Lewis Joseph Feik
Security Awarness
Week 5 lab B

What Was Taken

Incident date	***Affected organization***	***What was taken?***	***What exploits were used?***	***How to prevent this security breach?***	***Reference source***
May-June 2023	*Multiple organizations using MOVEit (file transfer software)*	*Sensitive personal data of ~93 million individuals, including payroll data, home addresses, bank details, etc. (Wikipedia)*	*Zero-day SQL Injection vulnerability (CVE-2023-34362) in MOVEit Transfer; attackers also used web shells to exfiltrate data. (Google Cloud)*	*Patch management of third-party software; applying security updates immediately; monitoring external facing servers; vendor risk assessment; intrusion detection. (CSHub)*	
September 2022	*Uber*	*Access to internal systems, including infrastructure tools (AWS, GSuite), internal code / credentials via privileged accounts; Slack messaging, etc. (UpGuard)*	*Attack started with stolen credentials of an employee/contractor, MFA fatigue, social engineering to get the user to approve a push notification; then lateral move using privileged tools. (UpGuard)*	*Strong MFA (resistant to fatigue attacks), training about social engineering, restricting privileged credentials, monitoring unusual access, using zero-trust architecture, limiting access rights.*	

Lewis Joseph Feik
Security Awarness
Week 5 lab B

(ManageEngine Blog)