QUESTION 1

Mobile devices are portable computing devices. They at risk due to their very nature of being portable.

XYZ is taken to be an organization having over a hundred staff, provides a few devices for top management staff and it allows for Bring-Your-Own-Device (BYOD) for other staff members in order to save cost.

XYZ ensures all staff get the information on the security policy on the use of mobile devices and trains them in best practice. The organization labels and tracks all mobile devices and takes regular inventory. XYZ also deployed mobile anti-virus solution.

Security Policy on use of mobile devices in XYZ

INTODUCTION

This security policy communicates the effects of architectural decisions to the user; highlighting his or her rights and obligations. This policy serves the purpose of illustrating correct and acceptable use and deterring misuse.

All mobile devices, both company-owned and personal that have access to corporate networks, data, and systems are governed by this mobile device security policy. Applications used by employees which store, or access company data are subject to this policy.

POLICY: Requirements

1. All devices must use these operating systems or later: Ios 12.0.1 or later, Android 9.0 or later.

2. All high risk users (employees with sensitive data) are briefed on the organization's security controls
3. All mobile devices connected to the company network must be secured (screen lock, PIN, password). This will be enforced by the IT department.
4. Mobile devices must use device encryption before accessing corporate e-mail
5. All employees must send request to add a device before being allowed to access company data on such device
6. All stolen or lost devices used must be reported to the IT department immediately (Company owned devices will be completely erased/wiped out while on the personal devices, only the company data will be erased)
7. Devices would not be allowed to automatically connect to Wi-Fi. Public Wi-Fi network safety measures are created.
8. Public USB ports in mobile devices should be disabled
9. Devices must store passwords as an encryption
10. Users must not load crack version or illegal software on the device
11. Devices should use firewalls and anti-malware software
12. Users must use an encrypted network (such as IPSec or SSL VPN connection, or a WPA2 secured WLAN connection) at all times
13. Devices must not be left unattended in vulnerable locations such as offices, airports and hotels.
14. Users must not copy sensitive server-hosted data - including confidential member information and company IP, to unencrypted local device storage.
15. All devices connected to the corporate network must be malware-free

16. Users cannot be granted access to a colleague's account
17. Devices must not have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
18. Bluetooth should be disabled when not in use
19. All devices must have a mobile security app
20. Users should avoid clicking link from untrusted sources
21. Employees must agree to never disclose their passwords to anyone.

The device will be locked, and/or wiped if:

1. It is jailbroken
2. It is lost or stolen
3. It contains a security vulnerable software

POLICY: Non-compliance

The above requirements will be checked regularly and should a device be noncompliant, the company may lock the device, or in particularly severe cases, a device wipe. A team will be set up to investigate the case, take disciplinary action, and possibly termination of employment.

QUESTION 2

Company XYZ is a leading firm in the tech industry. XYZ is working on a cutting-edge technology. This technology is more of software than hardware, so it involved thousands of lines of codes. The company allows for junior staff to access their emails on the go by using their personal mobile devices but with a policy that ensures login details are not saved on these devices. XYZ provides mobile phones for senior colleagues as they work with more sensitive and confidential information.

PLANNING

I researched about the company by asking many questions from the organization that hired me and the security men of XYZ after walking by the company and giving them some food twice. I figured the best way to go about this espionage due to XYZ's security protocols, is to apply for a job in a department whose role isn't very close to the IT in its operations. I took a few courses on Human Resource Management. At the end of one month, I could boast of having four different certifications. I created a LinkedIn profile with another name, put it some false info, and included my four certifications. I followed many organizations on LinkedIn, but XYZ was the only tech firm. This was done to avoid suspicion whatsoever.

I went to XYZ company's street a few more times during their break to bond with the staff there and showed my interest in working with the Human Resource (HR) department. Mr. A is an accountant at XYZ and is friends with the deputy head of HR. He promised to tell his friend about me; my interest, and qualifications. I later applied for the job, did a quick interview and got the job. I thanked Mr. A.

Now, as a staff in the organization, I figured most offices granted access to individuals using the ID card swipe. I went to Mr. A's office to know the security put in place, since it's the finance department. From experience, I know this department usually has one of the tightest securities in organizations.

Company XYZ security

In the finance department, it is noticed that:

- Staff ID is needed to get the door to open with a security personnel at the entrance to assist if the ID swipe doesn't work after trying twice
- there are no security cameras
- staff username and password requirements to access company system
- finance staff username and password to access documents in the Computer System
- all documents in the Computer system are finance-related
- Public network connectivity is allowed for mobile devices
- Confidential emails sent to external parties had little encryption

EXECUTION

Since XYZ allows employees to access emails using their mobile devices, I made friends with a junior staff in the IT department. I asked to use the Internet on his phone to browse. He allowed. I opened a private browser and I secretly downloaded a malware on his phone and installed. The malware is a keylogger. I cleared my search, then surfed a random thought (such as funny videos, and even told him to view and we laughed). This is to avoid any suspicion whatsoever. I also ensured I never borrowed his phone again. The installed keylogger made me gain access to all his login credentials. I got a new inexpensive PC and changed my IP address to another

country's own. I monitored his incoming and outgoing mails using his login details.. I used the junior staff's email to resend a previously sent mail to the IT team, but this time, it was sent with a malware. I did this to make the team think it was just a simple mistake, since it was same as a previous mail. The malware sent is a sniffer (Daemon) that runs in the background. From there, I was able to get some information of other senior team members. The information gathered include but are not limited to information on Wi-Fi details, all sites visited since sniffer installation.

I was able to get to the company's internal product site. I searched through the different projects and found the new project XYZ is working on. I got the blueprint, design and architecture of the system, and saved them on my PC.

I continued my job as the HR and left the organization a month after this espionage was carried out, claiming to have gotten a better offer which would help me grow more in my career.

ERASING FOOTPRINT

This espionage method did not leave any visible footprints, but in order to be safe, I carried out the following:

1. IP address initially changed to another country's throughout the operation was later changed back to home country
2. MAC address was erased
3. The Network Interface Card (NIC) was broken and disposed far away to avoid further tracing
4. VPN was used throughout the sniffing process to mask my identity

5. The computer allocated to me by XYZ did not have anything IT related and so cannot be traced back to me. I did not use the system at all during this espionage.
6. The company's internal product site was unedited

SECURITY MEASURES

The following are the security measures to be put in place to prevent the likelihood of other hackers performing the action in future

1. Daily system scanning for malware
2. Trainings should be given on the use of mobile devices (both company-owned and personal)
3. Company should always use all reasonable network security: firewalls, intrusion detection software, etc.
4. Setup a system for senior staff with access to sensitive data in a way that no one staff member has access and control over all critical information
5. The organization should provide mobile devices for all staff with strict security policies
6. The company should perform an employee background check. Give particular attention to IT personnel
7. Have all employees sign non-disclosure agreements
8. Junior workers should be treated well and compensated regularly. This reduces the chances of having disjointed employees who may give out company information
9. Install security cameras at strategic positions in the company, to help 'catch' a spy who works physically to get information
10. More biometric login should be included in departments with sensitive information.

QUESTION 3A

3 HA**M**LETS

1 **O**RACLE

9 MESSENGE**R**S

1 **S**HELL

4 ROD**E**NTS

1 **C**ALABASH

3 PR**O**PHECIES

1 **D**ESTINY

6 COWRI**E**S

Plain text: MORSECODE

QUESTION 3B

Cipher text: SING THAT RAP FALL

Plain text: THINGS FALL APART

QUESTION 4

Cipher text : TSJSFRHGTJQTNZS

Cipher text	T	S	J	S	F	R	H	G	T	J	Q	T	N	Z	S
Left Sub. Cipher (Key 5)	O	N	E	N	A	M	C	B	O	E	L	O	I	U	M

Columnar transposition cipher (key 5):

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

Reading it row by row, Plain text is ONCEINABLUEMOON (ONCE IN A BLUE MOON)