

Real-World Security Breaches - Categorized & Explained

Data Breaches (Personal Data Exposure)

Breaches where attackers stole personal information like names, emails, passwords, credit card data, etc.

1.1 — Yahoo Breach (2013–2014)

- **Impact:** 3 billion accounts compromised — the largest data breach in history.
- **What happened:** Attackers exploited weak security questions + poor encryption.
- **Data exposed:** Password hashes, emails, security question answers.
- **Root cause:**
 - Outdated hashing algorithm (MD5)
 - Lack of monitoring
 - Poor internal security culture
- **Lessons:**
 - Use modern hashing (bcrypt/argon2)
 - Multi-factor authentication (MFA)
 - Regular security audits

1.2 — Facebook 533M Scrape Leak (2021)

- **Impact:** 533 million users' phone numbers leaked.
- **What happened:** Misuse of a "contact import" feature allowed mass data scraping.
- **Data exposed:** Phone numbers, names, locations.
- **Root cause:** Insecure API rate limiting.
- **Lessons:**
 - Implement API throttling
 - Monitor unusual API usage patterns

1.3 — LinkedIn Data Scraping (2021)

- **Impact:** 700+ million user profiles scraped.
- **Root cause:** Public API allowed excessive access.

Ransomware Attacks

2.1 — WannaCry Ransomware (2017)

- **Impact:** 200,000+ computers in 150+ countries
- **What happened:** Used an NSA exploit called **EternalBlue** targeting SMBv1.
- **Root cause:** Missing Windows security patches.
- **Lessons:**
 - Patch systems regularly
 - Disable SMBv1
 - Network segmentation

2.2 — Colonial Pipeline Ransomware (2021)

- **Impact:** Shut down fuel pipeline across the U.S.; caused fuel shortages.
- **What happened:** A single **compromised VPN password** allowed attackers in.
- **Root cause:**
 - No MFA
 - Exposed VPN endpoint
- **Lessons:**
 - Mandatory MFA
 - Zero-trust network
 - Continuous credential monitoring

2.3 — Costa Rica Government Ransomware (2022)

- **Impact:** National emergency declared.
- **Reason:** Unpatched servers + legacy systems.

Cloud Security Failures (Misconfigurations)

Biggest cause of modern data breaches.

3.1 — Capital One AWS Breach (2019)

- **Impact:** 106 million customers affected.
- **What happened:**
 - A misconfigured **AWS WAF IAM role** allowed access to S3 buckets.
 - Attacker used **Server-Side Request Forgery (SSRF)** to access metadata server.
- **Root cause:**
 - Misconfigured IAM permissions
 - SSRF vulnerability
- **Lessons:**
 - IAM least privilege
 - Disable metadata v1
 - Strict AWS WAF monitoring

3.2 — Tesla Kubernetes Console Exposed (2018)

- **Impact:** Attackers used Tesla's Kubernetes system to mine cryptocurrency.
- **Cause:** Publicly exposed K8s dashboard without password.
- **Lessons:**
 - Never expose dashboards publicly
 - Use RBAC and network policies

3.3 — Microsoft Power Apps Leak (2021)

- **Impact:** 38 million records leaked
- **Cause:** Misconfigured OData API endpoints
- **Lesson:** Default settings must be secure

Supply Chain Attacks

Attackers compromise one trusted system to reach many victims.

4.1 — SolarWinds Orion Hack (2020)

- **Impact:** U.S. government + 18,000 organizations compromised.
- **What happened:**
 - Hackers inserted malware (*Sunburst*) into SolarWinds software update.
- **Root cause:**
 - Weak build pipeline security
 - Poor code-signing security
- **Lessons:**
 - Signed build verification
 - SBOM (Software Bill of Materials)
 - Build server isolation

4.2 — NotPetya (2017)

- **Impact:** Billions in damage; global companies shut down.
- **Cause:** Compromised updates in Ukrainian tax software.
- **Attack type:** Fake ransomware → actually data destruction.

Password & Credential Attacks

5.1 — Dropbox Employee Password Leak (2012)

- **Impact:** 68 million passwords leaked.
- **Cause:** Password reuse by an employee.
- **Lessons:**
 - Unique passwords
 - Enforce password managers

5.2 — Uber Breach (2022)

- **Impact:** Internal dashboards, AWS, GCP, Slack compromised.
- **What happened:**
 - Hacker social-engineered an employee
 - Got access to VPN
 - From VPN → admin credentials stored in PowerShell script
- **Root cause:**
 - Hardcoded credentials
 - No MFA protection
- **Lessons:**
 - Secrets rotation
 - No hardcoded passwords
 - Zero Trust

5.3 — LastPass Master Vault Breach (2022)

- **Impact:** Encrypted vaults stolen
- **Cause:** Engineer's home PC compromised → company vault accessed

Social Engineering Attacks

6.1 — Twitter BitCoin Scam (2020)

- **Impact:** Elon Musk, Obama, Apple, etc. accounts hacked.
- **Cause:** Social engineering of Twitter support employees
- **Lessons:**
 - Strong internal access controls
 - Employee training

6.2 — Google & Facebook Wire Fraud (2013–2015)

- **Impact:** \$121 million stolen
- **Cause:** Attackers impersonated hardware vendor (fake invoices).

Insider Threats

7.1 — Edward Snowden (2013)

- **Impact:** NSA classified data leak
- **Cause:** Abuse of privileged access
- **Lessons:**
 - Monitor privileged access
 - Just-in-time permissions

7.2 — Tesla Insider Sabotage (2018)

- **Impact:** Deleted configs + leaked manufacturing data
- **Cause:** Disgruntled employee
- **Lessons:**
 - Strict logging
 - Version control backup

Application Security Vulnerabilities

8.1 — Equifax Breach (2017)

- **Impact:** 147 million customers affected
- **Cause:** Unpatched Apache Struts vulnerability (CVE-2017-5638)
- **Root cause:**
 - Missed patch
 - No vulnerability scanning
- **Lessons:**
 - Continuous patching
 - CVE monitoring
 - Automated AppSec testing (SAST/DAST)

8.2 — Log4Shell (2021)

- **Impact:** Highest severity vulnerability in a decade
- **Cause:** Log4j library allowed remote code execution via logs
- **Lessons:**
 - Dependency scanning
 - SBOM
 - Automated patch testing

Financial & Banking Breaches

9.1 — Bangladesh Bank Heist (2016)

- **Impact:** \$81 million stolen via SWIFT
- **Cause:**
 - Malware on banking terminals
 - Weak firewall and network segmentation
- **Lessons:**
 - Isolated SWIFT systems
 - Endpoint monitoring

9.2 — JPMorgan Chase Breach (2014)

- **Impact:** 76 million households
- **Cause:** Missing two-factor authentication on a server

E-commerce & Retail Breaches

10.1 — Target POS Malicious Code (2013)

- **Impact:** 40 million credit cards stolen
- **Cause:**
 - HVAC vendor credentials stolen
 - Malware installed on POS terminals

- **Lessons:**
 - Vendor (third-party) security
 - POS segmentation
 - Application whitelisting

10.2 — eBay Breach (2014)

- **Impact:** 145 million accounts
- **Cause:** Compromised employee credentials