Cyber Risks at MM Corp

Cyber Risk Executive Report

Contents

About the document

This executive report presents direct and indirect risks along with recommended solutions that **MM Corp** possesses. The document is created for the executives at MM Corp.

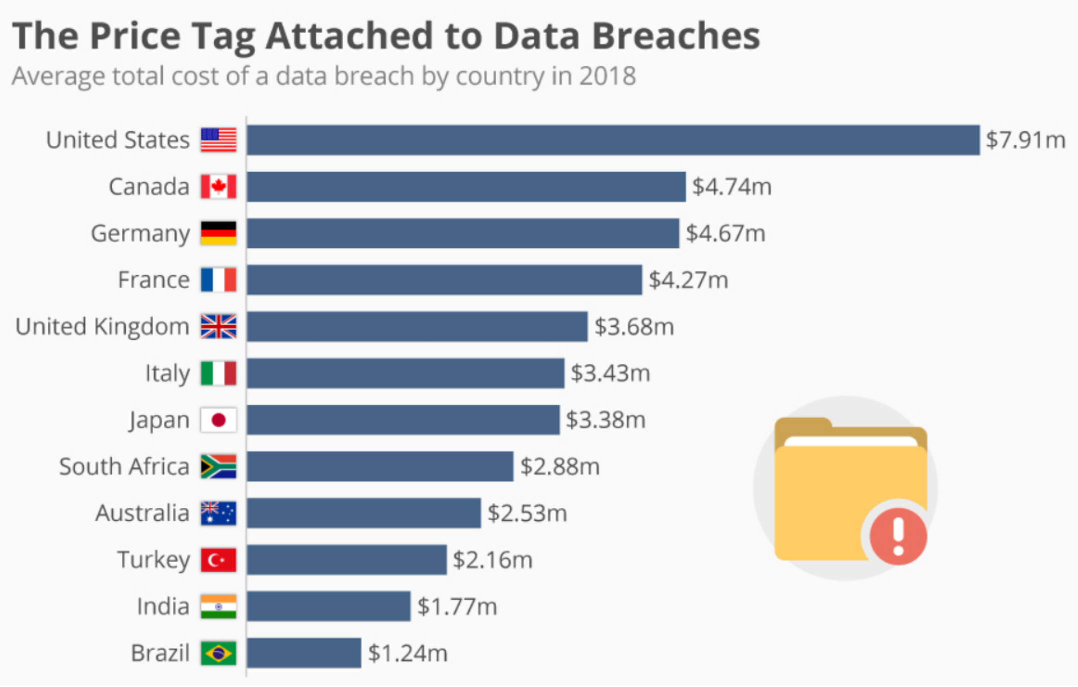
Problem

As a globally blooming organization with the company tools being featured in numerous press outlets, MM Corp is bound to be a major target for cyber attackers. The company's growth at a rapid pace and blooming market of services that we provide could also awaken high level of risks in cyberspace for MM Corp. The cybersecurity policies were implemented for a startup company but as the company's size grows, the implemented policies could be deemed inadequate. The financial and reputational risks for a growing company could be disastrous, in case of a successful cyber-attack.

Direct Cyber Risks at MM Corp.

Data Breaches

Since the pandemic, the sophistication and frequency of data breach attempts has increased according to the [1]2022 Thales Data Threat Report. Any vulnerabilities in the company's video chat system or other software can expose unauthorized access to the user data. Cyber attackers can find various methods to exploit these vulnerabilities.



1: Cost of data breaches by country in 2018.
Source: https://www.statista.com/chart/9918/the-price-tag-attached-to-data-breaches/

[1] 2022 Thales Data Threat Report, https://cpl.thalesgroup.com/en-gb/data-threat-report

A data breach is costly and damages the reputation of the company more than any other cyber risk. For a growing company like MM Corp, the cost of remediation and recovery from data breaches are very significant.

Unauthorized Account Access

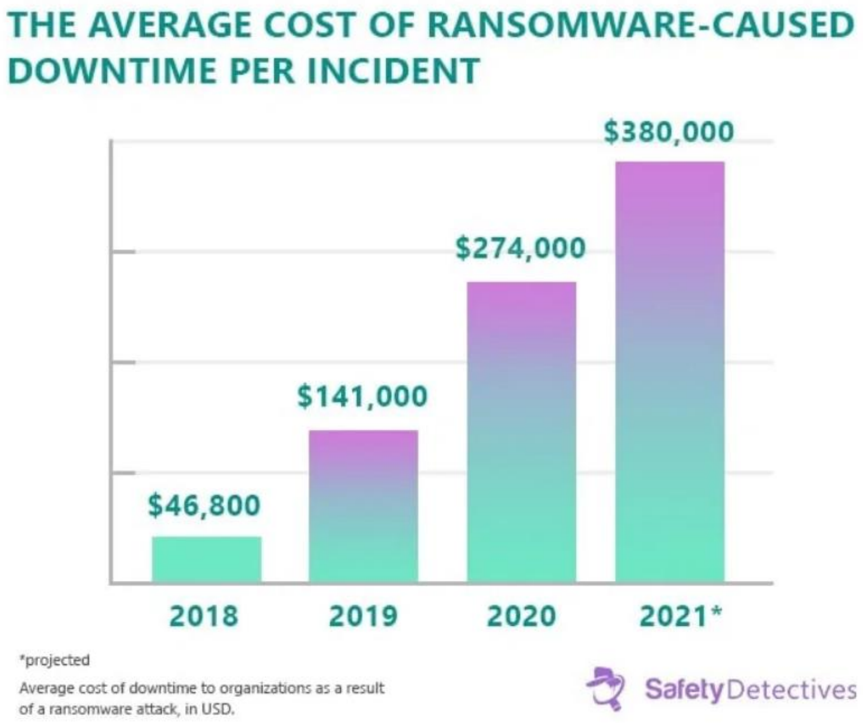
Unauthorized account access may occur due to a data breach or due to compromised account login information which could potentially lead to access of personal information, session notes and session recordings. An insecure communication due to misconfigured or intercepted connections could also result in unauthorized account access even though the E2E encryption is in place.

Malware

Malwares are pieces of software developed for malicious purposes. Any unauthorized access to the system could also let the cyber attackers install malware into the system.

Malwares can result in downtime and delays in services which leads to loss of productivity and damage company's reputation. Moreover, malwares also could lead to data loss which is damaging to the company due to the assets we hold.

Ransomware, a type of malware is more prominent in our industry, encrypts data in the system and demands payment in exchange for the decryption key. Often more than not, the companies which become a victim of malware attacks, do decide to pay a hefty ransom to decrypt the data.



[2]

[2] Ransomware Facts, Trends & Statistics for 2023, Safety Detectives, https://www.safetydetectives.com/blog/ransomware-statistics/

2: Average cost of ransomware-caused downtime per incident.
Source: https://www.safetydetectives.com/blog/ransomware-statistics/

In recent years, the cost of downtime due to a ransomware attack has increased. According to [3]Safety Detectives' statistics for 2023, sometimes the systems took weeks to resume as usual after a ransomware attack.

Insider Threats and Social Engineering

There are more 65 employees, and the number of employees is gradually increasing at MM Corp. Insider threats refer to the employees or authorized users who leak or misuse the user data. These leaks could be intentional as well as unintentional. Any employee with the authorization to access data can leak it to harm the company. However, an employee can also accidentally expose the data accidentally to wrong person or entities. These leaks could be serious to the company. The loss magnitude due to insider threats could be as high as loss of data. Moreover, exposure of data due to misconfigured databases is also a high probability.

Moreover, social engineering techniques like phishing is also a direct risk to the organization. The poor results in phishing tests suggests that the employees are vulnerable to these attacks. Phishing attacks could lead to all the other direct risks.

Poor Monitoring of data

Even though we have a Managed Security Service Provider (MSSP), the relationship is unclear. Moreover, the configuration of Intrusion Detection System (IDR) doesn't seem like properly configured or actively monitored. If the IDS is not configured properly or security alerts are not monitored actively, MM Corp may miss critical security events. Any of these events could lead to potential data breach or unauthorized access to data.

Indirect Cyber Risks at MM Corp.

Vendor Risk

MM Corp does not have proper vendor risk management strategy. There are several third-party vendors for services like MSSP, auditing, software security, digital contracting, and payment transactions. These vendors do provide resources and experience to support the operations at MM Corp, but we are also very much prone to indirect risks such as supply chain attacks, legal and regulatory non-compliance and/or business disruption due to a security incident on the vendor side.

Supply Chain Attacks

A breach at any of the vendors could lead to unauthorized access to MM Corp's data. This can lead to data breaches at MM Corp.

Legal and Regulatory Non-compliance

MM Corp could be non-compliant with laws and regulations if any of the vendors fail to meet the compliance requirements. This could also lead to fines and reputational damage for MM Corp.

Security Incident on the Vendor Side

If any of the vendors experience a security incident, MM Corp's productivity could be disrupted, and it could lead to loss for MM Corp.

Reputational Damage due to Data Breaches

Data breaches or other successful attacks at MM Corp will lead to negative publicity. Our company's reputation as an emerging company is important for attracting new clients and employees. A reputational damage due to data breaches or security incident can disrupt the trust of everyone towards the company.

Risks due to Remote Work

Allowing remote work for the employees could lead to potential security incidents. Remote work allows the users to remotely access the systems and database. The devices that employees use while working remotely are the major vulnerability to the company. The employees who have authorized access to sensitive data can lead to exposure of the company assets due to insecure devices or networks. Moreover, there is no incident response plans to accommodate the potential security incidents due to remote work.

Lack of Business Impact Analysis

MM Corp's lack of Business Impact Analysis (BIA) suggests that there may not be a proper understanding of how critical the increasing risk of business disruption we might possess in case of a security incident. A BIA is important component of a comprehensive business continuity plan as it helps identify the processes, assets and systems. This lack of clarity could lead to longer downtimes and increased losses or recovery costs in an event of a disruption of our service due to any security incident. So, in short, the lack of BIA could potentially harm the company's reputation by impacting the productivity and increasing downtimes.

Risk Matrix

The following Risk Matrix table can be used to assess and prioritize direct and indirect risks that MM Corp possesses. The table is based on the likelihood of occurrence and its potential impact to the company.

Risk Type	Risk Description	Likelihood	Impact	Risk Level
Direct Risk	Data Breaches	High	High	High
Direct Risk	Poor Monitoring of Data	High	High	High
Indirect Risk	Lack of BIA	High	High	High
Indirect Risk	Vendor Risk	High	High	High
Indirect Risk	Reputation Damage due to Data Breach	High	High	High
Direct Risk	Unauthorized Account Access	Medium	High	Medium
Direct Risk	Insider Threats	Medium	High	Medium
Direct Risk	Malware and Ransomware	Medium	Medium	Medium
Indirect Risk	Risk due to Remote Work	Medium	Medium	Medium

Recommendations

The following are the recommended security controls and policies that MM Corp can implement to strengthen the security and minimize the risks.

Authentication Measures

MM Corps can implement strong authentication measures like Multi-Factor Authentication for all users in contrast to just employees and mentees. This adds an additional layer of protection for any accounts which makes it difficult for the attackers to compromise the accounts. Just installing MFA can significantly reduce the risk of unauthorized access even if the user's credentials are compromised. This also helps reduce any vulnerabilities that comes from remote access so the employees can continue to work remotely. Moreover, installing strong authentication can also help improve trust towards the organization which could potentially lead to new business opportunities.

Implementing Access Control Measures

Implementing access control such as role-based access control could help protect sensitive data by ensuring that the users have authorization to access only the resources required for their roles. This makes it difficult for the attackers to exploit the vulnerabilities through phishing attacks or social engineering as they would have to gain information of users in specific roles with high level privileges. This will also help with mitigating insider threats as users have access to only what is necessary for their role. Moreover, the auditing process also gets enhanced as it becomes easier to identify security gaps.

Development of Risk Management and Incident Response Plans

A formal vendor risk management program can help evaluating, managing and mitigating the risks associated with vendors with a systematic approach. The program can help the organization by identifying potential risks associated with each vendor by taking factors like their security architecture and compliance with regulations into factor. It can also help find new vendors and hash out the ones which bring risk to MM Corp. Moreover, this also helps with generating contractual agreements with the vendors.

Development of Incident Response Plans (IRP) can help the organization manage and respond to security incidents. In case of a security incident, the IRP can help with clear communication, next steps and coordination among different departments for making better decisions during the situation. After the incident is resolved, a process for reviewing and analyzing the response can be documented which will further identify the areas for improvement.

Conducting Business Impact Analysis

Conducting Business Impact Analysis (BIA) can help the organization identify and prioritize business functions and objectives and develop strategies to minimize the impact due to disruptions. MM Corp needs to prioritize its resources and focus on protecting the assets. Furthermore, after conducting BIA, the organization can evaluate potential risks and vulnerabilities with a risk assessment. BIA also helps MM Corp to establish maximum acceptable downtimes and data loss which directly affects the budget for cybersecurity within the organization.

Training Programs and Simulation Exercises

There are several training and awareness programs, and simulation exercises that MM Corp needs to implement to improve the cybersecurity posture of the company. The following are the recommended training programs and simulation exercises to implement at MM Corp.

Cybersecurity Awareness

Cybersecurity awareness provides training all the employees to help them understand the importance of cybersecurity and recognize common threats in the company. This will help them learn best practices for protecting assets of the company. This could include social engineering training and secure coding training.

Phishing Simulation Exercises

Even though there is a regular phishing simulation exercise, the awareness seems to be low as the results suggest. Regular phishing simulation exercises will help us understand areas where any additional training is required. To improve the results, MM Corp needs to track improvements in these exercises.

Incident Response Simulation Exercises

MM Corp's incident response simulation tests the readiness to respond to cybersecurity incidents. These exercises should also involve different departments to ensure everyone knows what their role is during an incident. Incident response exercises helps with faster response and lower downtimes during a security incident at the company.

Data Privacy and Compliance Training

Providing training on data privacy such as GDPR and HIPPA ensures that any affiliated person with the company understand their responsibilities while handling sensitive data. This should be mandatory training for all mentors, mentees, and employees so that they, unintentionally, do not release something that they shouldn't.