Global security threat: A Decade of Global Cybersecurity Threats (2015–2024)

Overview

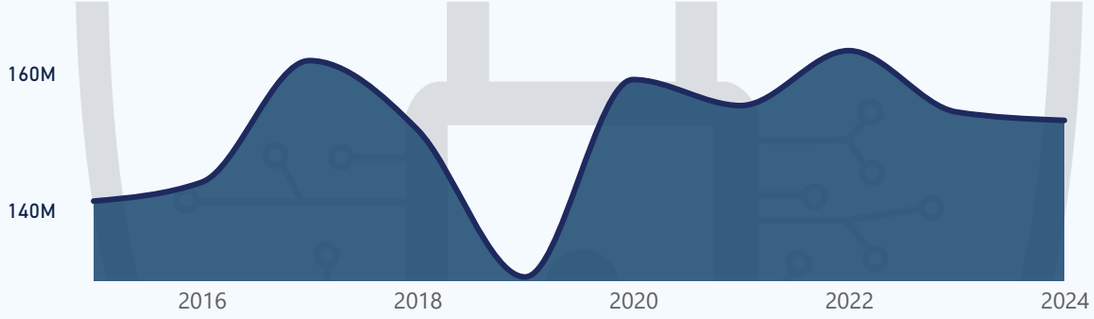
Impact Snapshot

Threats and Resolutions

Over the past decade, cybersecurity threats have evolved significantly, both in frequency and complexity. The dataset provides a deep dive into **3,000 cyber incidents** across countries, industries, and attack types, revealing crucial insights into the global threat landscape.

This 10-year snapshot of cybersecurity activity illustrates the **growing scale, complexity, and cost** of digital threats. By examining who is targeted, how attacks unfold, and what defenses are most effective, we can identify vulnerabilities, strengthen resilience, and guide smarter investments in cybersecurity.

Attack trend between 2016 to 2024



Total Financial Loss

$151.48bn

Ave. Financial Loss per Year

50.49M

Global security threat

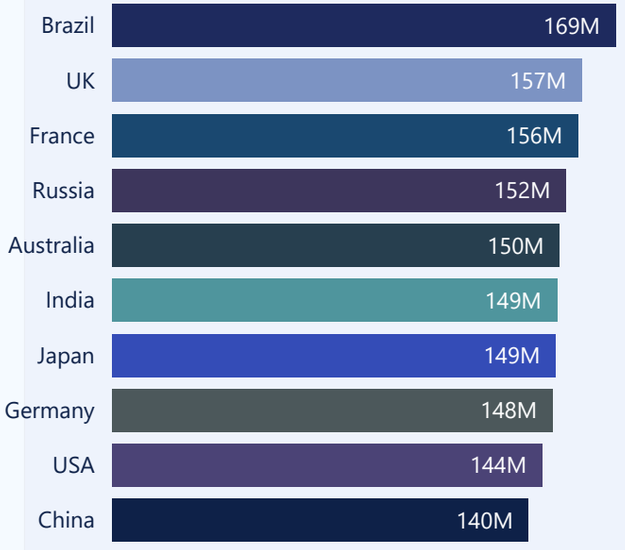
2015 — 2024

Overview

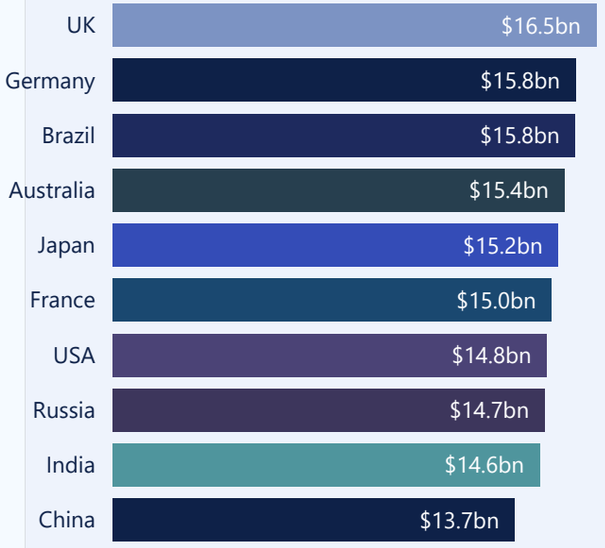
Impact Snapshot

Threats and Resolutions

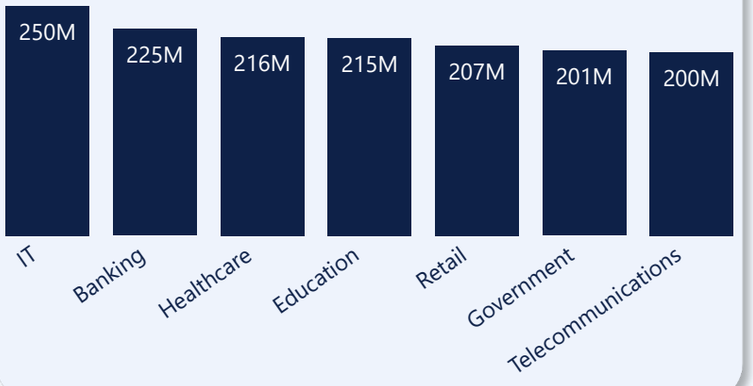
Total users affected by Countries



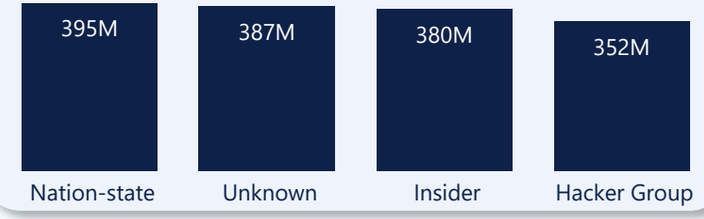
Total Financial lost by Country



Attacks by sector



Attack Source



- Brazil and the UK lead in cyberattack impact, with 169 million and 157 million users affected respectively.
- The UK suffers the highest financial loss of $16.5 billion, followed by Germany with $15.8 billion.
- IT, banking, healthcare, and education are the most targeted sectors. Nation-state attackers are responsible for the largest number of affected users (395 million), followed by unknown sources (387 million), while hacker groups cause the least impact with 352 million users targeted.

Global security threat

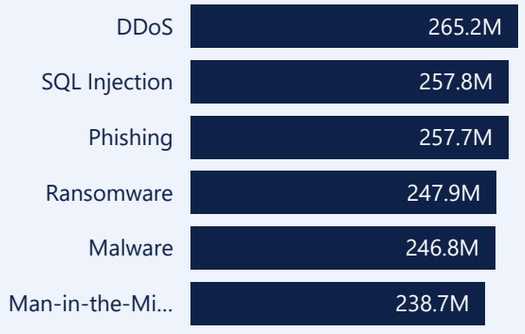
2015 — 2024

Overview

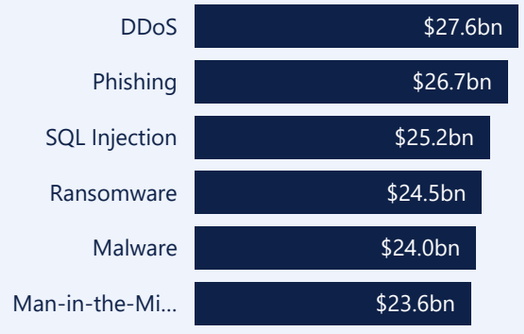
Impact Snapshot

Threats and Resolutions

Attacked method



Financial losses from attack type



- Over the years, DDoS, SQL injection, and phishing are the most common attack methods, affecting 265.2 million, 257.8 million, and 257.7 million users respectively. Among these, DDoS attacks cause the highest financial losses, followed by phishing. The most vulnerable factors exploited are zero-day vulnerabilities and weak passwords.
- VPN-based solutions lead in resolution speed, with an average of 36.9 hours to resolve attacks, closely followed by AI-based detection methods at 36.6 hours.

Security Vulnerability Type	Total_Attacked_Users	Total_Financial_Lost
Zero-day	396M	$40bn
Weak Passwords	379M	$37bn
Social Engineering	374M	$38bn
Unpatched Software	365M	$37bn

Average Attack resolution time by defence