OLATUNJI TEMITOPE OLATUNDE

15/ENGO2/043

COMPUTER ENGINEERING

500 LEVEL

COE 510 ASSIGNMENT

**QUESTION 1**

Security policy for company XYZ on the use of mobile phones in the company.

**PURPOSE OF THE POLICY:**

It is believed that all member of staff of the company use mobile phones. These policies will serve as a guideline for the usage of these mobile devices within the company. These policies are now put in place to ensure the safety and protection of delicate company files and company secrets.

**GOAL OF THE POLICY:**

The goal of the policy is to ensure that critical and important company document are not leaked, altered or compromised in any way either intentionally or unintentionally. It is also to protect the integrity of the company documents and secrets from damage, loss or theft both physically and virtually by thieves or hackers. This would help to maintain the credibility and reliability of the company and not tarnish it.

**APPLICABILITY**

This policy is applicable to all staff, both technical and non-technical, across all clearance levels, either with personal or company provided mobile devices. This includes cell phones, smart phones, laptops, desktops, any kind of specialized computers, tablets, etc

The policy addresses a number of security threats which include

**Theft** – Stealing of classified information either by an intruder or a compromised staff. It could also be virtually by a hacker.

**Malware Infection** – This compromises the integrity of documents and files on the company server.

**POLICIES**

1. All member of staff should have a separate mobile device for all personal engagements. The company will provide mobile devices for company activities but that is all those particular phones should be used for. These devices should not be used for social media, sending of personal mails, calling personal numbers, etc. It would result I adequate sanctioning from the higher authorities.
2. All member of staff should be aware that using personal mobile devices around delicate information is highly prohibited. Hence, there should not be personal mobile devices in the server rooms, in meeting rooms and in all delicate situations or events. Taking of pictures of documents is also highly prohibited, it does not matter if it is on a personal mobile device or a company device.
3. The security department will have access to all websites and links opened on the company network in order to monitor irregular activities as well as sweep websites for possible malware.
4. All company mobile devices must be turned it at the end of every week to the IT security department to monitor activities carried out on the devices and ensure there have been no breaches.
5. A secure mail link mail.xyz.com.ng is provided for all company related emails. These emails should only be logged in on the company provided mobile devices and should not be on personal devices to prevent leakage or breach of information.
6. The use of VPN on the company devices in the company network is prohibited as it could allow activities on the internet to be logged and transferred or sold to third parties.
7. No changes or modifications should be made to any company provided mobile device without the permission or aid of the IT security department. All changes or repairs should be made by the IT security department alone.
8. Any staff member leaving the company on a permanent basis should ensure all company devices are returned to the IT security department to be wiped properly. Failure to do so would result in intervention from the local authorities.

**QUESTION 2**

As a security expert, my first action would be to carry out a survey to determine the important departments that hold valuable information such as Financial and client information and company secrets. I would also select targets which would naturally be unhappy and vulnerable members of staff under the above departments in the XYZ company.

After doing this, the next step is to make initial contact with the determined weak links also surveying their importance to the company and their various clearance levels. I would go with the with the vulnerable staff with the highest clearance level.

Making initial contact would involve me carrying out social engineering and posing as a friend. I would try to form a relationship with said staff in order to allow me gain trust. I would ask subtle but delicate questions about personal life in order to help me get passwords and logins to accounts and devices as well as questions about the work in order to seem interested and gain an idea of the work being done and to keep updating myself is the staff chosen was the correct one. I would go further to plant spyware on the personal and work computer of the staff to enable me get get access to delicate information such as other passwords, client details, user activities, personal identification et cetera.

If after all this, I have still not gotten all the information I need or my cover is blown, the next thing to do is offer money way above the pay grade of the staff.

With all this I would also have a safety net that would ensure that the staff doesn’t give me up and blow the cover. This safety net was initially a back up plan in case the money offer was not taken. The safety net would involve all the dirt I would have been able to gather from my time with the staff accounts and devices. Anything that the staff did not want getting out, or anything that could get the staff thrown in jail or losing the job. This would ensure that the staff gives me all the information I need or help me carry out an attack if I need to.

In any case, I would send the staff into the company with a drive or flash to connect it to the company main computer systems/servers. This drive or flash could also give me remote access to the company servers to perform a zombie attack on systems on the company network.

**On the other hand, I would take some security measures to ensure that such breach doesn’t occur in the future.**

* I would ensure all the security protocols agrees and is up to the ISO 27001 standard
* Protection software would be installed on all the company and personal devices to prevent breaches
* The network firewall would be upgraded
* I would ensure that all my staff are paid adequately according to their job description (if it is up to me).
* I would ensure that only people related to a particular section or part of the company have access to the information concerning them. That means a breach in a particular sector does not necessarily mean a breach in the entire company.
* I would reduce the number of people with high security clearance to reduce the number of ways in which a breach could happen, the more people that have access, the more vulnerable the company is.
* A sign in would be required anytime any of the cleared staff is going to access the server room as no other member of staff would even be allowed inside. A biometric lock would be put in place that only recognizes cleared personnel. It would make it easy to track down the last person to make contact with the severs before a breach in order to easily trace the culprit and possibly undo the damage.
* Staff would not be allowed to do company work with personal devices and personal activities with the company devices. Staff would not be allowed to carry company devices outside the company as it could easily result in breach/loss of data whether through theft, assault or natural occurrence like fire.
* All company devices would be submitted at the end of every month to the IT security department to scrub for damage or malware or possible breaches.

**QUESTION 3**

a.

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 MESSENGERS - R

1 SHELL - S

4 RODENTS - E

1 CALABASH - C

3 PROPHECIES - O

1 DESTINY - D

6 COWRIES - E

The code is decrypted to form MORSE CODE

b. SING THAT RAP FALL

It is an anagram and it decrypts to form THINGS FALL APART

**QUESTION 4**

This is the 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.