Proxyrack

Global Cybercrime Report 2025

Global Cybercrime Report 2025

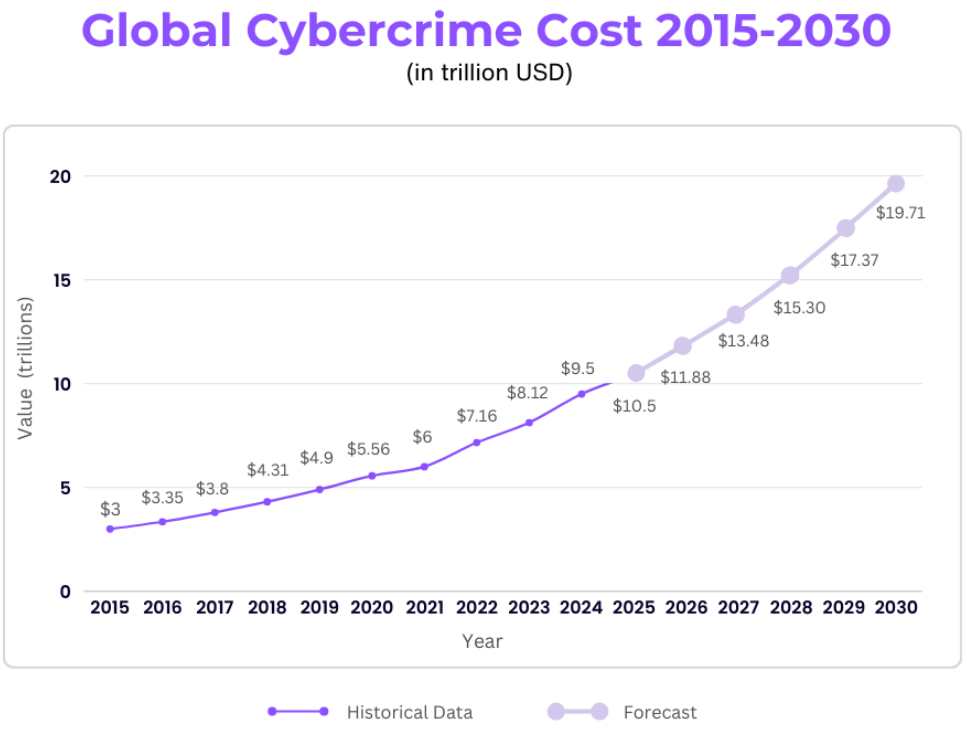
This report delves into the key trends, statistical insights, and geographical impacts of cybercrime, while exploring attack vectors and the industries and regions most affected.

Our report reveals that:

- The global cost of cybercrime will increase to $11.9 trillion USD in 2026, going all the way up to $19.7 trillion USD in 2030 - surpassing the current GDP of China.
- The 10 countries at highest and lowest risk: European and North American countries are among the safest, while Latin America and the Middle East are at high risk.
- Ransomware, phishing, and social engineering attacks continue to be the most popular ways of committing cybercrime, while some of the biggest rises in attacks have been in cryptojacking (136%) and software supply chain attacks (300%).
- The US (3.8%) is the country with most users rejected via the KYC process, followed by Vietnam (3.2%) and Indonesia (1.9%), according to Proxyrack internal data. They are also the three countries with most accounts suspended or locked due to potential malicious use.

Global Cybercrime Cost Forecast

Cybercrime continues to grow, posing one of the most severe threats to global security and economies. However, it's not growing linearly—our research shows that it's increasing exponentially.



Using global data from 2015 to 2024 to create a forecasting model, we predict that the cost of cybercrime around the world will go up to $11.9 trillion USD in 2026. By 2030, cybercrime will cost $19.7 trillion USD, eclipsing the current nominal GDP of China.

Katy Salgado, Operations Manager at Proxyrack and head of this cybercrime research, comments on what this means for businesses looking at cybersecurity measures to protect themselves:

"The exponential rise in the cost of cybercrime signals a growing global threat that will likely demand more advanced strategies and investments in cybersecurity. This trend emphasizes the need to stay proactive with preventative measures, enhance threat detection, and refine internal systems to address this escalating risk. It also highlights an increasing focus on resilience and adaptation to stay ahead of cybercriminal activities."

Cybercrime by Country

To assess the risk of cybercrime across countries, we looked at several factors. These include measures and indexes for cybercrime exposure, cybersecurity capabilities/preparedness, digital development, and legislation.

Top 10 countries most at risk from cybercrime

RANK	COUNTRY	BASEL AML INDEX	CYBERSECURITY EXPOSURE INDEX	NCSI	DIGITAL DEVELOPMENT LEVEL	GCI	CYBERCRIME RISK SCORE
1	Panama	5.81	5.69	4.32	5.16	3.35	4.86
2	Belarus	5.21	6.14	3.51	4.34	3.86	4.61
3	Chile	4.03	4.69	5.07	4.11	2.98	4.18
4	Costa Rica	4.58	4.38	4.68	3.77	2.49	3.98
5	Georgia	4.64	3.83	5.58	4.64	0.81	3.90
6	United Arab Emirates	5.70	3.59	5.97	3.11	0.00	3.68
7	Thailand	5.80	4.45	4.00	3.08	0.08	3.48
8	Saudi Arabia	5.28	3.90	4.08	2.92	0.00	3.24
9	Uruguay	4.07	3.48	3.92	3.15	0.53	3.03
10	Mauritius	5.03	2.00	3.75	3.99	0.00	2.95

With four countries on this list (Panama, Chile, Costa Rica, Uruguay), Latin America seems to have some of the biggest problems with cybersecurity. The Middle East also seems to have some issues; though both the UAE and Saudi Arabia got perfect GCI scores, showing their commitment to cybersecurity development, there is still a lot of work to be done to reduce their exposure and increase their readiness for cybercrime.

Top 10 countries least at risk from cybercrime

RANK	COUNTRY	BASEL AML INDEX	CYBERSECURITY EXPOSURE INDEX	NCSI	DIGITAL DEVELOPMENT LEVEL	GCI	CYBERCRIME RISK SCORE
1	Finland	2.88	0.11	1.56	1.73	0.00	1.26
2	France	3.52	0.23	0.91	2.00	0.10	1.35
3	Sweden	3.12	0.21	1.56	1.85	0.07	1.36
4	Denmark	3.56	0.12	1.43	2.17	0.00	1.45
5	United States	4.32	0.15	1.58	1.58	0.01	1.53
5	United Kingdom	3.63	0.21	1.56	2.27	0.00	1.53
6	Norway	3.50	0.13	1.17	2.78	0.30	1.58
7	Canada	4.25	0.21	1.25	2.15	0.68	1.71
8	Spain	3.88	0.21	3.25	1.98	0.03	1.87
8	Germany	4.21	0.24	2.50	1.79	0.62	1.87

Meanwhile, Europe leads the way in cybersecurity, with Nordic countries scoring especially well. France, the UK, Spain and Germany are also among the lowest-risk countries, with the US (notwithstanding its list of cybercrime hot spots) and Canada rounding off the list.

Katy thinks higher and lower-risk countries can tackle cybersecurity by focusing on differing priorities:

“This data on cybercrime risk by country shows how factors like cybersecurity readiness, digital infrastructure, and exposure vary widely around the world. This information highlights which regions may be more susceptible to cyber threats, helping guide strategic planning and response frameworks. Higher-risk countries may require more intensive security protocols and monitoring, while lower-risk countries often benefit from stronger digital infrastructure and robust cybersecurity practices. This perspective assists in allocating resources to support safer digital environments across different markets.”

Cybercrime Trends

Cybercrime has expanded both in scale and sophistication, with attackers continually refining their tactics. The global cybersecurity landscape is challenged by ransomware, phishing, malware, and cryptojacking, alongside other emerging threats.

Ransomware: A Continuing Menace

Ransomware continues to be one of the most prominent forms of cybercrime in 2024:

- **Ransomware Attacks** are projected to grow by **57%** year-over-year, with global damages forecasted to reach **$265 billion annually by 2031**.
- **32%** of global data breaches were due to ransomware in 2023.
- The average ransom demand increased from $5 million in 2020 to **$8 million in 2023**, as threat actors leverage more aggressive tactics.
- **Krebs on Security** notes that **double extortion** techniques, where attackers exfiltrate sensitive data before encrypting systems, have become the norm.
- **Germany**, **Saudi Arabia**, and **China** were among the hardest-hit countries in 2023, with hundreds of organizations forced to pay ransoms due to inadequate security controls.

Phishing and Social Engineering Attacks

Phishing remains one of the most prevalent attack vectors. In 2023:

- Phishing accounted for **36%** of all breaches worldwide, and **83%** of organizations reported experiencing phishing attempts.
- The rise of **spear-phishing**, where attackers target specific individuals or businesses, led to over **$1.8 billion** in business losses, often using email compromise.
- Phishing-as-a-Service (PhaaS) platforms are making it easier for attackers to launch large-scale campaigns.

Emerging Cyber Threats

As the digital world evolves, cybercriminals have adapted new methods of attack, exploiting trends such as cryptocurrency and cloud adoption.

Cryptojacking

Cryptojacking has surged as a favored attack vector in 2023:

- Cryptojacking is becoming a preferred method of attack. **CyberScoop** reports a **136% increase** in cryptojacking incidents, with attackers focusing on high-performance computing environments.

- Incidents of cryptojacking, where hackers secretly use a victim's computing resources to mine cryptocurrency, rose by **117%.**
- **89.4%** of cryptojacking malware was based on **XMRig**, a popular cryptocurrency mining tool.
- Cryptojacking attacks are now frequently targeting **cloud infrastructures** due to insufficient security measures.

Supply Chain Attacks

Supply chain vulnerabilities became a significant concern:

- In 2023, attacks targeting software supply chains increased by **300%**, with attacks like the **Kaseya breach** impacting over 1,500 organizations.
- Dark Reading emphasizes that **supply chain attacks** have grown by **300%** in the last year. Attackers are targeting vulnerabilities in third-party software and service providers to infiltrate high-value targets.
- Notable incidents, such as the **SolarWinds** and **Kaseya** breaches, have led to significant efforts to bolster supply chain security.

AI-Powered Cybercrime

- **AI-driven attacks** are growing in sophistication, with adversaries using artificial intelligence for **automated phishing** and **malware development**, according to **The Hacker News.**

Katy sees certain ways to prepare for these threats:

"The rise in supply chain attacks and cryptojacking underscores the importance of securing cloud environments and third-party vendors. Developing and implementing measures to mitigate these threats should be a top priority for organisational security."

Impact on Businesses and Individuals

Financial Impact

- Small and medium-sized enterprises (SMEs) are disproportionately affected, with **47%** of all cyberattacks targeting these businesses, resulting in devastating financial consequences.
- On average, data breaches cost businesses **$4.45 million** per incident in 2023, up by **10%** from the previous year.

Data Breaches

- The total number of records exposed in data breaches is set to exceed **40 billion** in 2024, as organizations struggle with securing personal information and sensitive data.

- Cloud-based services are increasingly targeted, with **93%** of companies reporting challenges related to rogue cloud apps and improper configurations.

Katy thinks SMEs need to be particularly vigilant:

“This data underscores the significant financial and operational risks posed by cybercrime, particularly for SMEs, which are more frequently targeted. Strengthening defenses for SMEs and ensuring proper cloud configurations should be top priorities to mitigate potential financial losses and reputational damage.”

Cybersecurity Measures and Defense

Investment in Cybersecurity

Despite growing threats, cybersecurity investments are lagging:

- Only **50%** of businesses in the US have full cyber insurance coverage.
- In the UK, just **23%** of businesses have a formal cybersecurity strategy.
- Globally, businesses that invest in **employee training** reported **30%** fewer successful attacks, showing the importance of education in cybersecurity defenses.
- **Dark Reading** and **Krebs on Security** advocate for widespread adoption of the **Zero Trust model**, which requires verification for every user and device, regardless of location, to mitigate insider threats and lateral attacks.
- Advanced technologies like **Extended Detection and Response (XDR)** and **AI-driven threat detection** are now critical investments for organizations looking to stay ahead of evolving threats.

Government and International Cooperation

Governments are taking action to strengthen their defenses:

- The **European Union** has introduced the **NIS2 Directive** to improve national cybersecurity strategies and promote information sharing between member states.
- In the US, the **Cybersecurity and Infrastructure Security Agency (CISA)** has ramped up its initiatives, aiming to protect critical infrastructure from growing cyber threats.

Cybersecurity Talent Shortage

- The global shortage of cybersecurity professionals remains a major challenge. **Cybersecurity Ventures** estimates a **3.5 million** workforce gap by 2025, urging governments and businesses to invest in training and talent acquisition.

The future of cybersecurity lies in the hands of global cooperation, stricter regulations, and heightened awareness. As cybercriminals refine their methods and expand their reach, both businesses and governments must prioritize the defense of digital infrastructures.

The **key to combating cybercrime** will be investment in technology, strong regulatory frameworks, and the development of a cybersecurity culture that includes **awareness, education, and collaboration** across sectors and regions.

By adopting **Zero Trust** policies, investing in **AI-powered defenses**, and securing **supply chains**, organizations can mitigate their risk exposure and protect critical infrastructures.

Top Recommendations:

- Strengthen **multi-factor authentication** (MFA) practices.
- Invest in **cybersecurity training** for employees to reduce human error.
- Implement **advanced threat detection** technologies such as **XDR**.

Katy identifies key areas that require the most attention:

"This data reveals critical gaps in cybersecurity investment, particularly in insurance, strategies, and employee training. The global shortage of cybersecurity talent emphasizes the need for better training and hiring strategies. To combat growing threats, organizations must adopt advanced technologies, strengthen MFA, and prioritize cybersecurity culture and cross-sector cooperation."

Proxyrack: Insights from Internal Data

As a proxy provider, our services include residential proxies and datacenter proxies, which could be targeted or misused in various ways by cybercriminals to commit the types of attacks outlined in current cybercrime trends:

1. **Ransomware and Malware Distribution**: Attackers may use proxies to hide their identity and location while deploying ransomware or malware to unsuspecting victims. By anonymizing their traffic, they can evade detection and prolong their malicious campaigns.
2. **Phishing and Social Engineering**: Proxies can be exploited by attackers to mask their origin when sending phishing emails or launching spear-phishing attacks. This makes it harder for victims or cybersecurity teams to trace the source of these attacks and block malicious IP addresses.
3. **Cryptojacking**: Proxies might be used to conceal cryptojacking activities, allowing attackers to mine cryptocurrency on compromised systems without being easily traced. Cloud infrastructures, in particular, are prime targets for such attacks due to the large computing resources available.
4. **Supply Chain Attacks**: Proxies can facilitate supply chain attacks by hiding the attacker's true location when infiltrating third-party service providers or software vendors. By masking their IP, attackers can bypass certain security measures and launch attacks on critical infrastructure.
5. **AI-Powered Cybercrime**: Proxies could be leveraged to deploy AI-driven attacks, such as automated phishing campaigns or the distribution of AI-generated malware. These proxies make it difficult to trace or shut down the source of these attacks, complicating the efforts of cybersecurity teams.

In each of these cases, it's critical for a proxy provider to have strong anti-abuse measures in place, such as monitoring for suspicious activity, implementing KYC protocols, and locking accounts linked to potential misuse.

These are the **top 10 countries** from our customer database where users are being **suspended or locked** due to potential malicious use of our services.

Account Rejection/Suspension by Country

	KYC-REJECTED PERCENTAGE	SUSPENDED PERCENTAGE
United States	3.75%	12.62%
Vietnam	3.24%	10.33%
Indonesia	1.86%	17.57%
Russian Federation	0.98%	1.71%
Hong Kong	0.80%	2.04%
Germany	0.62%	1.86%
India	0.40%	2.73%
Pakistan	0.36%	3.86%
United Kingdom	0.36%	0.84%
Brazil	0.22%	0.76%

One critical security measure for our services is the implementation of a Know Your Customer (KYC) process. A **KYC** process enhances security, ensures compliance, protects against abuse, and contributes to a better overall user experience. When your proxy provider uses a KYC process, you can be confident that they are committed to maintaining a safe, reliable, and high-quality service.

Accounts may be **locked** for various **reasons** to prevent malicious use of our services, including trial abuse, links to suspicious or fraudulent accounts, malicious request pattern recognition automation, chargebacks, KYC (Know Your Customer) issues, use of disposable email addresses, and high-risk transactions. This process is essential for maintaining the integrity of our platform, safeguarding user data, and reducing the risk of fraud.

Given the rising cybersecurity threats, proactive measures like locking accounts in our services are essential to safeguarding against malicious activity. As investments in cybersecurity lag—such as only 50% of US businesses having full cyber insurance and a

global shortage of cybersecurity professionals—businesses must rely on effective security protocols. Locking accounts linked to trial abuse, suspicious activity, or high-risk transactions aligns with the Zero Trust model, ensuring that every user and device is verified. This approach, coupled with advanced threat detection technologies, helps prevent breaches and protects our services from potential misuse.

Methodology

Global Cybercrime Cost Forecast

We used Cybersecurity Magazine estimations of the global cost of cybercrime for 2015 ($3 trillion USD), 2021 ($6 trillion USD), 2024 ($9.5 trillion USD) and 2025 ($10.5 trillion USD) as base data points. From these, we derived an exponential growth model to estimate the missing years and to project a forecast until 2030.

Cybercrime Country Rankings

We used the Human Development Index for our seeding list, using countries with a high human development score. We then removed any countries with missing data.

We used the Basel AML Index for the Basel AML Index scores.
We used the CEI 2020 for the Global Cybersecurity Exposure Index.
We used the NCSI for the National Cyber Security Index and Digital Development Level.
We used the ITU Global Cybersecurity Index 2024 for the GCI score, measuring the commitment of countries to cybersecurity.

We put this data into a weighted table, giving each factor a normalized score out of ten. We then took an average of these scores to provide each country's overall cybercrime risk score.

Other Sources

https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

https://aag-it.com/the-latest-cyber-crime-statistics/

https://www.upguard.com/blog/cybersecurity-websites

https://thehackernews.com/2024/10/from-misuse-to-abuse-ai-risks-and.html