NAME: DERRI COLUMBUS BOMAYE

MATRIC NO: 15/ENG02/017

DEPARTMENT: COMPUTER ENGINEERING

COURSE CODE: COE510

COURSE TITLE: COMPUTER SECURITY TECHNIQUES

 **ASSIGNMENT 2**

**QUESTION 1**

**Develop a security policy for an XYZ company on the use of mobile devices in that company.**

SOLUTION

**Purpose**

The purpose of this policy is to define standards, procedures, and restrictions for end users who have legitimate business requirements to use a private or the company provided mobile device that can access the college’s electronic resources. This mobile device policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

• Laptop/notebook/

• Tablet computers such as iPads

 • Mobile/cellular phones

 • Smartphones

 • PDAs

 • Any mobile device capable of storing District data and connecting to an unmanaged network.

The goal of this policy is to protect the integrity and confidential data that resides within the company’s technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently 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 District’s public image. Therefore, all users employing a mobile device connected to an unmanaged network outside of company’s direct control to backup, store, and otherwise access District data of any type must adhere to the company-defined processes for doing so.

**Applicability**

This policy applies to all the company employees, including full and part-time staff, contractors, faculty and other agents who utilize either company-owned or personally-owned mobile device to access, store, back up, relocate or access any District resources / info. Such access to the district resources / info is a privilege, not a right. Consequently, employment at company does not automatically guarantee the initial and ongoing ability to use these devices to gain access to District networks and information.

The policy addresses a range of threats:

**Threat Description**

* Loss: Devices used to transfer or transport work files could be lost or stolen.
* Theft: Sensitive District data is deliberately stolen and sold by an employee.
* Copyright: Software copied onto a mobile device could violate licensing.
* Malware: Viruses, Trojans, Worms, Spyware and other threats could be introduced via a mobile device.
* Compliance: Loss or theft of financial and/or personal and confidential information / data could expose the college to the risk of non-compliance with various identity theft and privacy laws.

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of IT. Unauthorized use of mobile devices to back up, store, and otherwise access any college related information / data is strictly forbidden.

This policy is complementary to any previously implemented policies dealing specifically with data access, data storage, data movement, and connectivity of mobile devices to any element of the company network.

**Policy and Appropriate Use**

 It is the responsibility of any employee of the company who uses a mobile device to access District resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any mobile device that is used to conduct the company business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user’s account. Based on this, the following rules must be observed:

 **Access Control**

1. IT reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to District and District-connected infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts the District’s systems, data, student, staff and faculty at risk.

2. Prior to initial use on the District network or related infrastructure, all mobile devices must be registered with IT. The company District IT will maintain a list of approved mobile devices and related software applications and utilities as needed. Devices that are not on this list may not be connected to District infrastructure. Although IT currently allows only listed devices to be connected to District infrastructure, it reserves the right to update this list in the future.

3. End users who wish to connect such devices to non-college network infrastructure to gain access to college data must employ, for their devices and related infrastructure, security measures deemed necessary by the IT department such as updated software, anti-virus software, and personal firewall. District data is not to be accessed on any hardware that fails to meet the company’s established IT security standards.

**Security**

4. Employees using mobile devices and related software for network and data access will, without exception, use secure data management procedures. All mobile devices must be protected by a strong password. See the company’s password policy for additional details. Employees agree to never disclose their passwords to anyone.

5. All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain the company data. Any non-District computers used to synchronize with these devices will have installed anti-virus and anti-malware software deemed necessary by the company’s IT department. Anti-virus signature files on any additional client machines – such as a home PC – on which this media will be accessed, must be up to date.

6. IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with in accordance with the company’s overarching security policy.

7. Employees, contractors, Full time faculty, part time faculty and temporary staff will follow all the company-sanctioned data removal procedures to permanently erase the company specific data from such devices once their use is no longer required.

8. In the event of a lost or stolen mobile device it is incumbent on the user to report this to IT immediately. The device will be remotely wiped of all data and locked to prevent access by anyone other than IT. If the device is recovered, it can be submitted to IT for reprovisioning.

9. Employees, contractors, Full time faculty, part time faculty and temporary staff will make no modifications of any kind to the company-owned and installed hardware or software without the approval of the company Division of Information technology. This includes, but is not limited to, any reconfiguration of the mobile device.

10. Division of Information Technology reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the company network.

**Organizational Protocol**

11. Division of Information Technology can and will establish audit trails and these will be accessed and used without notice. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse. The end user agrees to and accepts that his or her access and/or connection to the company’s networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. This is done in order to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains the company’s highest priority.

 **Policy Non-Compliance**

Failure to comply with the Mobile Device Acceptable Use Policy may, at the full discretion of the College, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment.

**QUESTION 2**

**You have been hired by a security company as a security expert to perform the role of an industrial espionage on a XYZ company. Using all the available tools, discuss how to carry out this attack without being noticed. Also discuss the security measures to prevent the likelihood of other hackers performing the action in the future.**

**SOLUTION**

Intelligence on competitors gathered in a legal way can give a leg up in the fight for market share. But sometimes it’s not enough. Competitors send spies to gather information more often than you would think, judging by the news.

Industrial espionage embraces illegal and unethical methods of collecting corporate data. It involves stealing intellectual property and trade secrets to use them for a competitive advantage.

**TARGETS OF ESPIONAGE**

You might be wondering what data your competitors want.

Usual targets of industrial espionage are:

* **Trade secrets:** While definition of “trade secret” varies from country to country, 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.
* **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.
* **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.
* **Marketing information:** This will allow your competitors to prepare a timely answer for your marketing campaigns, which, in turn, may render them ineffective.

Industrial espionage is hard to detect and even harder to prove.

Although there are a few truly sensational cases of industrial, economic, and corporate espionage that get media coverage, they’re just the tip of the iceberg.

Industrial espionage is an illegal yet widespread practice. If it hasn’t affected your company already, it’s only a matter of time. The question is why we don’t hear about it in the news that much.

There are several reasons why most companies do not report cases of industrial espionage:

* **Industrial espionage is hard to prove:** Industrial espionage is often performed by insiders that already have access to sensitive data. Espionage activities are almost indistinguishable from their normal everyday activities, so these actions are hard to detect and even harder to prove in court.

* **It’s hard to hold perpetrators accountable:** Since laws on trade secrets and industrial espionage are different everywhere, it may be very hard to hold foreign companies and governments accountable. And even if the perpetrator is domestic, they can prolong legal procedures to the point where it’s not feasible for your company to continue pursuing the case.

* **It may negatively affect your stock:** The value of your company’s stock may fall if it becomes publicly known that your security has been breached. It may undermine the trust of your investors and customers.

* **It can be seen as a violation** of [IT regulations](https://www.ekransystem.com/en/solutions/meeting-compliance-requirements)**:** A company is responsible for ensuring the security of its customers’ sensitive data. In certain countries and industries, if this data leaks or is stolen by industrial spies, the company will be fined. Yes, you can experience losses and be penalized because of espionage.

All of these factors compel companies to keep cases of espionage to themselves and conduct internal investigations. It’s their responsibility to establish effective detection and response procedures. However, effective prevention is the best way to deal with industrial espionage.

**HOW TO CARRY OUT THIS TASK**

**CONDUCT A RISK ASSESSMENT**

What corporate data is the most valuable for your company?

Find potential targets. You need to know what trade secrets and other valuable data your company possesses and how much they’re worth. You can evaluate your trade secrets by comparing them with products already available on the market or with known assets of your competitors.

Once you identify your most valuable data, you can guess who may want it. Once you know possible threats and potential attack vectors, you can detect vulnerabilities in your own defences.

Risk assessment is key to a risk-based approach to security, which should be part of the security strategy of every organization. You should also work out an [incident response plan.](https://www.ekransystem.com/en/blog/incident-response-plan-tips) It will help you respond in case of a data breach and minimize its impact on your business.

**ESTABLISH AN EFFECTIVE SECURITY POLICY**

Do all your employees follow your security policy?

All security rules should be formalized in a clearly written security policy. This policy should include rules prohibiting password sharing and employees bringing their own devices to work, among other things. Make sure all your employees are aware of it, starting with upper management.

**MAINTAIN AN EFFICIENT DATA ACCESS POLICY**

Who can access critical data? Do they really need to?

Many companies provide access to critical data and infrastructure by default. While it may be more convenient, this policy is not secure.

Your company should follow the [principle of least privilege](https://en.wikipedia.org/wiki/Principle_of_least_privilege) and prohibit access to all data unless necessary.

Applying the so-called “need to know” principle means that you provide access only to employees who really need information. If unauthorized employees occasionally need to work with confidential information, they can do it under the supervision of authorized staff.

By limiting the number of people with access to critical data, you strongly limit the risks of your competitors obtaining this data.

**SECURE YOUR INFRASTRUTURE**

Are you protected by a perimeter with a multi-layered approach?

Establish a secure perimeter around your company network. Conventional corporate cybersecurity software, such as firewalls and antivirus software, is your **first line** of defences.

Make sure to separate your valuable data from your corporate network and limit access to it. Protect your border routers and establish screen subnets. A secure perimeter with a layered approach is the best way to protect yourself from industrial and economic espionage through hacking and malware.

**EDUCATE EMPLOYEES**

Do your employees understand how they contribute to the company’s cybersecurity and why they should do?

The best way to prevent your employees from inadvertently helping the enemy is to educate them. Tell them about potential threats your company faces.

Make employees aware of the role they play in the security of your organization.

Teach them about simple security practices to use in their daily workflow. This will help protect your staff from social engineering and will prevent simple security mistakes, such as [sticking with default passwords](https://www.ekransystem.com/en/solutions/privileged-user-monitoring).

**CONDUCT BACKGROUND CHECKS**

Do you know who works for you?

Before hiring someone, the HR department usually conducts a [background check](https://en.wikipedia.org/wiki/Background_check).

This minimizes risks of finding a mole in your organization.

It can be helpful to repeat these checks once in a while – especially for employees with privileged access – to ensure that they don’t become spies. A sudden surge in standards of living, unexpected trips, or paying off debt are among potential causes for concern.

**CREATE A PROPER TERMINATION PROCEDURE**

Are you sure your ex-employees won’t access your company’s data?

In many cases, company espionage is performed in the last couple weeks of work. Employees’ credentials are often still active after termination, so they can still access sensitive data for malicious purposes.

Create and implement a proper termination procedure to protect your company from potential acts of industrial espionage by former employees.

**MONITOR EMPLOYEE ACTIVTY**

What are your employees doing online during their work time?

You’ll never know whether your employees are acting maliciously, intentionally, or inadvertently unless you monitor their online presence.

It’s especially important to keep an eye on privileged users, such as system administrators and upper management. They can easily gather intelligence while performing their normal tasks and explain any abnormal behaviour as a mistake.

[Employee monitoring](https://www.ekransystem.com/en/solutions/monitoring-employee-activity) makes all employees’ actions fully visible and allows you to detect data theft and take measures in a timely manner. In case an incident happens, you can use the records for your investigation.

Moreover, monitoring employees can deter opportunistic employees from stealing data, as they know their actions are recorded.

**A MONITORING SOLUTION FOR PREVENTING INDUSTRIAL ESPIONAGE**

Using Ekran system as a case study;

Ekran System is a universal employee activity monitoring solution specifically designed to combat insider threats, including industrial espionage.

It can monitor the actions of every user regardless of their level of privilege, allowing you to control the actions of system administrators and users with access to trade secrets and financial information.

Particularly, Ekran System provides you with the following features for detecting and preventing industrial espionage:

**MANAGE ACCESS AND AUDIT USER ACTIVITY**

* **The**[PASM](https://www.ekransystem.com/en/product/privileged-access-management)**solution in Ekran System helps you implement the**[principle of least privilege](https://en.wikipedia.org/wiki/Principle_of_least_privilege.). It provides access management for privileged and general user accounts. You can specify endpoints that particular users can access, limit the time of their sessions, and provide temporary and permanent credentials.

**MONITOR AND INVESTIGATE**

* [Screen video recording](https://www.ekransystem.com/en/product/user-activity-monitoring). You can watch all kinds of account sessions in a convenient YouTube-like player and filter them by username and IP. Videos are indexed with layers of text metadata, including visited URLs, typed keystrokes, and names of opened apps.
* **Ekran can record input and output audio streams on user endpoints.** Recorded audio can be exported for further analysis.
* **Key episode search.** Advanced session analysis allows investigators to search episodes by various parameters within the current session and across all recorded sessions.

**RESPOND TO THREATS IN REAL TIME**

* **User and entity behaviour analytics (UEBA)** is an artificial intelligence-powered module that analyses user activity to detect unusual behaviour. The UEBA module will help you prevent data breaches long before they happen.
* [Actionable alert system](https://www.ekransystem.com/en/product/alerts-and-notifications). In addition to an impressive collection of alert templates, you can set custom alert rules based on any suspicious events like opened URLs, process names, or connected USB devices. When the system identifies a suspicious event, your security team receives a notification so they can act immediately.
* **Automated incident response.** An automated response guards your data even before the security team reacts. You can assign a risk level and choose between blocking a user, terminating an application (or process), blocking a connected USB device, displaying warning messages, and other options.

In conclusion, industrial espionage can severely damage a company’s reputation and hinder opportunities for growth. By following the best practices mentioned above and using Ekran System as your user monitoring tool of choice, you can reliably prevent industrial espionage and protect your company from both outsider and insider threats.

QUESTION 3 AND SOLUTION

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 COWERIES = E

1. SING THAT RAP FALL = THINGS FALL APART

QUESTION 4

Moriarty Smith works for GT Bank and you suspect him of sending customer details to credit card fraudster by email. You confront him but he sneers at you and you and says ‘’You have no proof because you will never break my cipher.in fact, in my next email I will tell you when I think you will catch me’’. From observation of his encrypted emails you suspect that he is encryption his text using a Caesar substitution cipher (key 5) and a columnar transposition cipher (key 5). You intercept his very last email containing the short message TSJSFRHGTJQTNZS. What does it say?

**SOLUTION**

**Caesar substitution cipher (key 5)**

ABCDEFGHIJKLMNOPQRSTUVWXYZ

From the English alphabets above Caesar shift of 5 gives

VWXYZABCDEFGHIJKLMNOPQRSTU

Decrypted Caesar cipher: ONENAMCBOELOIUN

**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