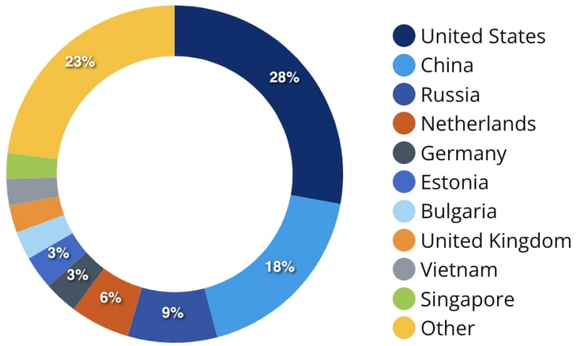
Top 10 Cybersecurity Threats

U.S. ARMY

The global annual cost of cybercrime is projected to reach $9.5 trillion by 2024 and damages are forecast to reach $10.5 trillion by 2025. These statistics highlight the ongoing challenge organizations face in protecting their systems and data from cybersecurity threats.

Top 10 Countries Originating Attacks



In 2023, there were 420 million cyberattacks, averaging 13 attacks per second, originating from 212 countries, with 28% coming from the US and a notable increase in attacks from China.

“Forty-eight percent of attacks came from [IP addresses] managed by [Internet services providers], 32% from organizations in business, government, and other sectors, and 10% from hosting or cloud providers. This reflects an increase in the use of compromised devices to launch attacks, whether directly or via ‘residential proxies,’”

Cyberattacks

Cyberattacks like malware, phishing, and ransomware pose the biggest threat to businesses, individuals, and governments.

Geopolitical Threats

The increase in cyberattacks has significantly altered geopolitics, serving as a new tool for both state and non-state actors to target governments, businesses, and individuals.

Deepfake Technology

Deepfakes use AI to create convincing fake videos, audio, and images, raising concerns about impersonating top-level executives with significant consequences.

IoT Vulnerabilities

Cloud-based threats target cloud systems, networks, and data to compromise availability, integrity, and confidentiality.

Cloud-Based Cyber Threats

The number of IoT devices is set to nearly double from 15.1 billion in 2020 to over 29 billion in 2030, leading to increased cyber threats.

Third-Party Cyber Threats

Third-party cyber threats are cybersecurity risks and attacks that come from external sources like suppliers, contractors, or outside organizations’ networks or systems.

Intelligent Social Engineering

Cybercriminals are combining social engineering with other attacks, such as ransomware, making it harder to detect and defend against these sophisticated and targeted attacks.

AI-Enhanced Cyber Threats

Cybercriminals can exploit AI systems to accelerate and execute more sophisticated attacks. Industries like finance, transportation, healthcare, and defense have becomes increasingly vulnerable to cyber threats,

Shortage of Professionals

The cybersecurity skills gap is a major issue, leaving companies vulnerable to cyber threats such as malware, ransomware, and data breaches.

Mobile Security Threats

Mobile devices like smartphones, tablets, and wearables are prime targets for cybercriminals due to frequent loss or theft, leading to unauthorized access to sensitive data.

Sources: Top 10 Cybersecurity Threats in 2024: How to Protect Your Data? (Techopedia)
Trends in cyberattacks, exploits, and malware 2023 Global Threat Roundup
Reporrends in cyberattacks, exploits, and malware 2023 Global Threat Roundup Report (Forescout Research)

Techopedia