Student Name: Oluwatimilehin Oluwagbemi

Reg. No: 2025/GRC/10712

GRC 104 Lab Compliance Frameworks and Legal Requirements

Instructor: Miss Sharon

Date: 1st November, 2025

Executive Summary

The focus of this report is on the 2023 MOVEit breach and 2024 ransomware attack on Change Healthcare, the two attack highlight the dynamic nature of threat landscape and how strong cybersecurity practices is essential to organizations no matter the size.

MOVEit breach was due to an SQL injection zero-day vulnerability in their file transfer software which compromised hundreds of businesses worldwide, while the Change Healthcare breach is as a result of vulnerability in their vital infrastructure which was exploited by a ransomware gang and led to the disruption of their operations.

This report examines the size, industry, geographic location of the affected organization, type of incident, security requirements and regulations relevant to each organization, root causes, detection timeline, organizational / regulatory response, impact assessment, lessons learned and prioritized remediation roadmap.

The comparative analysis of both breach shows that Change Healthcare attack was as a result of weakness in their network segmentation and credential management, while MOVEit breach occurred due to an exposed structural problem with third-party software dependencies.

Common trends found in the analysis include regulatory scrutiny, delayed detection, and serious financial and reputational repercussions.

In conclusion recommendations and prioritized remediation were given in this report to enhance the cybersecurity posture of the organizations.

Incident A: MOVEit Transfer Breach (2023)

Affected Organization:

- Industry: Organizations such as the government (U.S. Department of Energy), finance (Shell), media (BBC), healthcare, and education
- Size: small business to large organizations
- Geographic Location: Asia, Europe, North America

Type of Incident: Supply-chain Compromise

Security Requirement and Regulation related to MOVEit:

- GDPR (General Data Protection Regulation)
- HIPPA (Health Insurance Portability and Accountability Act)
- SOX
- Data localization laws

Root causes and control failures that enabled the incident are:

- Technical: MOVEit software has an unpatched SQL injection zero-day vulnerability.

- Process: Insufficient patch management and third-party risk assessments
- Human Factor: Lack of awareness and delayed response from IT teams

Detection and Disclosure Timeline: Progress Software detected a suspicious activity in the software environment on 28th May, 2023. By 31st May, 2023, the suspicious activity has identified an unknown flaw in the software also known as zero-day vulnerabilities, which has already been exploited by threat actors.

Organizational and Regulatory response: Progress Software carried out an emergency patch, and MOVEit quickly notified impacted customers. US Securities and Exchange Commission (SEC) started investigation on the breach, while some customers filed a lawsuit against Progress Software. Cybersecurity and Infrastructure Security Agency (CISA), CrowdStrike, Mandiat, Microsoft Huntress and Rapid7 assisted with incident response and ongoing Investigation.

Impact Assessment:

- Data Exposure: personal and financial data of over 60 million individuals were exposed due to the incident.
- Financial: MOVEit had to pay legal fees, pay for remediation which costs a fortune
- Operational: due to the incident there was disruption of services and data transfer, as a company that handles transfer of data from one end to the other.
- Customer Trust: this incident cost MOVEit a loss of customer trust and brand credibility.

Lessons Learned & Prioritized Remediation Roadmap:

- Immediate patching was conducted to contain the incident
- Vendor risk management was put in place with incident response protocols
- Zero-trust architecture was adopted with continuous vulnerability scan.

Accountability and Criminal Exposure: there has not been a criminal charge but there's an ongoing security scrutiny. Third-party vendors were notified to improve their software security.

Incident B: Change Healthcare Ransomware Attack (2024)

Affected Organization:

- Industry: Healthcare and Billing Services
- Size: Largest Healthcare in USA
- Geographic Location: United State of America (USA)

Type of Incident: Ransomware Attack

Security Requirement and Regulation related to Change Healthcare

- HIPAA (Health Insurance Portability and Accountability Act)
- HITECH (Health Information Technology for Economic and Clinical Health)

- State-level Healthcare data laws such as California Consumer Privacy Act (CCPA)

Root causes and control failures that enabled the incident are:

- Technical: Lateral movement was made possible by the absence of network segmentation.
- Process: Insufficient oversight and administration of credentials
- Human factor: Possible phishing or credential reuse vulnerabilities

Detection and Disclosure Timeline:

- Wednesday, February, 21, 2024: Change Healthcare Cyber Attack was detected.
- Thursday, February, 22, 2024: hospitals, health systems, and pharmacies report disruptions from the attack.
- Monday, February, 26, 2024: BlackCat claimed responsibility for the attack.
- Tuesday, February, 27, 2024: the department of health and human services (HHS) warns hospitals to be wary of BlackCat hackers.
- Thursday, February, 29, 2024: Change Healthcare confirmed BlackCat was behind the attack.

Organizational and Regulatory response:

- There was immediate response from Change Healthcare by disconnecting affected systems and services.
- Cybersecurity experts and Data analyst were brought to analyze the effect and to restore affected systems and services.
- Financial assistance was provided by UnitedHealth Group to affected healthcare providers.
- Affected individuals were notified about the data breach.
- Ransom Paid: $22 million in Bitcoin

Impact Assessment:

- Operational Disruption: the attack disrupted medical claim processing, delayed insurance verification and prior authorization. It had great impact on patient care by delaying necessary medical services.
- Financial Impact: the cyber-attack causes a financial strain on healthcare providers, especially smaller practices. It led to revenue cycle disruptions and cash flow problem. There was an increase in recovery efforts.
- Data Exposure: protected health information (PHI) including names, contact address, date of birth, social security numbers and medical information was compromised which was leaked to dark web.

Lessons Learned & Prioritized Remediation Roadmap:

- Implement multi-factor authentication for all remote access and critical systems

- Improve on network segmentation to limit lateral movement.
- Regular update and patching of systems to curb vulnerabilities.
- Robust endpoint detection and response (EDR) solutions should be deployed.
- Strong encryption for data at rest and data in transit should be implemented.
- Principle of least privilege for data access should be enforced.
- Conduct regular security audits and vulnerability assessment.
- Enhance information sharing and collaboration among healthcare organizations.
- Promotion of vendor diversification to reduce reliance on single vendors.
- Redundancy and failover capabilities for critical systems must be implemented.
- Establishment of clear standards and regulations for Cybersecurity in the healthcare industry.

Comparative Analysis: MOVEit Transfer Breach and Change Healthcare Ransomware

Similarities:

- Regulatory Exposure: According to important data protection rules (including HIPAA and GDPR), both occurrences sparked investigation and necessitated breach reports and compliance audits.
- Delayed Detection: Both breaches relied on internal or vendor detection and were not immediately detected by outside parties, exposing flaws in real-time threat monitoring.
- Third-Party Risk: The significance of supply-chain security was highlighted by the fact that both incidents involved flaws in third-party systems, specifically those of Change Healthcare as a service provider and MOVEit as a software vendor.
- Severe Impact: Both affected millions of people and vital services, resulting in extensive operational disruption, financial losses and reputational harm.
- Regulatory & Legal Fallout: Investigations, legal actions, and demands for more robust cybersecurity governance evolved out of each incident.

Differences:

Category	MOVEit Breach	Change Healthcare Breach
Attack Vector	A zero-day vulnerability in software for file transfers.	Ransomware exploiting credentials that have been compromised.
Industry	Multi-sector (finance, government, education)	Healthcare
Scope	Global, hundreds of organizations	U.S. focused, single large provider
Response	Patch deployment, breach notifications	Ransom payment, system rebuild
Data Type Exposed	Personal, Financial and Sensitive files	Patient health records, billing, prescriptions

Root Cause	Software Flaw and delayed Patching	Weak Access Controls and Network Segmentation
Public Perception	Viewed as a vendor failure	Viewed as a critical infrastructure failure

Recommendations & Remediation Roadmap

Recommendation	Owner	Timeline
Implementation of zero-trust architecture to limit lateral movement and unauthorized access	Chief Information Security Officer (CISO)	3 months
Comprehensive third-part risk assessments must be conducted and patching must be enforced	Risk & Compliance Team	3 months
Advanced threat detection tools like EDR SIEM should be deployed with continuous monitoring.	Security Operations Center (SOC)	6 months
Networks should be segmented with least privilege access control	Infrastructure Team	6 months
Regular update of Incident Response Playbook	Security Governance Lead	9 months
Conduct staff training on phishing awareness and credential hygiene	HR & Training Department	12 months

Sources:

1. https://orx.org/resource/moveit-transfer-data-breaches
2. https://www.ncsc.gov.uk/information/moveit-vulnerability
3. https://en.wikipedia.org/wiki/2023_MOVEit_data_breach
4. https://hadrian.io/blog/moveit-cyberattacks-timeline-of-the-largest-hack-of-2023
5. https://hyperproof.io/resource/understanding-the-change-healthcare-breach/
6. https://www.ama-assn.org/about/leadership/hard-lessons-learned-change-healthcare-breach
7. https://disb.dc.gov/page/change-healthcare-cybersecurity-incident
8. https://www.ibm.com/think/news/change-healthcare-22-million-ransomware-payment

Appendix A: Incident Timelines

MOVEit Breach

- May 28th, 2023: the vulnerability was discovered by Progress Software
- May 31st, 2023: the breach was disclosed to the public and path were released
- June–July 2023: Affected organizations begin breach notifications

Change Healthcare Attack

- February 21, 2024: Ransomware attack initiated
- February 22, 2024: Public disclosure and service disruption
- March 2024: Ransom paid and partial recovery begins

Appendix B: Regulatory Frameworks Overview

Regulation	Scope	Relevance
GDPR	EU data protection	MOVEit breach (EU victims)
HIPAA	U.S. healthcare data	Change Healthcare
HITECH	Health IT security	Change Healthcare
SOX	U.S. public companies	MOVEit-affected financial firms