CCCY 321 Information Security Management

Course Project

CY7

- Razan Alghanmi 2111007

- Shahad Kulaibi 2114565

- Elaf Salem 2110527

1) **Preliminary Activities**

a) What are the company's key assests?

Physical Assests	Potential Cyber Security Threats to Assess
Company Iphones for all staff members	• Open Network. • Infiltration of malicious or pirated programmes.
Digital Security Culture	• Phishing attacks • Lack of awareness
Hardware	• Complicated network of suppliers • Investment level at record low • Cheaper, faster and more complicated • Outdated technology
Laptop	• Randomware attacks • Theft

Information Assests	Potential Cyber Security Threats to Assess
1) Users must give their bank details when signing up to pay in-app games	There are cases where cybercriminals have learnt to mimic legitimate banking websites by using their URLs. When a person logs in, the hackers steal their data to use later.
2) User business	Cyberattacks targeting private companies are no different from those targeting public companies. Due to their opportunistic nature, cybercriminals are constantly on the lookout for new ways to attack. However, private companies have their own qualities that lead to unique cyber security risks.

3) Users with whom you are speaking lack identity evidence	Without the knowledge or consent, the attackers may be able to locate your friends and demand a ransom.
4) Healthcare Data	Because they contain personal information that could be exploited for identity theft, medical records are a common target for fraudsters. This data is often used to forge prescriptions and other forms of health insurance fraud.

b) How have other companies been affected by cyber security attacks? What can Chatter learn from these experiences?

Componay name	**Description of their cybersecurity attack**	**How might this be a risk for Chatter?**
Facebook	According to the company, the data of over 50 million Facebook users may have been compromised, regardless of whether news or financial data was accessed. The hackers were able to crack Facebook via three different security vulnerabilities. Facebook fixed the problem by resetting the access token for each account. Users did not have to reset their passwords as the tokens do not store them.	Chatter could be vulnerable as hackers are likely to exploit the same underlying vulnerabilities to steal data. In addition, many people use their passwords from one service to another. If the hackers manage to crack a password database, they could potentially access user accounts on Chatter.
Saudi Aramco	One of the biggest oil producers in the world, Saudi Aramco, was the target of a cyberattack that was a serious occurrence that affected many aspects of their business. The virus used in the attack was called "Shamoon," and its only function was to find and destroy data.	The cyberattack that targeted Saudi Aramco teaches Chatter a valuable lesson by drawing attention to possible threats. One such risk is that hackers might target Chatter in an

	The hackers successfully erased the data on some 30,000 machines during the attack, which caused a large loss of information and interfered with the business's operations. The attack is noteworthy even though it had little effect on Aramco's cash flow since it showed how cyberattacks might have a direct influence on the real world.	attempt to alter or destroy the data it has processed, which might cause it to lose important user data and interfere with its regular business operations. It is imperative that Chatter implement strong data redundancy, backup procedures, and security measures to prevent unwanted access in order to reduce this risk.
Adobe	Hackers stole user account information, credit card records, login credentials, and other private information during the cybersecurity attack on Adobe. Nearly three million encrypted payment card records and login credentials were reportedly hacked at first. Later on, though, the number was raised to include 38 million active users' encrypted passwords and IDs. More research also showed that a previously uploaded file included over 150 million hashed password pairs and usernames that were stolen from Adobe. Names, passwords, and debit/credit card information of customers were compromised.	A prime example of the possible dangers and ramifications for Chatter's cybersecurity is the hack on Adobe that led to the loss of consumer information. Similar to Adobe, Chatter might keep sensitive data as well as user details. Cybercriminals could misuse personal information and violate user privacy by taking advantage of this data if there is a security breach. It is crucial that Chatter create strong encryption, access limits, comply with applicibal policies and frequent security

		updates to minimize these dangers and safeguard user data.

1) Refer to the tables above to identify Chatter's cyber risks (Assests/potential vulnerability/threate)

Asset	**Potential vulnerability**	**Threat**
Iphones	Unpatched software/apps	• An attack vector that could be taken advantage of by attackers
Company laptops and desktops	Theft	• Inadequate security measures for laptops can lead to unauthorised access, as can the practise of storing usernames and passwords on sticky notes or in the laptop itself for less skilled workers.
Staff	Uneducated and untrained employees	• The theft of a company laptop and other inappropriate behaviour in the face of an attack are examples of misused company assets.
Network Devices(firewalls, switches, routers)	• Firewallsmisplacement • Missetting firewalls rules • Notmonitoring network traffic	• Money lost because firewalls are inefficient due to poor placement. • Bypass firewall rules, ineffective rules can allow malicious traffic into the corporate network.

When registering for paid in-app games, users must provide their financial details.	Unsecure/unauthorizedpayment processescompany's services.	• Users' credit card details have been leaked, which could lead to a number of problems.
User Credentials (usernames and/or passwords)	Simple passwords and predictable usernames	• Bruteforce attacks
Personal pictures and videos	• Use a simple password • Share photos and videos with suspicious chatter friends	• Blackmailing the users by the untrusted people • Hacking their accounts

3. Risk analysis: assign a score to each identified risk using a qualitative or a semiqualitative method as detailed in chapter 4.

Likelihood Scale		
Rating	Description	Definition
5	Very High	Probability of the event occurring once within a three-year period is >50%
4	High	Probability of the event occurring once within a three-year period is 30 to 50%
3	Moderate	Probability of the event occurring once within a three-year period is 15 to 30%
2	Low	Probability of the event occurring once within a three-year period is 5 to 15%
1	Very Low	Probability of the event occurring once within a three-year period is <5%

Figure 1. Risk likelihood scale

Magnitude of impact	Impact definition	Score
High impact/ High probability	**Very high** They are the biggest risks that entrepreneurs should pay attention.	**5**
High impact / Medium probability Medium impact / High probability	**High** These risks have either a high probability of occurrence, or a significant impact	**4**
Medium impact / Medium probability	**Medium** There is a medium chance that the risks appear noticeable impact.	**3**
Medium impact / Low probability Low impact / Medium probability	**Low** These risks can occur in some situations and have a low to medium impact.	**2**
Low impact / Low probability	**Insignificant** There are risks with low probability of occurrence and low impact. Can therefore be neglected.	**1**

Figure 2. Risk Impact scale

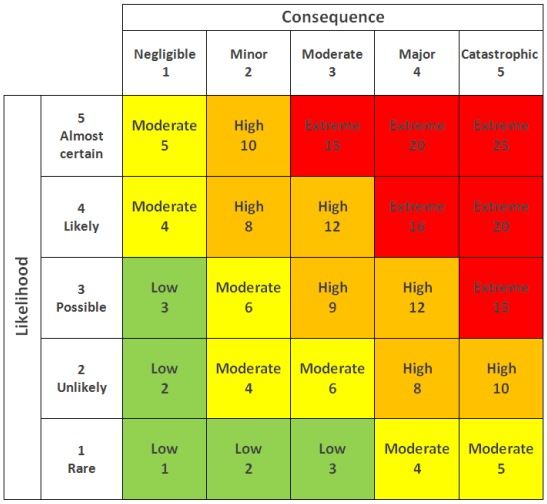

Figure 3. Risk Rating Matrix

By considering the above figures in the risk analysis process, we have concluded the following:

Risk Rating Matrix:

Asset	Vulnerability	Likelihood	Impact	Risk-Rating Factor
Iphones	Unpatched software/apps	3 (Moderate)	4 (High)	12 (High)
Company laptops and desktops	Theft	2 (Low)	3 (Moderate)	6 (Moderate)
Staff	Uneducated and untrained employees	4 (High)	2 (Low)	8 (High)
Network Devices (firewalls,	Firewalls misplacement	2 (Low)	3 (Moderate)	6 (Moderate)

switches, routers)				
Network Devices (firewalls, switches, routers)	Missetting firewalls rules	3 (Moderate)	4 (High)	12 (High)
Network Devices (firewalls, switches, routers)	Not monitoring network traffic	3 (Moderate)	4 (High)	12 (High)
When registering for paid in-app games, users must provide their financial details.	Unsecure/unauthorized payment processes company's services.	2 (Low)	4 (High)	8 (High)
User Credentials (usernames and/or passwords)	Simple passwords and predictable usernames	4 (High)	3 (Moderate)	12 (High)
User Credentials (usernames and/or passwords)	Use a simple password	4 (High)	2 (Low)	8 (High)
Personal pictures and videos	Share photos and videos with suspicious chatter friends	3 (Moderate)	3 (Moderate)	9 (High)

Based on the risk analysis conducted above, it appears that missetting firewall rules, not monitoring network traffic, unpatched software/apps, and simple passwords and predictable usernames must be addressed first by the risk treatment team and dedicate their efforts on because they have the highest risk rating (12).

4. Risk Treatment: How would you treat each identified risk? Indicate the treatment strategy (Mitigation, avoidance, transfer, etc., …) and justify your response. (CLO 3.3, 4 Marks)

We have created extensive methods and practices in order to further manage the dangers that have been identified. To learn more about each strategy's ability to reduce potential dangers, let's take a closer look at it.

Using the risk mitigation strategy, we will put in place a reliable mechanism for frequent updates and patch installations in order to reduce the danger of iPhones running unpatched software or

apps. This involves keeping a careful eye out for software flaws and swiftly applying the required updates to guarantee that the devices are shielded from known security threats. We want to protect the integrity and security of our iPhone fleet by taking a proactive stance.

Using the risk transference strategy, purchasing full insurance coverage to transfer the risk of laptop and desktop theft is a wise move. The insurance policy will offer financial protection in the unfortunate case of theft or loss, reducing potential losses. With this method, we can concentrate on replacing devices quickly and smoothly, causing the least amount of disruption to worker productivity.

Using the risk mitigation strategy, maintaining a secure environment requires addressing the risk of staff members who lack education and training. We'll put in place thorough training courses covering a range of security best practices topics. Employees will receive training on the value of data security, safe surfing practices, and the identification of possible dangers through interactive sessions, workshops, and seminars. We hope to reduce the possibility of dangerous actions by our employees by cultivating a culture of security awareness.

Using the risk avoidance strategy, we will follow industry rules and suggested practices during installation and configuration to reduce the possibility of firewall misplacement. In this way, our network infrastructure is effectively protected from unwanted access and any security breaches by making sure that network equipment, like firewalls, are positioned strategically and configured accordingly.

Using the risk mitigation strategy, we are going to implement strict change control procedures to prevent misconfigured firewall rules. The approval and review process for any changes made to firewall rules is rigorous to guarantee that only approved and required changes are put into effect. To help detect and quickly fix any misconfigurations, this strategy will be reinforced by routine audits that add another level of control.

Using the risk mitigation strategy, to spot possible security risks and irregularities, proactive network traffic monitoring is crucial. Thus, we will put in place reliable network monitoring instruments and create thorough monitoring procedures. By doing this, we will be able to quickly identify and address any unusual activity, reducing the possibility that security breaches would go undetected.

Using the risk termination strategy, we are dedicated to completely stopping any payment procedures that are not secure. Rather, the implementation of safe and approved payment gateways that follow industry guidelines and use robust encryption techniques will take precedence. We can prevent potential security breaches for our clients and our business by making sure that all payment operations are secure, and that sensitive financial information is kept securely.

Using the risk mitigation strategy, we shall impose strong password policies in order to reduce the risk associated with weak passwords. For sensitive accounts, this entails establishing minimum complexity criteria, changing passwords on a regular basis, and using multi-factor authentication. We'll also teach staff members and inform users on the importance of password

security, encouraging them to create strong, one-of-a-kind passwords that work on all platforms and gadgets.

Using the risk acceptance strategy, although decisions about publishing personal content are left to the individual, we recognize and accept the risks involved. However, we advise users to share images and videos with caution and awareness, especially if they are with unknown or suspicious people. This reminds people to be aware of potential threats and to safeguard their personal privacy and security when using the internet.

To determine whether these techniques are effective and to spot any potential new concerns, regular risk assessments will be carried out. Our systems and policies will stay strong and current thanks to ongoing monitoring, which will also help us remain alert in a threat landscape that is always changing.

We may create a thorough and proactive security framework that successfully reduces risks and protects the confidentiality and integrity of the data and operations of our firm by implementing these tactics.

5. Draft two policies that may help Chatter in its defense strategy against the identified risks.

Employee Training and Awareness Policy:

The level of awareness among employees is low. Therefore, the company needs to implement a policy to ensure raising security awareness and continuous training for employees, which includes training them in social engineering methods, how easy it is to crack simple passwords using programs available to the public.

Acceptable Use Policy:

Since employees work inside and outside the company via their devices. It is important that they know the acceptable use policy for company devices. Such as the programs available to download and update periodically, the hours of Internet connection, and restrictions on using their personal accounts on these devices.

Data Protection Policy:

Since the company's main product is an application that users use. Their data will naturally be stored, transmitted and processed. Therefore, the company must implement a policy that explains safe ways to do this. Among them are instructions for encrypting data, methods for safe transmission, and how to dispose of it safely.

Remote Work Policy:

Due to the incident that occurred in the company due to the failure to implement a policy for employees who work remotely. The company must establish one to limit or reduce and control these incidents as much as possible and the impacts and threats they incur in the future.

6. Which PwC team (refer to the case study) do you think Chatter needs to help them improve their cyber security strategy and why?

We believe that the company needs a crisis team due to the presence of various threats surrounding the company and the lack of a plan to manage them. This team will help the company prepare well and confront crises before they occur. There are several main points that cover the company's security needs.

1. Rapid Response:

Usually, companies need to respond quickly to incidents and make immediate decisions. Because any additional time will be given to the one causing the threat, causing additional destruction to the company.

2. Specialized Expertise:

A person without experience cannot make quick decisions. Therefore, relying on a team with administrative, legal and security experience will give the company more time and effort to focus on developing the product away from focusing time on the company’s secondary goals.

3. Risk Mitigation:

The company needs to develop good plans as much as it needs employees with administrative and security competencies. The crisis team proactively identifies, evaluates and mitigates risks before, during and after they occur.

4. Reputation Management:

The importance of the crisis team is expanding in managing psychological crises that may sow in the hearts of users and stakeholders and cause panic about using the company's applications or contracting with the company due to their unsafety. Therefore, reputation management protects the company and its assets, such as the brand, indirectly.

5. Preparedness and Planning:

Crisis teams dedicate time and effort to prepare for potential crises. They develop crisis response plans, conduct training and simulations, and stay updated on emerging risks and best practices. This preparedness enables them to respond effectively when a crisis occurs and minimize the negative consequences for the company and its assets.

References:

Figure 1: Chaparro, M.R. (2014). A new dimension to Risk Assessment.

Figure 2: Iacob, V. (2014). Risk Management And Evaluation And Qualitative Method Within The Projects. *Ecoforum, 3*, 10.

Figure 3: Kaya, Gulsum. (2018). Good risk assessment practice in hospitals.

Fox, J. (2023) *8 biggest cyberattacks in history*, *Cobalt*. Available at: https://www.cobalt.io/blog/biggest-cybersecurity-attacks-in-history (Accessed: 16 November 2023).

The 15 biggest data breaches of the 21st Century (2022) *CSO Online*. Available at: https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html (Accessed: 16 November 2023).