**Slide 1: Title Slide**

**Title:** Data-in-Use: MOVEit Data Breach Case Study

**Nithish Sunkara**

Indiana Institute of Technology

IS5700 - Information Security and IT Governance

Changhao Chenli

April 1, 2025

**Slide 2: What is Data-in-Use?**

**Definition:**  
Data-in-use refers to active data being processed by applications, systems, or users. It resides in RAM, CPU, or cache memory and is vulnerable during manipulation.

**Examples:**

* Filling an online form (credit card, SSN, etc.)
* Real-time collaboration (Google Docs, MS Teams)
* AI/ML model training in the cloud

**Risks:**

* Memory scraping
* Insider threats
* Malware or unauthorized access

*Compared to data-at-rest or data-in-transit, data-in-use is the most exposed.*

**Slide 3: Case Study – MOVEit Data Breach (2023)**

**Incident Overview:**  
MOVEit Transfer, a file transfer tool by Progress Software, was exploited via a zero-day SQL injection vulnerability by the Cl0p ransomware group.

**What Was Affected:**

* Sensitive PII: names, SSNs, financial and contact info
* Over 62M individuals affected worldwide

**Major Victims:**

* Shell, BBC, British Airways, US Government Agencies

**Impact:**

* Severe reputational damage
* Regulatory and legal action (HIPAA, GDPR)
* Data leaked on the dark web

*The breach targeted data while in-use: being accessed or transferred.*

**Slide 4: Prevention & Recovery Strategies**

**If I were the IT Leader:**

**Prevention:**

* Deploy Runtime Memory Protection tools (e.g., Fortanix, Intel SGX)
* Apply Zero Trust principles
* Schedule regular code audits and threat modeling
* Use Behavior-based Intrusion Detection Systems (IDS)

**Recovery:**

* Isolate compromised systems
* Notify impacted stakeholders and regulators promptly
* Roll out emergency patches and disable affected services
* Conduct forensic investigations and lessons-learned review

*Layered defense plus rapid response = stronger resilience.*

**Slide 5: References**

1. CISA. (2023). MOVEit Transfer Exploit Advisory. https://www.cisa.gov/news-events/alerts/2023/06/01/ongoing-exploitation-moveit-transfer-zero-day
2. BleepingComputer. (2023). MOVEit Hack Hits Government Agencies. https://www.bleepingcomputer.com/news/security/moveit-transfer-hack-hits-us-government-agencies/
3. Progress Software. (2023). MOVEit Security Bulletin. https://www.progress.com/security/moveit-transfer