Cybersecurity Risk Assessment

Risk Assessment Definition

RISK MATRIX			LIKELIHOOD				
			Rare	Unlikely	Possible	Likely	Almost Certain
		(description)	May only occur in exceptional circumstances	Could occur at some time	Might occur at some time	Will probably occur in most circumstances	Is expected to occur in most circumstances
CONSEQUENCE	Severe	Critical failure(s) preventing core activities from being performed. The impact threatens the survival of the organisation.	HIGH	VERY HIGH	VERY HIGH	EXTREME	EXTREME
	Major	Breakdown of key activities leading to reduction in performance (e.g service delays, revenue loss, client dissatisfation). Survival of organisation is threatened.	HIGH	HIGH	VERY HIGH	VERY HIGH	EXTREME
	Moderate	Impact on the organisation resulting in reduced performance such as targets not being met. Organisations existence is not threatened, but could be subject to significant review.	LOW	MEDIUM	MEDIUM	HIGH	VERY HIGH
	Minor	Some impact on business areas in terms of delays, system quality but able to be delt with at operational level.	VERY LOW	LOW	MEDIUM	MEDIUM	HIGH
	Insignificant	Minimal impact on non-core business operations. The impact can be dealt with by routine operations.	VERY LOW	VERY LOW	LOW	MEDIUM	MEDIUM

https://github.com/hhphu/InfoSec/blob/main/Projects/Forage/Datacom/Task-Two/risk-matrix-definition.png

Assets to protect

- Confidential customer data
- Proprietary business information
- Financial information
- Intellectual property
- Physical infrastructure & equipment

Risks

Cyber attack VERY HIGH

A cyberattack is a deliberate attempt by hackers to gain unauthorized access to a company's computer systems or networks, with the goal of stealing sensitive information, causing damage or disruption, or holding data ransom. The perceived sources for a cyberattack could include organized crime groups, nation-states, or individual hackers.
Causes: Organized crime groups, nation-states, or individual hackers
Consequences: Data theft, system downtime, reputational damage, and financial losses.

Current Risk Rating VERY HIGH

Existing Control

Firewalls, intrusion detection systems, antivirus software

Effectiveness of existing control measures

Firewalls - Excellent control. Configured, maintained & tested properly. Highly effective and very fit for purpose. It substantially reduces the likelihood and/or consequence of the risk. It is cost effective.
Intrusion detection systems - Moderate control. Configuration needs to be improved.
Antivirus - Good control. Effective and fit for purpose. Configuration, maintenance and testing are good enough.
The likelihood is likely and the consequence is major. Hence the risk is VERY HIGH.

Target Risk Rating MEDIUM

Additional control Measure

Treat - reduce the likelihood or impact of risk by following these additional control measures:
- Multi-factor authentication (MFA)
- Penetration testing
- Regular security awareness training

Transfer - We can also transfer this risk to a 3rd party by letting a Managed Security Service Provider make the organization's Security Information and Event Management (SIEM) tool.

Effectiveness of additional control measures

Excellent / Good / Moderate / Weak

Multi-factor authentication (MFA) - Good Control. This would add an extra layer of security by requiring users to provide additional authentication factors beyond a password.

Security Information and Event Management (SIEM) - Excellent Control. This would enable real-time monitoring of security events and alerts for any suspicious activity, and help with incident response.

Penetration testing - Good Control. This would simulate a cyberattack to identify vulnerabilities and weaknesses in the system and help to improve the existing controls.

Regular security awareness training - Good Control. This would help to educate employees about cyber threats and best practices to prevent them, and reduce the risk of human error or negligence.

The likelihood is unlikely and the consequence is moderate, hence the risk is **MEDIUM**.

Natural Disaster HIGH

A natural disaster is an unpredictable event caused by natural phenomena, such as earthquakes, cyclones, floods or bushfires, that can cause significant damage to a company's physical assets, disrupt operations, and pose a threat to employee safety.
Causes: Natural phenomena beyond human control
Consequences: Property damage, loss of life, disruption of supply chains, and financial losses.
The likelihood is rare and the consequence is severe. Hence the risk is **HIGH**.

Current Risk Rating LOW

Existing Control

Emergency response plans, backup power generators, and building reinforcement measures.

Effectiveness of existing control measures

Emergency Response Plans: Good control. The organization has established plans for responding to natural disasters, which reduces the consequence of the risk.
Back up Power generators: Good control. Backup power generators can help ensure continuity of operations during a natural disaster, reducing the consequence of the risk.
Building Reinforcement Measures: Excellent control. The organization has taken steps to reinforce the building against natural disasters, reducing the likelihood and consequence of the risk.
The likelihood is rare and the consequence is moderate. Hence the risk is LOW.

Target Risk Rating LOW

Additional control measures

Accept - Acknowledge the risk and choose not to resolve, transfer or treat.
Effectiveness of additional control measures
Regular testing and maintenance: Good Control. Regularly testing and maintaining emergency response plans, backup power generators, and building reinforcement measures to ensure they are effective and up-to-date.
The likelihood is rare and the consequence is moderate. Hence the risk is LOW.

Employee Negligence MEDIUM

Employee negligence arises when employees fail to follow established security protocols or engage in careless behavior that puts company assets at risk. This could include employees failing to properly store or dispose of sensitive information, sharing login credentials, or falling for phishing scams.
Causes :Employees who are not aware of the security protocols, don't take security seriously, or don't understand the consequences of their actions.
Consequences: Data breaches, reputational damage, and financial losses.
The likelihood is possible and the consequence is moderate. Hence the risk is MEDIUM.

Current Risk Rating MEDIUM

Existing Control

Security awareness training, access Control

Effectiveness of existing control measures

Security Awareness Training: Good control. Regular training sessions are carried out to educate employees about security threats and best practices to minimize the risks of employee negligence.
Access Control: Excellent control. Measures have been put in place to ensure that employees only have access to the data and systems that are necessary for their job function.
The likelihood is possible and the consequence is moderate. Hence the risk is MEDIUM.

Target Risk Rating LOW

Additional control measures

Treat - reduce the likelihood or impact of risk by following these additional control measures:
- Monitoring and auditing of employee actions
- Role-based access control

- Incident response plan

Effectiveness of additional control measures

Monitoring and auditing of employee actions: Good Control. Regular monitoring and auditing of employee actions on company systems can help identify any suspicious activity or potential risks.
Role-based access control: Excellent Control. Implement role-based access control to ensure employees only have access to the systems and data they need to perform their job functions, reducing the risk of accidental or intentional data breaches.
Incident response plan: Good Control. Develop and implement an incident response plan to provide guidelines on how to respond to security incidents or data breaches caused by employee negligence.
The likelihood is unlikely and the minor is moderate. Hence the risk is **LOW**.