RZOLUT

Data Breach

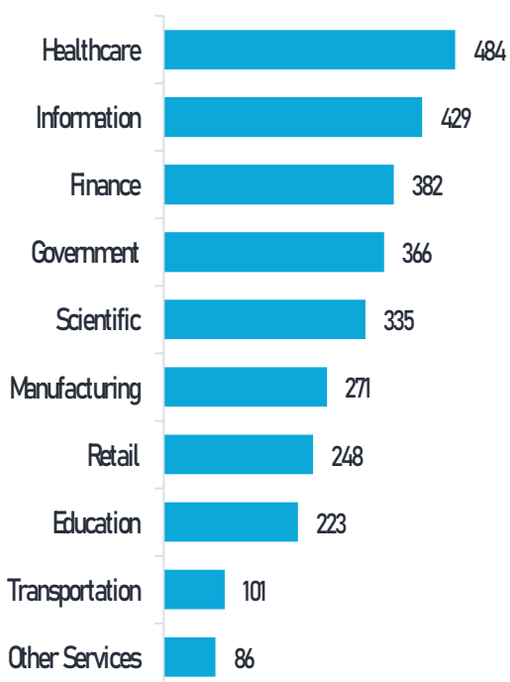
A security incident in which malicious insiders or external attackers gain unauthorized access to confidential and protected information. A data breach can result in the loss of personal information such as social security numbers, bank account or credit card information, health information, passwords, and emails. In recent years, there has been a dramatic increase in the number of data breaches, which have cost organizations millions of dollars.

Types

- Ransomware
- Information Theft
- Password Attacks
- Recording Keystrokes
- Phishing
- SQL Injection
- Skimming
- Eavesdrop Attack
- Malware or Virus
- Denial-of-Service Attacks
- Insider Threat

Impact

Number Of Breaches By Sector In 2020



Trends

- According to IBM, the average cost of a data breach was USD 3.86 million in 2020, and organizations took 280 days to identify and contain a breach
- Organizations in the US face the highest costs at an average of USD 8.64 million per breach
- The 2021 Thales Data Threat Report has found that almost half (45%) of companies in the US have suffered a data breach in the past
- Cybercrime is estimated to cost the world USD 10.5 trillion annually by 2025, according to Cybersecurity Ventures