# MM CORP

Major Deliverable III

MARCH 14, 2023

KENDRA BIKRAM NINGLEKHU
CIS - 653

# Table of Contents

## Overview

At MM Corp, business is booming with modern, well-known brand-name clients being signed up each day. MM Corp, whose mission is to assist clients to get modern abilities by receiving mentoring from outside tutors. The company employs a web-based video chat approach to associate tutors & mentees and payment is taken care of by a partitioned installment processor. Since there are chances of cybersecurity risks being involved if not managed properly. This report contains the risks involved that harm the MM Corp bringing loss in millions of dollars if not handled properly so, countermeasures are mentioned to better prepare against mentioned cybersecurity risks.

## Asset and Threats

Asset for the MM Corp in this scenario are:

- Web-based video chat (i.e., Zoom)
- Credentials
- Passwords
- E-mails
- Data (i.e., job title, age, current workplace, name)
- Payment processor (i.e., PayPal)

Threats for the MM Corp in this scenario are:

- Mentors
- Mentees
- Attackers
- Employees

## Cybersecurity Risks

Cybersecurity risks are the probability of the company being harmed and causing losses due to cyber threats in its systems, networks, or data. There are two types of cybersecurity risk such as primary risk and secondary risk.

Primary Risk

Primary risks are the direct risks related to cybersecurity occurrences resulting in damage to the company’s frameworks, network, or data. Some of them in this scenario are as follows:

- Data breach:

The breaches of data in MM Corp's cybersecurity framework from external attackers would cause significant damage as they gain data on both mentee and mentor which exposes them to malicious malware/phishing attacks further in the future. They will be able to gain credit card data which they can use to steal dollars from the users of the MM Corp platform. These data can be also sold to the highest bidders in the dark web by the attackers making the MM Corp more vulnerable to other numerous attacks.

In November 2022, a hacker was able to get to the sensitive data of 200,000 clients involving Rancho Mesquite Casino over a few days containing full names and social security numbers. This resulted in class members and plaintiffs confronting significant chances of out-of-pocket extortion losses such as loans, medical administrations charged in their name, tax return extortion, utility bills in their names,

credit card extortion, and identity theft[1] which would be the same for the MM Corp in the case of a data breach incident.

- Insider Threats and unauthorized access:

Insider threats are one of the growing concerns in the case of cybersecurity since employees intentionally or unintentionally share the company's data or sabotage its system by giving access to external parties. Insider threats accounted for 35% of all unauthorized access risk occurrences within the third quarter of 2022 recorded by Kroll which is a risk management company.[2]

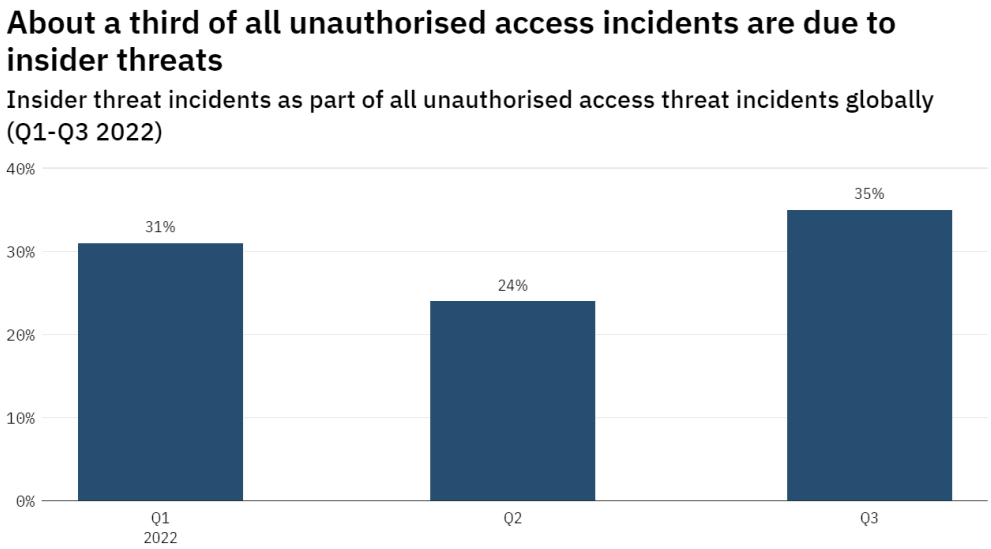


*Fig: Kroll's recorded study report*

The figure shows how the insider threat has increased during the end of the year which falls during the employee termination process. The disgruntled employee has attempted to steal gigabytes worth of data by copying it to the cloud storage so they can leverage it at their new company according to the report. The MM Corp may face similar scenarios of insider threats by using recorded sessions containing sensitive data as leverage and sharing unauthorized access to external parties.

- Malware and phishing attacks:

This attack can be used on individuals or groups of mentees or mentors of the MM Corp to get them to slip up and make them install the malware in the system to be used for future purposes. As mentioned in a data breach, their data on their name, address, phone number, emails and so on can be shared on the dark web making the exposed individual target of spear phishing, whaling, smishing, and vishing resulting in compromised logins, access to the system and payment processor data.

- Social Engineering attacks:

The mentee or mentor can use the MM Corp platform from anywhere when they are connected to the internet so, the attackers can use shoulder surfing attacks to gain credentials if the users are not careful when they are using the platform in public spaces. Another way the attackers can gain credentials,

[1] Hackers obtain personal data from 200K+ in southern Nevada casino data breach, class-action lawsuit says: https://www.8newsnow.com/news/local-news/hackers-obtain-personal-data-from-200k-in-southern-nevada-casino-data-breach-class-action-lawsuit-says/

[2] Insider threats are a growing cybersecurity problem for businesses: https://techmonitor.ai/technology/cybersecurity/cybersecurity-insider-threats

passwords, and credit card data is directly through users by being baited, quid pro quo, pretext, and scareware which are some of the other social engineering attacks.[3]

- Third Parties:

MM Corp depends on third-party service suppliers for payment processing and other administrations so, whereas these suppliers may have their security degree in place, they can still be a potential vulnerability for MM Corp as the attackers need to exploit them not the company to gain sensitive data on the payment used by the user. The attackers can further use their access to the company as third-party service suppliers bypassing the cybersecurity without alerting it and stealing the company's sensitive data.

- Lack of backups and updates:

In my findings in MM Corp, I found that they have not backed up for 24 months which can have permanent data loss in the occurrence of a cybersecurity breach and other disasters. The company will not be able to recover sensitive data leading to its inevitable failure. The software can be vulnerable to the company with easy access points for attackers to gain access if it's not regularly updated with the latest version which is often addressed in software updates.

- Misuse of the platform:

There is a possibility of the platform being misused when the mentor or mentee uses it for other purposes besides mentoring and sharing sensitive data or inappropriate content.

Secondary Risk

Secondary risks are the indirect risks related to cybersecurity occurrence which are the results of a primary risk incidents. Some of them in this scenario are as follows:

- Reputation damage:

If the breach of data occurs in MM Corp mentioned in primary risk, then the company will experience damage to its reputation resulting in difficulties in attracting new clients which can make the ongoing negotiation falls thorough with the healthcare group, universities as healthcare consider the protection of data their top priority. This will lead to millions of dollars in loss to the business and employees will be leaving for other businesses to escape the failure of the business.

- Legal and regulatory risks:

MM Corp will be subject to legal and regulatory prerequisites related to cybersecurity in the event that they handle sensitive client data and on the off chance that found non-compliant when cyber incidents happen at that point, the company is bound to confront critical punishments, fines resulting from extra financial loss moreover losing potential client and incomes.

- Financial loss:

If any primary risks incident occurs then MM Corp will have thousands to millions of financial losses in dollars depending on how long it took to recover, what assets were harmed, what was damaged, what data were stolen, did users suffer from the incident. There will be more costs for the company associated with forensic investigations, remediation efforts, and legal fees. There has been a case of

[3] Ten Social Engineering Techniques Used by Hackers: https://businessplus.ie/tech/social-engineering-techniques-used-by-hackers/

cyber-attack impact, with direct and indirect costs adding up to $54 million, not including the insurance payments involving Canadian Scobey's and FreshCo supermarket chains.[4]

- Business Disruption:

Cybersecurity incidents for MM Corp's business will bring downtime for systems and services, loss of data, and difficulty in providing services to clients. This will result in damage to the company's reputation, service availability, and the company's reliability will be questioned.

- Loss of trust:

A cybersecurity breach of MM Corp will cause a loss of trust among the current users and future potential users. This will result in current users leaving the platform due to not being able to protect the personal and sensitive data of its user bringing loss to the business and may potentially lose the business altogether.

In the case of successful cyber-attacks, 37% of companies lose about £90,000 per cyberattack on average whereas 22% of companies endured beginning from £90,000 to £445,000 which is equal to $109,363 to $540,939 in US dollars. These companies are more anxious to report the cyberattack occurrence due to fear of losing clients' trust resulting in more perilous and frequent cyberattacks causing large harm to the business. As 31% of businesses experienced disturbance of partner and client operations and robbery of financial data, 28% of companies endured reputational harm losses in thousands of pounds, 23% experienced hindrance of trading or business operation, and 18% endured cash robbery after effective cyber-attacks.[5] These discoveries show that the financial and reputational loss from effective cyber-attacks is noteworthy.

## Control Measures

The mitigation and control measures for the mentioned risks found in MM Corp are as follows:

- Implementation of multi-factor authentication and passwords requirement:

The two-face authentication must be implemented using various methods such as an authentication app, SMS text messages, or security keys to better protect your account and access to the payment data in the payment processor. Along with multifactor authentication, the users must only be able to create passwords that meet complexity requirements with numbers, symbols, and different cases of letters.

- Implementation of monitoring systems, networks, and access controls:

A reporting system should be implemented that reports if unseemly behavior or content is found within the platform when the mentor and mentee are utilizing the platform. The system should distinguish any unordinary behavior that demonstrates that sensitive data are being accessed and screen for unordinary login patterns or movement on the network of the MM Corp framework.

- Implementation of policies and procedures:

The policies to change passwords in an interval of time should be implemented along with not allowing old passwords to be reused to prevent compromising of credentials. There should be the implementation of clear policies and procedures for the appropriate use of the platform for mentors and mentees. These policies should be communicated to all users through regular training sessions. Policies

[4] Sobeys parent says total impact of cyber-attack could be over $54 million: https://www.itworldcanada.com/article/sobeys-parent-says-total-impact-of-cyber-attack-could-be-over-54-million/533125

[5] 37% of Businesses Lose Almost £90k per Cyber-attack: https://www.digit.fyi/37-of-businesses-lose-almost-90k-per-cyber-attack/

should ensure that all contracts with third parties be clear and specific with cybersecurity requirements and specify the third-party responsibility and liabilities in the occurrence of cybersecurity incidents.

- Firewall and intrusion detection:

Executing firewalls and intrusion detection frameworks will offer assistance in avoiding unauthorized access to the server of company. This framework should be tried on a regular premise to guarantee its viability against the most recent threats. Regular penetration testing and vulnerability testing can offer assistance in addressing the vulnerabilities in this framework before being misused by attackers.

- Implementation of the SETA (Security Education Training and Awareness) program:

The SETA program should be introduced to educate and train the MM Corp employee regarding attacks, aware them of the attacks such as vishing, phishing, and other forms of cyber-attack that exploits human error. MM Corp can initiate this program for users to help them better protect themselves from a cyber threat which can result in trust between the company and users bringing future potential users.


*Fig: Three parts of the SETA program*[6]

- Simulation of phishing:

Phishing simulations aid employees of MM Corp to recognize, avoid and report potential cyber threats that can compromise the sensitive data and frameworks of the company. As a portion of client security awareness, mimicking phishing gives employees the ability to recognize the threats of potential attacks, and the threat of social engineering and take suitable activities to secure the sensitive data with security best practices.[7] This can be part of the SETA program to see who falls victim and who avoids the fake phishing attack, creating a baseline for security awareness in the company to plan a program to train them accordingly.

- Creation of disaster and cybersecurity recovery team:

A disaster recovery team must be created within the MM Corp focusing on getting business back to normal as fast as possible by minimizing the financial losses taken from man-made incidents or disasters. A cybersecurity recovery team must be created to protect the assets after the breach of data. This team will focus on collecting evidence from the scene and analyzing the root cause. A fast response from these teams will help protect the company's reputation and not lose the trust of users. Some of the differences between these two teams are:

[6] Security Education, Training and Awareness: https://www.dami.army.pentagon.mil/site/SETA/AboutPD.aspx
[7] Phishing Simulation: https://www.barracuda.com/support/glossary/phishing-simulation

| | Disaster recovery plan | Security recovery plan |
|---|---|---|
| **Primary objective** | Provide business continuity after disruption from man-made or natural causes | Protect data assets after a data breach |
| **Response requirements** | Open communication with stakeholders, focus on rapid data recovery | A stealthy approach that includes evidence collection and preservation, and root cause analysis |
| **Tactical differences** | Rapid, accurate data recovery | Protective controls focused on preventing future loss |
| **Plan management** | Dedicated team that focuses on best practices and lessons learned from disaster recovery experiences | Dedicated team that keeps up to date on new cyber security threats and modifies the plan accordingly |

CSO

*Fig: Different between the team*[8]

- Regular updates of software, frameworks, and backups:

The software run should be updated to the latest version with the latest security updates and patches as this will help prevent any vulnerabilities of software to be exploited by attackers. Execute a standard backup of all critical data, to be stored safely both on location and off location to guarantee that they are available within the occasion of an incident. While doing the backup, testing the backup and recovery procedures regularly will ensure that it's working correctly. An update of the frameworks to patch any vulnerabilities is a must to not give attackers chance to get into the framework.

- Conduct regular security assessments:

Conducting regular security assessments to distinguish vulnerabilities and shortcomings in the frameworks and data will aid guarantee any potential threats to be addressed before they can be distinguished and exploited by attackers. This should incorporate the review of policies and procedures of the company regarding cybersecurity for upgrades concurring with emerging cyber threats. Amid assessment, MM Corp should evaluate the recovery team to guarantee they are viable and access control and monitoring systems to permit only authorized people to have access to frameworks and sensitive data.

## Heat map

The table below contains the mentioned cyber risks along with their control measures, the risks score with and without controls are there to show the severity of the cyber risks.

[8] Here's How to Develop a Cybersecurity Recovery Plan: https://www.lightedge.com/blog/develop-a-cybersecurity-recovery-plan/

| Risks and potential incidents | Will Affect | Risk Score without controls | Control measures | Risk Score with controls |
|---|---|---|---|---|
| Data Breach | MM Corp | 12 | a) Firewall and intrusion detection<br>b) Creation of disaster and cybersecurity recovery team | 3 |
| Insider threats and unauthorized access | Employees, Mentor, Mentee | 16 | a) Implementing SETA program<br>b) Implementing access control and monitor frameworks | 4 |
| Malware and phishing attacks | Employees, Mentor, Mentee | 10 | a) Simulation phishing | 5 |
| Social Engineering attacks | Mentor, Mentee | 8 | a) Implementing multifactor authentication | 3 |
| Third Parties | MM Corp | 11 | a) Implementing policies and procedures<br>b) Conduct regular security assessment | 6 |
| Lack of backups and updates | MM Corp, Mentor, Mentee | 17 | a) Regular updates of software, frameworks, and backups | 2 |
| Misuse of the platform | MM Corp | 9 | a) Implementing network and access control and monitor frameworks | 3 |

*Fig 1: Heat map table*

| Risk – Severity | | | | | | Risk Score - description | | |
|---|---|---|---|---|---|---|---|---|
| | Insignificant | Minor | Moderate | Major | Fatal | Risk Score | Risk Level | Description |
| Very unlikely | 1 | 2 | 3 | 4 | 5 | (1-4) | Acceptable | No further action needed |
| Unlikely | 2 | 4 | 6 | 8 | 10 | (5-9) | Tolerable | Should be reviewed |
| Possible | 3 | 6 | 9 | 12 | 15 | (10-15) | Undesirable | Immediately review and decide on further action |
| Likely | 4 | 8 | 12 | 16 | 20 | (16-25) | Unacceptable | Stop and make immediate improvements |
| Almost certain | 5 | 10 | 15 | 20 | 25 | | | |

*Fig 2: Risk Severity*