Assignment Risk Management

Student’s name: A K M Mahmudul Haque
Student-ID: AB0208
Student number : 2110841

1 Assignment

The task is to identify risks and threats related to your own computer. Create tables according to the specification (check examples from presentation material). The goal of the assignment is to understand the importance of your own computer from a cyber security/information security perspective. Return the file in Moodle (return folder “Risk Management”) as **PDF** format and name the file with your own information **studentID_surname_firstname.pdf**

SCORING / ASSESSMENT

- Passed/Failed

MINIMUM CRITERIA

- Attack matrix and risk matrix has 3 rows and 3 columns
- Risk identification done
- Risk probability calculation table filled
- Follow-up measures and summary/free word filled

1.1 Attack Matrix

Possible threats	Identity Thieves	Impact
Physical loss	Stolen physical devices	Data loss
Malware	Unauthorized malicious software damaging the system	System damage
Hacking	Unauthorized access	System damage, data loss/theft

1.2 Risk Matrix

Assets	Physical damage	Consequences
Files (documentation)	Medium	Data loss and data theft
Privacy	Medium	Identity theft, unknown access to rob financial accounts: Data leaks
System	Medium	Failure of the system, loss of data, downtime, and the potential for being unable to use the computer

1.3 Risk Identification

Which are the biggest risks based on the attack and risk matrix? Define at least 3 bullet points. Check example from slides from “Risk Management”, chapter/slide “Identified Risks”.

Based on the attack and risk matrix, some of the biggest risks include:

Physical theft or loss with significant impact: This risk involves the theft or loss of physical assets such as laptops, mobile devices, or storage media that contain sensitive information. The impact of such an event can be severe, as it can lead to unauthorized access, data breach, or loss of valuable data. It is crucial to implement physical security measures such as access controls, monitoring, and tracking to minimize the risk of theft or loss.

Malware infection leading to system damage and/or data loss: This risk involves the infiltration of malware into the system, which can cause damage to the infrastructure, compromise the integrity of the data, or result in data loss. It is important to implement security measures such as firewalls, anti-virus software, and regular system updates to minimize the risk of malware infection.

Lack of backup: This risk involves the absence of a backup plan or outdated backups, which can lead to data loss in the event of a security breach or system failure. It is important to regularly backup data and test backup systems to ensure their effectiveness and minimize the risk of data loss. Having a backup strategy can also help to recover from security incidents quickly and minimize the impact on the business.

1.4 Riskien probability calculation

Asset	Attack	Impact	Likehood	Significance
Files (documentation)	Malware Infection	10 €	Medium	12500 €
Privacy	Loss	10 €	Medium	20000 €
System	Hack	6 €	Medium	2000 €
Device	Theft	1.5 €	High	750 €

2 Follow-up measures

1. Secure your passwords by using a password manager and enabling two-factor authentication. This will help protect against password theft and unauthorized access.
2. Keep your software up to date. Regularly installing updates and patches can help protect against known security vulnerabilities and reduce the risk of malware infections.
3. Use antivirus software to protect against malware infections and other security threats.
4. Backup your data regularly to prevent data loss in the event of a security breach or system failure.
5. When accessing public networks, use a virtual private network (VPN) to ensure your online activity remains secure and private.
6. Be cautious about where you take your computer to avoid physical loss or accidental damage. Keep your device with you or store it in a secure location when not in use.
7. Pay close attention to possible scams such as phishing emails or social engineering tactics. Be wary of unsolicited requests for personal or financial information and verify the legitimacy of any emails or messages before responding.

3 Summary/Free word

The training and assignment have helped me to realize the significance of cybersecurity and the risks associated with leaving my computer unsecured. The risks can range from physical theft or loss of my device to various online threats, including hacking and malware attacks. Thus, it's crucial to take measures to protect myself better.

One step I plan to take is to install better antivirus software to protect my computer from malware attacks. Additionally, I will change the passwords I recently created and store them securely in a password manager, reducing the likelihood of unauthorized access.

Another step I plan to take is to back up my data regularly to minimize the risk of data loss in case of a security breach or system failure.
Overall, the training has been valuable in raising my awareness of cybersecurity threats and their potential impact. I'm now more empowered to take proactive measures to mitigate the risks and safeguard my computer and personal information.