT to regain access.
* Rooted or jail broken phones are prohibited as they are more prone to hacking.
* Employees are automatically prevented from downloading, installing and using any app that does not appear on the company’s list of approved apps.
* Smart phones and tablets that are not on the company’s list of supported devices will not be allowed to connect to the network.
* Smart phones and tablets belonging to employees that are for personal use only are/are not allowed to connect to the network.
* Employees’ access to company data is limited based on user profiles defined by IT and automatically enforced.
* The employee’s device may be remotely wiped if

1. The device is misplaced
2. The employee terminates his or her employment contract
3. IT detects a data or policy breach, a virus or similar threat to the security of the company’s data and technology infrastructure.

### ****Risks/Liabilities/Disclaimers****

* While IT will take every precaution to prevent the employee’s personal data from being lost in the event it must remote wipe a device, it is the employee’s responsibility to take additional precautions, such as backing up email, contacts, etc.
* The company reserves the right to disconnect devices or disable services without notification.
* Lost or stolen devices must be reported to the company within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
* The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company’s acceptable use policy as outlined above.
* The employee is personally liable for all costs associated with his or her device.
* The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, [malware](http://www.itmanagerdaily.com/mobile-malware-grew-three-fold-last-year/), and/or other software or hardware failures, or programming errors that render the device unusable.
* Company XYZ reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

Question 2

The purpose of espionage is to gather knowledge about (an) organization(s). It may include the acquisition of intellectual property, such as information on industrial manufacture, ideas, techniques and processes, recipes and formulas. Or it could include sequestration of proprietary or operational information, such as that on customer data sets, pricing, sales, marketing, research and development, policies, prospective bids, planning or marketing strategies or the changing compositions and locations of production. It may describe activities such as theft of trade secrets, bribery, blackmail and technological surveillance. As well as orchestrating espionage on commercial organizations, governments can also be targets. How would I go about the espionage undetected.

As mentioned, In every company, there are certain information that are targeted during industrial espionage they are listed with the reason for the target mark.

1. **Trade secrets.**  it generally means protected information about existing products or products in development. This information may help your rivals make their products more competitive or even bring a similar product to the market faster than you can.
2. **Financial information.** Financial information about your company can be used to offer better deals to your clients and partners, win bids, and even make better offers to your valuable employees.
3. **Client information.** Data of your clients, including their financial information, can be used to steal business or can be leaked to damage the reputation of your company.
4. **Marketing information.** This will allow your competitors to prepare a timely answer for your marketing campaigns, which, in turn, may render them ineffective.

As a new employee it would be mandatory for me to be guided and shown the inner working of the company, during breaks and leisure time I would speak to the older staff members, managerial staff as well because they most likely would be in charge of some of the documents listed above.

My major targets would be staff that are under the departments that handle the information listed above. My discussions would always drift towards current and previously developed projects, company rivals, financial situation of the company, stock market placement, etc.

As an IT employee I would be asked to fix minor issues in several devices of employees in which case I would seize the opportunity to deliberately install security malware(malicious software) on specific computer systems, the major target in this case would be the department of human resource and administration. I would need access to more computer systems for more information, I would use the access I have from the admin department to send a phishing mail to staffs of the selected departments, this email will be sent out with a Remote Access Trojans which will give me administrative control over all staff systems and revert all filled surveys and reports back to my system.

To ensure i am not detected I would try to look for loopholes in my own system and cover up my tracks, I would ask staff of anything unusual they noticed and endeavour to get them fixed to reduce suspicion.

To avoid such situations in the future, I would advise the company to employ certain measures which includes

****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 ground keepers. 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.

Question 3

1. The number before the text give the location of the actual relevant letter in that particular line of text. For example; 3 HAMLETS; I’ll take the third letter of the text because 3 is the number before the text, and it gives me M.

3 HAMLETS – M

1 ORACLE – O

9 MESSANGERS – R

1 SHELL – S

4 RODENTS – E

1 CALABASH –C

3 PROPHECIES- O

1 DESTINY – D

6 COWRIES – E

Answer: MORSE CODE

b). SING THAT RAP FALL

It is an anagram and it decrypted to form the phrase

THINGS FALL APART.

Question 4

Encrypted message; TSJSFRHGTJQTNZS

Using Caesar’s substitution cipher with key 5, the alphabet will now look like this compared with the regular alphabets

V W X Y Z A B C D E F G H I J K L M N O P Q R S T U – Shift key 5

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z – Regular alphabet

This will translate to O N E N A M C B O E L O I U N

Now to apply the Columnar transposition cipher with key 5

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |
| O | N | C | E | I |
| N | A | B | L | U |
| E | M | O | O | N |

This translates to ONCE IN A BLUE MOON.