# Assignment 3

## Supply Chain Cybersecurity Breach

## (Progress Software – MOVEit Transfer Breach)

**Name** – Yash Sanjaybhai Patel

**Student ID** - 134094184

**Course** – CYT145 – Cybersecurity and Threat Management Program

**Professor** – Ionut Anghelache

**Date** – 6th November 2025

## Table of Contents

# 1. Introduction

This report describes the MOVEit Transfer cybersecurity incident, which is one of the biggest supply-chain data breaches in recent years. MOVEit Transfer is a software application developed by Progress Software Corporation, a U.S. company that provides secure file transfer solutions for companies worldwide. This software is used to upload, download, and share important and confidential data between employees, vendors, and partners securely.

In May 2023, a serious vulnerability was discovered in the MOVEit Transfer software. Attackers used this vulnerability to steal data from many organizations that were using MOVEit or the vendors that used it. The main target was the software vendor (Progress Software); also, the damage spread to many other organizations through the vendor's software. So, this made it a classic supply-chain attack.

I selected this case because it is the most recent and well-documented incident that clearly shows how a weakness in a vendor’s product can affect hundreds of other organizations. It also helps to clarify how laws like Tort Law and data-protection regulations come into play when a breach occurs through a third party.

## 2. Summary

According to official sources like Progress Software, CISA, and NCSC UK, the incident began in late May 2023. Hackers found a previously unknown software flaw, which is known as a zero-day vulnerability, inside MOVEit Transfer. The vulnerability was identified as CVE-2023-34362, which allowed attackers to perform a SQL injection and run unauthorized commands in the MOVEit database.

A cyber group called CL0P ransomware gang (TA505) took advantage of this vulnerability. They used this to install a web shell, which is a small malicious program on servers that runs MOVEit Transfer, and then steal the sensitive data. This took place before the vendor realized what was going on. On May 31, 2023, Progress Software publicly announced the problem and issued the security patches.

The attack spread very fast because many companies and service providers used MOVEit Transfer. For example, the UK payroll provider Zellis used MOVEit to manage data for clients like BBC, British Airways, and Boots. When hackers breached Zellis through MOVEit, they gained access to employee information belonging to those big companies.

The type of incident was mainly a data breach and ransomware extortion case. The attackers did not encrypt systems, but also stole the data and then threatened to release it unless the victims paid a ransom. Different organizations lost different types of data, like names, social insurance numbers, addresses, financial details, and other private information.

The affected companies and Progress Software immediately took action. The vendor released security updates and instructed clients to take their MOVEit servers offline until it is patched. Organizations had to notify customers and regulators, perform forensic investigations, and improve security controls. Agencies like CISA and the FBI also issued guidelines to help victims check for compromise indicators and remove the web shell.

Under Tort Law, organizations may be liable for negligence if they fail to take reasonable steps to protect the data. In this case, Progress Software had a duty of care to test and secure its software before release. If the vulnerability was due to weak testing or a lack of security reviews, they could be held responsible for any damages. At the same time, organizations using MOVEit must also ensure vendor security in their contacts. If they did not review vendor risks, they could also face legal consequences.

In 2024, some class-action lawsuits were filed in the U.S. against organizations that were breached via MOVEit. This shows how legal liability can spread through the supply chain after a vendor breach.

## 3. Impacts on the Organization

The impact of the MOVEit incident was very large and global. Thousands of companies, government departments, and service providers were affected. Because this was a supply chain attack, some victims did not even know they used MOVEit. They were impacted indirectly through a vendor like Zellis or other managed service providers.

Financial impact – The cost of investigation, forensic analysis, and data notification was massive. According to estimates by cybersecurity companies like Emsisoft and Fortinet, the total financial damage could exceed $15 billion USD worldwide because millions of records were exposed. Larger organizations had to spend money on security audits, lawyers, and public relations to rebuild trust.

Reputational Damage – The MOVEit breach hurt the image of many companies that were not directly at fault. People sometimes blamed the victims, like the BBC, instead of the vendor. This caused loss of trust and damaged their reputation.

Operational Impact – Many organizations had to shut down MOVEit systems to fix and check them. This stopped normal file transfers and delayed payroll and other work for a few days.

Legal and Regulatory Impact – After the breach, regulators became stricter about vendor security. Under laws like GDPR and PIPEDA, companies must report breaches and show good security practices and face fines.

The case showed that vendor security is very important. Even if a company is secure, weak vendors can cause problems. Companies should review vendors and make sure updates are done quickly

## 4. Conclusion

This incident teaches us a very important lesson about cybersecurity and supply chain management. It shows that security is not only about protecting your own network but also about having knowledge and understanding of the products and vendors with which you have a contract. A single flaw in a third-party application can cause a large amount of damage to hundreds of companies.

In my opinion, Progress Software reacted quickly once they discovered the attack, but they could have prevented it with more frequent security testing and independent code audits. It also shows that companies should not fully trust vendors just because they are famous or well-established. Regular reviewing of risks, patch monitoring, and incident response plans should be part of every organization's security program.

From a legal and ethical view, both the vendors and clients shared responsibility. Vendors must secure their products and respond transparently to incidents, while clients must check vendor security and be ready to act when breaches happen. In this case, many victims had to depend on the vendor's updates and guidance to recover.

Overall, the MOVEit breach is a real-world example of why supply-chain security is now one of the most important parts of cybersecurity management.

## 5. References


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

[2]“CISA and FBI Release #StopRansomware: CL0P Ransomware Gang Exploits MOVEit Vulnerability | CISA,” *www.cisa.gov*, Jun. 07, 2023. https://www.cisa.gov/news-events/alerts/2023/06/07/cisa-and-fbi-release-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability

[3] “MOVEit vulnerability and data extortion incident,” *Ncsc.gov.uk*, 2025. https://www.ncsc.gov.uk/information/moveit-vulnerability

[4] Rapid7, “CVE-2023-34362: MOVEit Vulnerability Timeline of Events | Rapid7 Blog,” *Rapid7*, Jun. 14, 2023. https://www.rapid7.com/blog/post/2023/06/14/etr-cve-2023-34362-moveit-vulnerability-timeline-of-events/

[5] J. S. Imano Fred Gutierrez, and Shunichi, “MOVEit Transfer Critical Vulnerability (CVE-2023-34362) Exploited as a 0-day | FortiGuard Labs,” *Fortinet Blog*, Jun. 08, 2023. https://www.fortinet.com/blog/threat-research/moveit-transfer-critical-vulnerability-cve-2023-34362-exploited-as-a-0-day

[1]“Industry Letter - June 2, 2023: MOVEit Transfer Vulnerability,” *Department of Financial Services*, 2023. https://www.dfs.ny.gov/industry_guidance/industry_letters/il20230602_moveit_vulnerability