1. **MOVEit File Transfer Attacks (May 2023)**
    - **Type:** Data breach
    - **Methodology:** A vulnerability in the MOVEit file transfer tool was exploited by the Russian-speaking Clop group, leading to data theft without encryption, deviating from traditional ransomware tactics.
    - **Impact:** Over 2,600 organizations and 84 million individuals were affected, including government agencies and major corporations like IBM and Cognizant.
    - **Mitigation:** Most companies involved had to negotiate with the attackers, though it's unclear who paid the ransom. The attack is ongoing with significant data leak risks.
2. **Barracuda Email Security Gateway Attack (May 2023)**
    - **Type:** Exploit of vulnerability
    - **Methodology:** A critical vulnerability in Barracuda's ESG appliances was exploited by a Chinese state-linked group, UNC4841, compromising 5% of all active ESG devices.
    - **Impact:** U.S. government agencies were targeted, prompting Barracuda to advise clients to replace compromised devices.
    - **Mitigation:** Barracuda provided free replacements to affected clients and continued to advise complete device replacement.
3. **Microsoft Cloud Email Breach (June 2023)**
    - **Type:** Data breach
    - **Methodology:** Chinese hackers, tracked as Storm-0558, exploited a flaw in Azure Active Directory, targeting U.S. government email accounts, including high-profile officials.
    - **Impact:** 60,000 emails from U.S. State Department officials were compromised.
    - **Mitigation:** Microsoft identified and patched the flaw, though the breach spurred investigations into the company's security practices.
4. **3CX Supply Chain Attack (March 2023)**
    - **Type:** Supply chain attack
    - **Methodology:** North Korean-linked hackers compromised 3CX's communications software through an earlier supply chain attack on a financial firm, Trading Technologies.
    - **Impact:** 600,000 organizations using 3CX, including American Express and Coca-Cola, were potentially impacted.
    - **Mitigation:** The breach was detected and stopped within weeks, significantly reducing potential damage.
5. **Colonial Pipeline Ransomware Attack (May 2021)**
    - **Type:** Ransomware (DarkSide group)

- **Methodology:** A cyber extortion attack on Colonial Pipeline using ransomware led to fuel supply disruptions across the U.S. East Coast.
- **Impact:** Fuel shortages, panic buying, and a $4.4 million ransom payment.
- **Mitigation:** Colonial Pipeline paid the ransom, but the U.S. Department of Justice later recovered a portion of the payment.

6. **SolarWinds Supply Chain Attack (Discovered December 2020)**
    - **Type:** Supply chain attack
    - **Methodology:** Russian state-sponsored hackers injected malware into SolarWinds' Orion platform, gaining access to U.S. government agencies and corporations.
    - **Impact:** Affected U.S. federal agencies and Fortune 500 companies.
    - **Mitigation:** Detection came late, but wide-scale monitoring and patching efforts followed.
7. **Kaseya Ransomware Attack (July 2021)**
    - **Type:** Ransomware (REvil group)
    - **Methodology:** The REvil group exploited a vulnerability in Kaseya's IT management software, affecting 1,500 businesses globally.
    - **Impact:** Operations of multiple businesses were halted due to ransomware encryption, with a $70 million ransom demand.
    - **Mitigation:** Kaseya developed a patch, and REvil's servers were later taken down by global law enforcement agencies.
8. **Log4Shell Exploit (December 2021)**
    - **Type:** Remote code execution vulnerability
    - **Methodology:** Hackers exploited a zero-day vulnerability in Apache's Log4j, allowing them to remotely execute code and control affected systems.
    - **Impact:** This vulnerability impacted countless systems globally, including major tech companies like Amazon, Microsoft, and Google.
    - **Mitigation:** Urgent patches and updates were deployed, but the long-term impact is still being managed.
9. **T-Mobile Data Breach (August 2021)**
    - **Type:** Data breach
    - **Methodology:** Hackers exploited unsecured T-Mobile systems, stealing personal information of over 50 million customers.
    - **Impact:** Names, Social Security numbers, and other sensitive data were compromised.
    - **Mitigation:** T-Mobile offered affected customers credit monitoring services and enhanced its security measures.

10. **Uber Data Breach (September 2022)**

- **Type:** Social engineering attack
- **Methodology:** A hacker gained access to Uber's internal systems through a multi-factor authentication (MFA) fatigue attack, leveraging social engineering to bypass security.
- **Impact:** Sensitive employee information and corporate communications were exposed.
- **Mitigation:** Uber strengthened its internal security practices and reported the incident to law enforcement.