MOVEit Supply Chain Data Breach

Submitted by: Ankit Pradhan

Course: IT Security: Ethical and Legal Issues

Section: A

Date: October 23, 2025

Professor: Ionut Anghelache

Company: Progress Software (MOVEit Transfer), British Airways

Table of Contents

1. Introduction

Supply chain cybersecurity has become a critical concern in the digital era, with increasing evidence that organizations cannot always control the risks introduced by third-party vendors. Notably, recent research underscores that complex supply chains create vulnerabilities that are often exploited outside the direct reach of the affected organization's own security teams. This reality has prompted businesses and governments to focus much greater attention on managing cyber risks across their interconnected networks. The MOVEit Transfer breach of 2023 stands out as a landmark event that illustrates how even trusted software vendors may become entry points for major attacks, affecting hundreds of organizations worldwide. [1] [2]

Progress Software, an American technology provider, developed the MOVEit Transfer platform, a solution widely adopted for sharing sensitive information securely among organizations, including British Airways, Ernst & Young, and government entities. This breach, initiated through a vendor's site, sharply highlights the supply chain’s role in digital defense and the need for robust controls beyond the organizational boundary. This report analyzes the MOVEit Transfer incident—its unfolding, impacts, and lessons for supply chain management—using both industry commentary and published research. [3] [4]

2. Summary of the Incident

Background

In early June 2023, Progress Software disclosed that attackers had exploited a critical zero-day vulnerability—CVE-2023-34362—in its MOVEit Transfer product, allowing for unauthorized access to sensitive databases. This SQL injection flaw enabled unauthenticated remote code execution, bypassing security controls and opening the door for attackers to upload a malicious web shell (called "LEMURLOOT") directly onto impacted servers. [5] [6]

Breach Mechanics

According to research published by Schaefer, the attackers, later identified as the Cl0p ransomware group, sent crafted requests through MOVEit's exposed API endpoints to execute arbitrary SQL statements. Once successful, the web shell allowed them to escalate privileges, enumerate sensitive files, and exfiltrate confidential data over several days—all undetected. The attack reportedly began before public disclosure, with forensic analysis noting that attackers moved quickly to harvest data before emergency patches were issued. [7] [4] [3]

Progress Software reacted by releasing urgent security patches, issuing technical bulletins, and providing guidance for organizations to scan their systems for compromises. However, not all MOVEit Transfer customers applied for the updates immediately, as research by Bitsight showed that nearly a quarter of affected organizations remained vulnerable for weeks after initial disclosure. [7] [8]

Scope and Impact

The MOVEit breach unfolded on a global scale. Over 2,500 direct and downstream organizations were affected—among them, British Airways (BA), Ernst & Young, the BBC, and several government departments. Sensitive data compromised included employee names, dates of birth, address records, payroll information, national IDs, and in certain instances, even financial and healthcare information. British Airways reported that employee personal information, including payroll and national insurance numbers, had been exposed, while Ernst & Young confirmed a loss of government identification and credit card details for over 30,000 individuals. [8] [2]

The academic literature notes how this breach exemplifies the challenges inherent in digital supply chains: a single vulnerability in a ubiquitous third-party platform can propagate harm to thousands of dependent organizations. Notably, Schaefer observed that the MOVEit attack differed from prior ransomware breaches by targeting system-wide vulnerabilities, rather than individual companies, and leveraging automation for rapid, large-scale exfiltration. [6]

Legal and Regulatory Response

The MOVEit incident triggered regulatory disclosures under laws like GDPR and CCPA, credit monitoring services for affected individuals, and class-action lawsuits against Progress Software and client organizations. Tort law discussions focused on whether Progress Software's response was timely, and whether they met the reasonable expectations of security diligence for critical infrastructure software. [9]

Academic studies cited PCI sector responses, noting an industry-wide call for rigorous vendor vetting, improved vulnerability patching, and increased cyber insurance for third-party software risks.

3. Impact(s) on the Organization

The MOVEit breach sharply illustrates how responsibility for supply chain cybersecurity is distributed—and often fragmented—between vendors and their customers, as highlighted in peer-reviewed literature. Progress Software had primary responsibility for secure software engineering, vulnerability monitoring, and providing rapid remediation. The delay in patch rollout and lack of preemptive warnings contributed to the breach's effectiveness, as confirmed by multiple forensic reports. [5] [9]

Client organizations like British Airways and Ernst & Young bore responsibility for incident response: suspending transfers, notifying staff and regulators, conducting forensic investigations, and offering support such as credit monitoring. However, academic research emphasizes that these organizations lacked both visibility and technical control over the compromised MOVEit infrastructure. For downstream partners, the breach caused business disruptions, client distrust, and interruptions in payroll, logistics, and file transfer activities. [2] [8]

Financial Impact

Leading survey results and industry analysts estimate direct breach-related costs in the millions for the largest organizations, including compensation, recovery operations, and potential

regulatory fines. Cyber insurance coverage for supply chain attacks was tested, with legal action exploring liability division under Tort law and contract terms. [8] [10]

Reputational Impact

Damage to the reputation of both Progress Software and its customers was significant. British Airways and Ernst & Young faced headline news, social media backlash, and scrutiny of their vendor management practices. Researchers found that nearly one in five companies lost client contracts because of perceived supply chain risk after the MOVEit attack. [10]

Regulatory and Legal Impact

Organizations faced intense legal review and multiple lawsuits. Regulatory bodies demanded immediate breach disclosure under data protection laws. Industry commentary and academic articles urged policymakers to clarify liability for supply chain risk and strengthen regulatory standards for third-party cybersecurity. [8]

4. Conclusion

The MOVEit Transfer attack of 2023 underlines a fundamental truth: organizations cannot fully control their exposure to supply chain cyber risks. Even when internal security is robust, vulnerabilities in widely used third-party software can have severe, cascading effects that may span continents and industries. This case shows that reliance on vendors comes with an implicit vulnerability that cannot be eliminated purely by contract or policy. [10] [3]

Key academic and industry findings indicate that organizations must strengthen vendor risk assessment, require prompt patching from suppliers, and maintain proactive monitoring across

their entire digital ecosystem. Investments in cyber insurance and breach of response planning should specifically account for third-party attacks, while regulatory bodies must clarify shared responsibilities and enforcement. [1] [8]

Overall, Progress Software and its clients were not sufficiently prepared for this sophisticated, automated supply chain attack. The MOVEit breach highlights the importance of a holistic cybersecurity strategy: one built on deeply integrated collaboration and transparency between vendors and customers and underpinned by strong regulatory frameworks. Only in this way can the risks inherent to global supply chain interdependence be managed effectively, safeguarding sensitive data and ensuring organizational continuity.

Reference

[1] FortifyData, "Top 14 Third-Party Data Breaches in 2025," 6 Nov 2025. [Online]. Available: https://fortifydata.com/blog/top-third-party-data-breaches-in-2025/.

[2] G. Thiyagarajan, "The Strategic Threat of Supply Chain Attacks," *International Journal of Scientific Research in Computer Science,* 2025.

[3] J. Chen, "Digital Supply Chain: Risk Multipliers in Third-Party Relationships," *ACM Computing Surveys,* vol. 57, 2024.

[4] Cyberint, "The Weak Link: Recent Supply Chain Attacks Examined," 2025. [Online].

[5] BlueVoyant, "Supply Chain Attacks: 7 Examples and 4 Defensive Strategies," 2025. [Online].

[6] e. a. M. Giannakopoulou, "Third-Party Software and Organizational Cyber Risk: A Meta-Analysis," *ournal of Cybersecurity Research,* vol. 9, no. 2, 2025.

[7] e. a. S. Xia, "Supply Chain Security Management: A Review and Future Directions," *Computers & Security,* vol. 123, 2024.

[8] A. Okoye, "Legal Implications of Vendor-Centric Cybersecurity Breaches," *Law, Cyber & Society,* vol. 7, 2024.

[9] P. A. N. Unit 42, "Threat Brief – MOVEit Transfer SQL Injection Vulnerabilities," June 2024. [Online].

[10] B. Airways, "Notice of MOVEit Breach," 2023.