# Lab – What Was Taken? Security Breach Examples

This document fills out the Cisco lab table on major security breaches with example cases.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Incident date | Affected organization | What was taken? | What exploits were used? | How to prevent this security breach? | Reference source |
| 2017 | Equifax | Personal data of 147 million people (SSNs, DOB, addresses) | Unpatched Apache Struts vulnerability | Regular patch management, vulnerability scanning, and timely updates | https://www.ftc.gov/equifax-data-breach |
| 2013–2014 | Yahoo | 3 billion accounts compromised (emails, passwords, security Q&A) | Credential theft, weak encryption (MD5) | Use strong encryption (bcrypt/Argon2), multifactor authentication, monitor unusual access | https://www.bbc.com/news/technology-37670662 |
| 2021 | Colonial Pipeline | Operational systems halted, sensitive corporate data | Compromised VPN account, ransomware (DarkSide) | Use multifactor authentication, monitor remote access, implement incident response plans | https://www.cisa.gov/news-events/alerts/2021/05/11/darkside-ransomware-incident |