Assignment 4 — MOVEit Transfer Breach

Name – Yash Sanjaybhai Patel

Student ID - 134094184

Course – CYT145 – Cybersecurity and Threat Management Program

Professor – Ionut Anghelache

Date – 20th November 2025

Table of Contents

1. Introduction

MOVEit Transfer is a file-sharing software that is used by many companies around the world to move sensitive data in a safe manner. Organizations use this to send and receive documents, such as payroll files, customer information, and employee records. I chose this company because the breach became very big and it affected hundreds of businesses, including government offices, banks, and private companies. It also showed how a small mistake in a vendor's software can create a big impact on many organizations at the same time.

2. Summary

In May 2023, hackers found a weakness in the MOVEit transfer software. This was a zero-day vulnerability, which means the company did not know about the problem before the attack was done. The hackers used this weakness to break into MOVEit servers and steal files from many organizations that were using this software. The attackers were part of a well-known ransomware group. Instead of encrypting systems, their focus was mainly on stealing the data,

The stolen information included personal data such as names, addresses, birthdates, Social Insurance Numbers, and financial details, and employee records. Because MOVEit is a vendor used by many companies, the attack affected hundreds of organizations across different sectors like healthcare, government, education, and banking. After finding out the breach, MOVEit quickly released security patches, informed customers, and worked with cybersecurity experts to stop more attacks. Many affected companies also notified their customers, reset the passwords, improved monitoring, and contacted privacy regulators to reduce legal risks.

3. Best Preventative practices

To prevent a breach like MOVEit, organizations need strong steps in place before anything goes wrong. First, companies should hire employees carefully, which means doing proper background checks and making sure staff understand basic cybersecurity rules. Regular training is also important because workers must know how to handle sensitive information, avoid phishing, use strong passwords, and follow safe work habits.

Companies should also monitor how employees use systems, especially when they work with financial or personal information. Good monitoring tools can alert the organization if someone downloads too many files or accesses data they should not see.

Technology plays a big role in prevention. All software, especially third-party tools like MOVEit, must be updated on time. Having a clear list of inventories of all systems and software helps companies see which tools may have risks. Doing risk assessments every few months helps identify the weaknesses early. Organizations should also use firewalls, endpoint protection, strong authentication, and encryption to protect sensitive information.

Network monitoring systems, like intrusion detection tools, can catch abnormal behavior. Companies should also create clear policies for vendors. This means checking if the vendor has strong security, asking for reports, and creating contracts that explain responsibilities if a breach happens. Cyber insurance and a full incident-response plan also help reduce damage after an attack.

To detect a breach early, organizations should double-check logs, track file transfers, and receive alerts about unusual activity. When an incident is found, the company should activate its response plan to isolate affected systems, apply patches, contact the vendor, notify management, inform privacy regulators, and communicate with affected people. Recovery includes fixing weak areas, updating policies, improving vendor checks, and offering credit monitoring if needed.

Another important practice is to improve vendor management. Many companies depend on outside tools like MOVEit, but they do not always check how secure these vendors are. Organizations should review their vendors at least once a year to see if they follow strong security standards. They can ask vendors for security reports, penetration test results, and proof that they follow privacy laws. Companies should also include security requirements inside contracts, such as asking vendors to notify them quickly about any problems, apply patches fast, and follow data protection rules. By doing this, companies reduce the risk that a vendor’s mistake will harm their own systems and customers.

4. Litigation Exposure

The MOVEit breach created large legal risks for both the vendor – MOVEit and the organization using the software. MOVEit faced lawsuits because many customers claimed the company did not protect their software properly or respond fast enough. Many affected organizations also faced legal pressure because people’s personal information was stolen.

In Canada, companies must follow privacy laws that require them to protect the personal data. The main federal law is PIPEDA (Personal Information Protection and Electronic Documents Act). It says companies must protect personal data, notify affected people quickly, and report major breaches to the Office of the Privacy Commissioner of Canada. If they fail to notify, they can face investigations, penalties, and lawsuits. Several provinces have their own privacy laws too, like:

- British Columbia’s Personal Information Protection Act (PIPA)
- Alberta’s Personal Information Protection Act (PIPA)
- Quebec’s privacy laws updated under Bill 64

If health information were exposed, laws like Ontario’s Personal Health Information Protection Act (PHIPHA) may apply.

On top of privacy rules, Canadian criminal laws also apply. The Criminal Code makes hacking, unauthorized access, and data theft illegal. Even though the hackers committed the crime, companies can still face civil lawsuits for not protecting data properly.

Many class-action lawsuits were filed against MOVEit and organizations that used the software. People claimed emotional harm, privacy loss, and financial risk because their data was exposed. This shows how both the vendor and the organizations can face financial loss, legal investigations, and long-term damage to reputation.

Some companies also face international legal exposure because the MOVEit breach affected businesses in many countries. Different regions have different privacy laws, such as Europe’s GDPR, which has very strong rules about data protection. If any European citizens' information was affected, companies could have faced bigger fines or legal complaints from European regulators. This makes the situation more complex; therefore, companies must follow several privacy laws at the same time.

5. Conclusion

The MOVEit breach showed how one software weakness can create huge problems for many organizations. The main lesson is that strong security controls must be in place before a breach happens. This includes training employees, updated systems, vendor management, and strong incident-response planning. The breach also proved that companies must monitor their file-transfer systems closely and respond quickly when something unusual happens.

It also raised some questions about whether organizations had enough physical security, employee training, and strict policies for passwords and safe internet use. Many companies learned that depending too much on a vendor without checking their security adds major risk. In the end, the incident pushed many organizations to improve their security practices and take data protection more seriously.

6. Information Sources

[1] “MOVEit Data Breach Litigation,” *Cohen Milstein*, May 06, 2024. https://www.cohenmilstein.com/case-study/37803-2/

[2] “MOVEit and More Critical Vulnerabilities | A Matter of When, Not If,” *Brown & Brown*, 2023. https://www.bbrown.com/us/insight/moveit-and-more-critical-vulnerabilities/

[3] Progress, “MOVEit Transfer and MOVEit Cloud Vulnerability,” *Progress.com*, Jul. 05, 2023. https://www.progress.com/trust-center/moveit-transfer-and-moveit-cloud-vulnerability

[4] Government of Ontario, “Personal Health Information Protection Act, 2004,” *Ontario.ca*, 2014. https://www.ontario.ca/laws/statute/04p03

[5] C. Condon, “Observed Exploitation of MOVEit Transfer Vulnerability CVE-2023-34362 | Rapid7Blog,” *Rapid7*, Jun. 01, 2023. https://www.rapid7.com/blog/post/2023/06/01/rapid7-observed-exploitation-of-critical-moveit-transfer-vulnerability/

[6] C. Page, “Microsoft says Clop ransomware gang is behind MOVEit mass-hacks, as first victims come forward | TechCrunch,” *TechCrunch*, Jun. 05, 2023. https://techcrunch.com/2023/06/05/microsoft-clop-moveit-hacks-victims/

[7] L. Abrams, “New MOVEit Transfer zero-day mass-exploited in data theft attacks,” *BleepingComputer*, Jun. 01, 2023. https://www.bleepingcomputer.com/news/security/new-moveit-transfer-zero-day-mass-exploited-in-data-theft-attacks/