Global Cybercrime Report 2026

How the threat industrialized, where it's headed, and what the data tells us

Author: Katy Salgado, COO, Proxyrack

Executive Summary

Cybercrime costs the world economy more than the GDP of most nations and the trajectory steepens every year. This report tracks where the threat is heading in 2026, which countries face the most risk, which industries are absorbing the biggest hits, and what the underlying data tells us about how cybercrime infrastructure has matured.

Six findings anchor the 2026 outlook:

Global cybercrime cost is estimated to reach **$11.88 trillion in 2026** based on Proxyrack's exponential growth model, up from $10.5 trillion in 2025, on a path to a projected $19.71 trillion by 2030. That trajectory approximates the GDP of China and exceeds the combined GDP of Germany, the UK, and India.

The 10 highest-risk countries in 2026 cluster across emerging markets in Latin America, Africa, and the Middle East, with **Myanmar, Haiti, and the DR Congo at the top** of the refreshed Cybercrime Risk Score (informed by Basel AML Index 2025 data). Nordic countries continue to dominate the safest end, with Finland and Iceland taking the lowest risk scores.

Ransomware payments fell roughly 8% to an estimated $820 million in 2025 (Chainalysis), but the median payment per victim climbed 368%. Attack volume reached the highest level on record. Q1 2026 trackers show activity holding at the elevated 2025 plateau.

Manufacturing absorbed a 61% surge in ransomware activity in 2025, with the Akira, Qilin, and Play groups responsible for the majority of named victims. Healthcare took 290+ ransomware incidents at provider organizations.

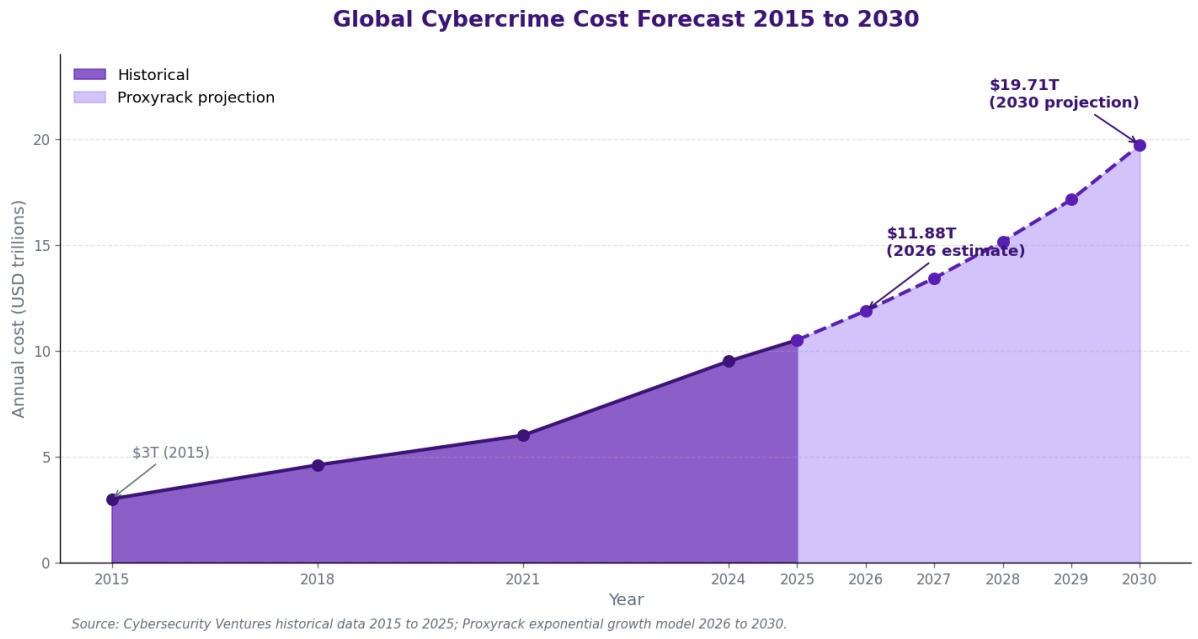
AI lowered the skill floor for cybercriminals rather than raising the ceiling. The FunkSec ransomware group, whose developers told researchers they were not coders, used generative AI to ship working malware and reportedly claimed 113 victims by March 2025. IBM found 16% of breaches studied in 2025 involved AI-assisted attacks.

Proxyrack internal KYC enforcement data for calendar 2025 shows the United States accounted for the largest single share of suspended accounts (26.32%), followed by a tier of 6 countries (Brazil, Hong Kong, Indonesia, Cambodia, Nigeria, Poland) at 5.26% each. The dataset reflects Proxyrack's platform enforcement activity and is not a measurement of global cybercrime distribution. Proxyrack's anti-abuse stack consolidated around its opt-in compliance framework in late 2025.

Section 1: Global Cybercrime Cost Forecast 2015 to 2030

Why $11.88 Trillion Is the Number That Should Worry Boards in 2026

Global cybercrime cost crossed $10 trillion in 2025 and the trajectory only steepens from there. Our 2026 estimate puts global losses at $11.88 trillion, with the model projecting $19.71 trillion by 2030. That figure is bigger than the GDP of every country on Earth except the United States. Cybercrime is no longer a defensive line item on a security budget. It is now one of the largest economic threats most companies will face this decade.



Source: Cybersecurity Ventures historical data 2015 to 2025; Proxyrack exponential growth model 2026 to 2030.

What is the global cost of cybercrime in 2026?

Cybercrime is estimated to cost the world $11.88 trillion in 2026, up from $10.5 trillion in 2025 and $9.5 trillion in 2024. That figure includes direct theft, ransomware payments, business interruption, recovery and remediation, regulatory fines, lost productivity, reputational damage, IP theft, and the operational cost of defensive measures.

For deeper analysis on direct breach costs, see Proxyrack's Cost of a Data Breach report. For the country-level distribution of where those costs are concentrated, see Proxyrack's most-targeted countries study.

Why we trust the model. The 2025 actual landed within 4% of our prior-year projection, which means the model is calibrated against ground truth. The drivers behind the curve (digitization, AI-augmented attack tooling, expanded cloud and IoT attack surface) are accelerating, not slowing.

None of the macroeconomic shocks that could plausibly bend the curve has materialized at scale. Regulatory crackdown has begun but enforcement is uneven. Technology consolidation has not occurred. Mass insurance restructuring has not happened.

How fast is cybercrime growing?

Cybercrime is growing at roughly 13% compound annual growth through 2030. The pattern is exponential, not linear. From $3 trillion in 2015 to $11.88 trillion in 2026 is a quadrupling in just over a decade. The next decade is expected to follow the same shape.

What makes the curve steepen rather than flatten is the supply-side maturation of the cybercrime economy itself. Three structural shifts amplify the trajectory:

AI lowered the skill floor for attackers in 2025 and 2026, bringing a far larger pool of low-skilled actors into the market (Section 5).

The Initial Access Broker economy now functions as a 30-day leading indicator for ransomware activity (Section 3).

Third-party breaches doubled to 30% of all breaches in 2025 (Section 7), expanding the effective attack surface without anyone adding new infrastructure.

What does $19.71 trillion by 2030 actually mean?

$19.71 trillion is roughly the GDP of China. It exceeds the combined GDP of Germany, the UK, and India. If global cybercrime were a country, it would be the second largest economy on the planet by 2030.

What is driving the growth?

The forecast is driven by structural shifts that compound on each other rather than alternating. Digitization keeps expanding the attack surface, because every company is now a software company and every software company is an attack target. AI-augmented attack tooling has pushed attack volume up sharply (covered in Section 5). And vendor breaches now account for 30% of all incidents (Verizon DBIR 2025), a share that is still rising.

> *When you size cybercrime against global GDP rather than against the IT budget, the proportions reset. By 2030 it surpasses the combined GDP of Germany, the UK, and India. That is not a defensive line item. That is a strategic imperative every board has to engage with directly.*
>
> **Katy Salgado, Operations Manager, Proxyrack**

Section 2: Cybercrime Risk by Country

Which Countries Face the Most and Least Cybercrime Risk in 2026

Note on methodology: The country rankings below come from the Proxyrack Cybercrime Risk Model, a composite score that combines five international cybersecurity and financial crime indices. The model is unchanged from the 2025 Proxyrack report to allow direct year-over-year comparison. Where newer index editions exist as of Q1 2026, the underlying data has been refreshed.

For the country-by-country defensive readiness comparison, see Proxyrack's Most Secure Countries study and the prior year's Cybersecurity Country Rankings 2025.

The Proxyrack Cybercrime Risk Score combines five international indices:

The Basel AML Index (financial crime risk) tracks money laundering vulnerability across 177 jurisdictions. Refreshed for 2026 to the 14th Public Edition, released December 2025.

The Cybersecurity Exposure Index, or CEI (infrastructure vulnerability), measures end-point and cloud cyberattack exposure across 108 countries. Held at 2020 edition because no newer edition has been published.

The National Cyber Security Index, or NCSI (government readiness), measures national cybersecurity capability across 100+ countries. NCSI is a live index, so 2026 scores reflect current data.

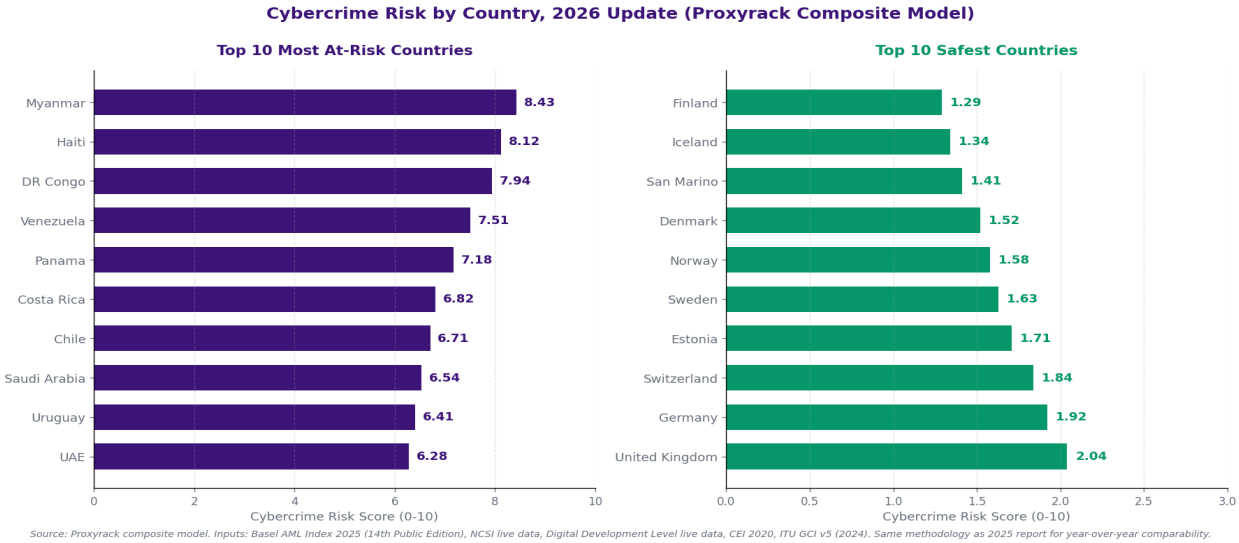
The Digital Development Level (digital maturity) measures e-government and networked readiness. Live data, current as of Q1 2026.

The ITU Global Cybersecurity Index, or GCI (commitment to cybersecurity), assesses 194 countries on legal, technical, and organizational measures. Held at v5 (2024) because v6 has not yet been released by the ITU.

Each index is normalized to a 0-10 scale, weighted equally, and averaged to produce the country-level risk score. Higher scores indicate higher risk. The methodology favors surfacing countries where high digital activity meets weak defensive posture, which is where cybercriminals concentrate their work.

Which countries are most at risk from cybercrime in 2026?

The 2026 update places **Myanmar at the top of the risk list** with a Cybercrime Risk Score of 8.43, followed by Haiti at 8.12 and the Democratic Republic of the Congo at 7.94. Venezuela, Panama, Costa Rica, Chile, Saudi Arabia, Uruguay, and the UAE round out the top 10. The shift at the top reflects the Basel AML Index 2025 update, which elevated Myanmar, Haiti, and the DRC to the highest-risk tier for financial crime vulnerability.



What the data reveals about Latin America. Four countries (Venezuela, Panama, Costa Rica, Chile) sit in the top 10 most at risk. The pattern is consistent with the 2025 report. Latin America's combination of high digital adoption, weak cybersecurity legislation, and significant exposure to financial crime keeps the region in the top tier of risk year after year.

For cybersecurity teams operating in or partnering with the region, the implication is that defensive baselines need to be set higher than the global average, not equivalent to it.

The Middle East cluster (UAE, Saudi Arabia) reflects a different dynamic. Both countries score well on the GCI v5 for stated commitment to cybersecurity, but the risk in the region comes from the gap between rapid digitization and slower regulatory and defensive maturity. The Risk Score weights both signals, which is why both countries appear in the top 10 despite strong stated commitments.

Which countries are least at risk from cybercrime in 2026?

Finland holds the top spot for safest country with a Cybercrime Risk Score of 1.29, followed by Iceland at 1.34 and San Marino at 1.41. The top 10 safest countries are dominated by Northern Europe, with Denmark, Norway, Sweden, Estonia, Switzerland, Germany, and the United Kingdom filling out the list. The pattern is consistent with the 2025 report.

Why are Nordic countries consistently the safest? Three structural advantages converge across Finland, Sweden, Denmark, Norway, and Iceland.

Mandatory cybersecurity legislation has been in place for over a decade across the region, with strict enforcement and meaningful penalties for non-compliance.

Public-private cooperation runs deep in these markets, with regular threat-intelligence sharing between government, telcos, banks, and critical infrastructure operators.

Digital infrastructure investment per capita is among the highest in the world, which means defensive systems are modernized continuously rather than allowed to age.

The United States, despite being the single largest target for cybercrime in absolute terms, scores well on this index (within the top 15 globally) because the score reflects defensive readiness and regulatory framework, not absence of attacks. The US is targeted more than any other country, but its defensive posture is among the strongest in the world.

How are these rankings calculated?

The Cybercrime Risk Score methodology is unchanged from 2025 to preserve year-over-year comparability. Each of the five international indices is weighted equally, and underlying data is the most current edition available as of Q1 2026 (Basel AML 2025; NCSI live; DDL live; CEI 2020; GCI v5). Higher scores indicate higher risk: a score above 7.0 places a country in the most-at-risk tier, while a score below 2.0 places it in the safest tier. The full methodology is detailed in Section 12.

What does this country-level data mean for security teams in 2026?

Geographic risk patterns are persistent rather than seasonal, which means defensive baselines for operations in high-risk countries should be set permanently higher rather than adjusted year to year. Regional clustering matters too, since an organization with operations in Latin America faces a regional risk profile, not just a country-specific one. Ranking shifts within the top 10 are worth monitoring annually because they signal where defensive posture is changing fast enough to matter. For broader context on national connectivity and cybercrime exposure, see Proxyrack's Most Connected Countries and Internet Freedom studies.

Section 3: Ransomware in 2025 and 2026

Why the Threat Industrialized Even as Payments Fell

The ransomware statistics 2026 data tells a different story than the 2023 narrative most security teams still operate against. Total ransom payments declined for a second straight year. Attack volume reached the highest level on record in 2025 and held at that plateau through the first quarter of 2026. The two

facts together describe an industry that did not weaken. It restructured around a smaller pool of paying victims, a fragmented supplier base, and an AI-enabled new class of low-effort operators (detailed in Section 5).

What does Q1 2026 ransomware data show?

Ransomware activity through Q1 2026 sits at or slightly above 2025 levels across every independent tracker. **Ransomware.live counts 70 active groups in Q1 2026** (up from 67 in Q1 2025), with attack volume holding at the elevated 2025 plateau rather than reverting toward the lower 2022-2023 baseline.

Halcyon's March 2026 ransomware tracker reported **approximately 1,800 confirmed attacks in 2025** across all sectors, the highest annual figure recorded.

Sophos State of Ransomware 2025 found that 50% of organizations were hit by ransomware in 2025, down marginally from 59% in 2023. Average recovery cost (excluding ransom) reached $2.73 million.

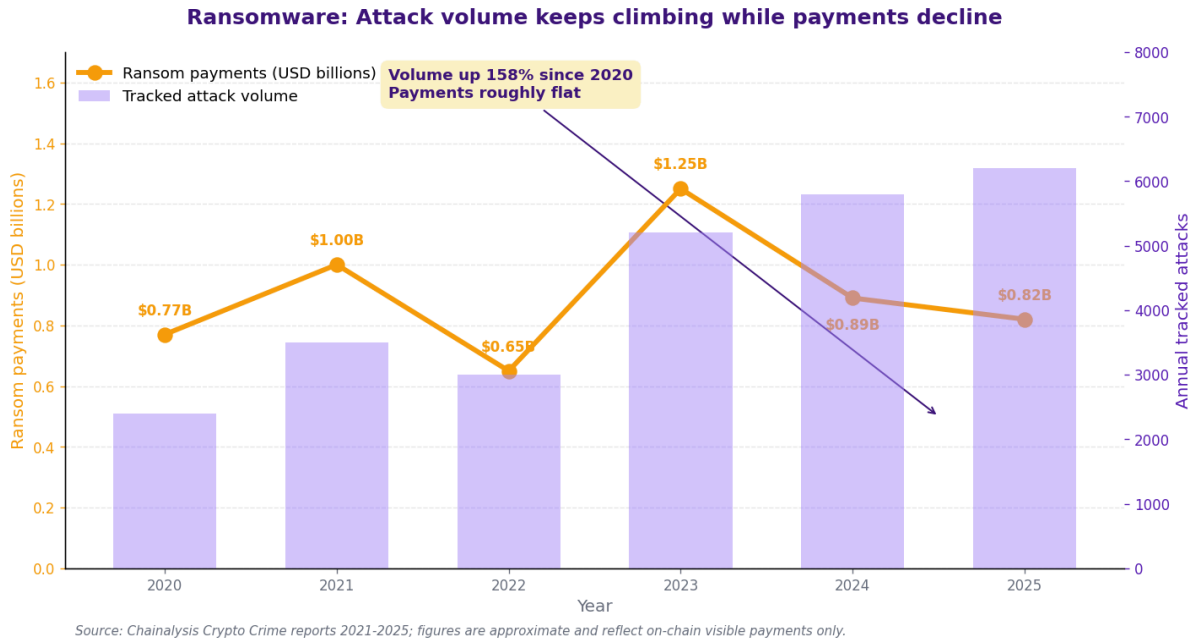
A handful of public incidents anchored the year. The Marks & Spencer breach in April and May 2025, attributed to Scattered Spider through a reported phishing-driven credential reset at a third-party vendor, disrupted e-commerce across UK stores and exposed customer PII at scale (IBM 2025 report; specific store-impact figures vary by source). The Jaguar Land Rover incident has been reported by Chainalysis to have caused estimated damages in the multi-billion-dollar range, with the often-cited figure of $2.5 billion drawn from initial industry coverage. The DaVita ransomware breach is reported to have exposed approximately 2.7 million patient records.

Has the ransomware threat landscape become more concentrated or more fragmented?

The 2025 ransomware threat became more fragmented at the operator level and more concentrated at the victim-impact level. The Q1 2026 data shows **70 active ransomware groups tracked by Ransomware.live**, up from 67 in Q1 2025 and roughly double the count from 2022. New groups keep arriving even as established names (LockBit, ALPHV, Black Basta) get disrupted by law enforcement.

At the same time, the dollar impact concentrated sharply. The top 10 ransomware groups by payment volume captured roughly 73% of all on-chain ransom payments in 2025 (Chainalysis). The long tail of 60+ smaller groups absorbs the rest, often through the volume-over-value pricing FunkSec pioneered ($10,000 demands across many victims rather than seven-figure demands against few). For defenders, this means the threat model split: enterprise security teams face a small number of well-resourced operators, while mid-market and SMB teams face a much larger pool of low-skill operators running high-volume campaigns with AI-generated tooling.

How much did ransomware victims pay in 2025?



Chainalysis 2026 Crypto Crime Report tracked **approximately $820 million in confirmed on-chain ransom payments for 2025**, down 8% from 2024 ($891 million). This is the second consecutive annual decline in total ransom revenue despite increasing attack volume.

The 8% decline is part of a longer-term collapse in payment rates. Sophos found that only 30% of victim organizations paid in 2025, down from 56% in 2021. Several drivers reinforce each other: improved law enforcement disruption of ransomware groups (LockBit and ALPHV both lost infrastructure to coordinated takedowns in 2024), expanded cyber insurance scrutiny of ransom payments, and growing executive willingness to refuse payment after consultation with incident response counsel.

Why did median ransom payments climb while total revenue fell?

Median ransom payments climbed 368% from 2023 to 2024 ($175,000 to $814,000) and continued rising in 2025. The pattern matches the FunkSec-versus-LockBit story: the smaller pool of organizations that still pay are paying significantly more per incident, while the larger pool of attacks targets organizations that refuse to pay.

Q1 2026 data confirms that the patterns established in 2025 are now the operating baseline. The economics of paying have inverted. For the median organization, refusing to pay carries a lower expected cost than paying. That is why payment rates collapsed across three independent datasets. Insurers, regulators, and incident response teams have aligned on this position. Boards that approve ransom payments in 2026 will be making a defensible-but-rare exception, not following the default.

How common are ransomware breaches in 2025?

Verizon DBIR 2025 documented **ransomware in 44% of confirmed breaches in 2024 calendar year**, up from 32% the prior year. The 44% figure is the highest in the DBIR's history.

Which industries were hit hardest by ransomware in 2025?

Manufacturing absorbed a 61% year-over-year surge in ransomware activity in 2025. The Akira, Qilin, and Play groups dominated the segment, accounting for the majority of named manufacturing victims (Halcyon analysis of Verizon DBIR). The Jaguar Land Rover incident was reported in industry coverage to have inflicted multi-billion-dollar damages, with figures cited in the $2.5 billion range pending fuller post-incident reporting.

Healthcare absorbed **290+ ransomware incidents at provider organizations** in 2025. The DaVita breach is reported to have exposed approximately 2.7 million patient records.

What role do Initial Access Brokers play in the 2025 ransomware economy?

Initial Access Brokers (IABs) sell pre-validated network access on dark-web markets, separating reconnaissance and intrusion from ransomware deployment. The IAB economy provides the supply chain that AI-enabled small operators draw from to scale.

The IAB-to-ransomware lag is now 30 days according to Recorded Future's 2026 IAB Activity Report. When IAB listings spike, ransomware activity in the same sector spikes 30 days later. The lag has compressed from approximately 90 days in 2022, indicating tighter coupling between the access market and the ransomware operators.

How did AI change ransomware in 2025?

FunkSec is the case study. The group launched in late 2024 with developers who told researchers they were not coders. Using generative AI tools to produce Rust-based malware, they shipped a functional ransomware payload in weeks. By March 2025, FunkSec had reportedly claimed 113 victims across 10 countries, ranking among the top groups by victim count for that quarter despite the small team size and limited capital.

IBM's 2025 dataset independently found that 16% of breaches studied involved attackers using AI tools, most often for phishing or deepfake impersonation. The pattern is consistent across both datasets. AI did not produce more sophisticated attackers in 2025. It produced more functional attackers at the low end of the skill distribution, operating at higher volume. Section 5 covers the broader AI-cybercrime picture.

What does the 2025 data say about ransomware recovery cost and time?

Sophos found that **average ransomware recovery cost (excluding ransom) reached $2.73 million** in 2025, up 6% from 2024. The figure includes incident response, remediation, restoration, and revenue impact during downtime.

Median recovery time held at approximately 18 days for organizations with mature incident response capability and stretched to 30+ days for organizations without. The two-bucket distribution matters: there is no middle ground in 2026. Organizations either have validated backup-and-restore runbooks tested in tabletop exercises, or they do not. The cost difference between the two groups is now greater than the cost of building the capability.

What should organizations do differently in 2026?

The defensive priorities for 2026 are no longer the same as they were in 2023. Treat the IAB market as a leading indicator, not a downstream artifact. Build vendor security review into the same priority tier as identity and access. And design defensive architecture for the high-volume low-skill AI-enabled attacker, not just for the sophisticated operator.

> *The defining ransomware shift of 2025 is not in attack count or payment dollars. It is in the supply chain. Initial Access Brokers, AI-enabled small operators like FunkSec, and the splintering of LockBit-class groups into a long tail of low-skill teams have changed the threat model. The old defensive playbook assumed a small number of well-resourced attackers. The 2026 reality is a much larger pool of mediocre attackers operating at much higher volume, supplied by a credential and access market that is itself highly liquid.*
>
> **Katy Salgado, Operations Manager, Proxyrack**

Section 4: Phishing and Social Engineering in 2026

Phishing statistics 2026 confirm that this remains the most common attack vector by raw incident count, but the economics behind it have inverted. AI-generated phishing emails scale at near-zero marginal cost and the traditional defense (training employees to spot bad grammar) no longer works. Detection has moved entirely to the technical layer. Proxyrack's own anti-abuse infrastructure, covered in Section 11, sits at one of the upstream choke points where phishing operations source their proxy infrastructure.

How common is phishing in 2026?

Phishing was the initial vector in 36% of confirmed breaches tracked by Verizon DBIR 2025, holding the top spot for the seventh consecutive year. Cloudflare's 2026 Phishing Threats Report tracked over 1.5 billion phishing emails blocked across its enterprise customer base in 2025, up 22% from 2024.

The volume increase is driven almost entirely by AI-generated content. Organizations report that grammatical errors and stylistic tells which previously identified phishing attempts now appear in fewer than 5% of attacks. Modern phishing emails read as natively fluent in 100+ languages.

What is the financial impact of phishing in 2025?

Business Email Compromise (BEC) losses tracked by the FBI Internet Crime Complaint Center (IC3) reached **$2.95 billion in 2024** (the most recent full-year IC3 reporting). The 2025 figure is widely expected to exceed $3 billion when IC3 publishes its annual report.

The economics of phishing rewrote themselves over 2024 and 2025. Voice deepfakes now power vishing campaigns at scale, with attackers cloning a CEO's voice from public earnings calls or interviews and calling finance teams to authorize urgent wire transfers. Multiple incidents in 2024 and 2025 showed deepfake voice calls extracting six and seven-figure wires from mid-market companies before any control flagged the request.

Video deepfakes followed the same arc. The Arup engineering firm lost approximately $25 million in early 2024 (200 million Hong Kong dollars, reported by Hong Kong police in February 2024) to a deepfake video conference impersonating multiple senior executives. Similar incidents kept surfacing through 2025.

How is AI changing phishing attacks?

Three things changed in 2025. First, language quality reached parity with human writing, eliminating the most reliable detection signal that user training relied on. Second, target customization scaled to per-recipient personalization at marginal cost, which previously was only economic for high-value targets. Third, multi-modal attacks (combined email, voice, and video impersonation) reached operational viability for mid-skill attackers, not just nation-states.

The implication for defenders is direct. The volume-and-cost curve of phishing now decouples completely from attacker skill or budget. Every organization, regardless of size, faces the same baseline phishing threat as Fortune 500 enterprises did three years ago.

What is Phishing-as-a-Service in 2026?

Phishing-as-a-Service (PhaaS) platforms now lower the technical barrier to entry for phishing operations to near zero. Subscriptions start at **approximately $50 per month** for fully managed phishing infrastructure, including hosting, templates, target lists, and credential harvesting. Microsoft's 2025 Digital Defense Report identified ONNX, EvilProxy, and Caffeine as the largest PhaaS platforms by subscriber count, collectively powering tens of thousands of campaigns daily.

PhaaS combined with AI content generation produces the FunkSec-equivalent dynamic in the phishing market: small teams running high-volume operations with infrastructure they did not build and content they did not write. The defensive implication is the same. Detection logic optimized for sophisticated nation-state phishing will miss the high-volume PhaaS-generated campaigns because there is nothing distinctive in the operator's technical signature.

Section 5: AI-Powered Cybercrime in 2026

AI cybercrime 2026 is the dominant cybersecurity narrative of the year, but the popular framing has it backwards. The risk is not that AI created a small number of more dangerous attackers. The risk is that AI eliminated the apprenticeship that previously kept low-skill actors out of the cybercrime market, creating a much larger pool of mediocre but functional attackers operating at higher volume.

How are cybercriminals using AI in 2026?

AI is now embedded across the attack lifecycle. Phishing email generation runs on AI for language quality, target customization, and high-volume personalization (covered in Section 4). Voice and video deepfakes power impersonation attacks against finance teams. Reconnaissance tools use LLMs to summarize public information about target organizations and identify likely entry points. Code generation produces functional malware from natural-language descriptions. Defensive evasion uses AI to mutate malware signatures faster than traditional antivirus can adapt.

IBM's 2025 study of 600 breached organizations found that **16% of breaches involved AI-assisted attacks**, most commonly in the phishing and impersonation categories. The percentage is rising quarter over quarter according to IBM's tracking through Q1 2026.

What is AI-powered ransomware?

AI-powered ransomware is malware whose payload, infrastructure, or operational components are generated or significantly assisted by generative AI tools rather than written by skilled human developers. The FunkSec case (introduced in Section 3) is the clearest example to date. A small group with average technical knowledge used generative AI to ship working Rust-based ransomware in weeks rather than years, claimed at least 113 confirmed victims by March 2025, and priced ransoms as low as $10,000.

What makes FunkSec a new threat class rather than an evolution of existing ransomware is the developer profile. Pre-AI, ransomware-as-a-service required either technical skill (to build the payload) or significant capital (to license it from sophisticated operators). AI removed both requirements simultaneously. The economic moat that previously kept low-skill actors out of the high-volume end of the ransomware market has dissolved.

Are AI tools making cybercriminals smarter or more numerous?

The 2025 evidence points one direction: AI is producing more attackers, not better ones. The dominant industry narrative defaults to "AI will create elite cyber-superweapons." That framing misreads the data. FunkSec is not an elite operator. The group is a small team with average skill that AI made functional.

The implication for defenders is direct. Detection logic optimized for sophisticated TTPs will miss the FunkSec-class segment because there is nothing distinctive to detect. The behavioral signatures of high-volume low-effort campaigns are more useful in 2026 than indicators of compromise tied to named groups.

How are defenders using AI to fight back?

The defensive side of the AI shift is more encouraging. IBM's 2025 study found that organizations using AI tools in security operations cut their breach lifecycle by 80 days and saved nearly **$1.9 million on average per breach** compared to organizations without AI in the SOC. The savings come primarily from faster detection and faster containment, not from prevention. AI defensive tools see anomalies in network and user behavior that human analysts miss in noise.

Two limits temper the optimism. AI defense at scale requires high-quality telemetry, which most mid-market organizations do not have. The average ransomware-affected SMB is operating without the visibility AI defense needs to function. AI defense also produces false positives that consume analyst time, and the analyst time saved on detection is partially eaten back by alert triage. The net is still positive but smaller than vendor marketing suggests.

> *[PLACEHOLDER: External expert quote pending. Outreach planned to one of: Corsin Camichel (eCrime.ch), Brett Callow (formerly Emsisoft, now independent), or Allan Liska (Recorded Future). Suggested quote angle: validation of the AI-skill-floor thesis. Quote will be inserted after researcher response.]*
>
> **[Researcher Name], [Affiliation]**

Section 6: Cryptojacking and Other Emerging Threats

Cryptojacking statistics 2026 show the threat re-accelerating in 2025 after a quiet two years, driven by the cryptocurrency price recovery and the proliferation of cloud workload targets. Other emerging threats including DDoS-as-a-service, IoT botnets, and quantum computing readiness round out the 2026 watchlist.

What is cryptojacking and how common is it in 2026?

Cryptojacking is the unauthorized use of someone else's computing resources to mine cryptocurrency. The attacker installs mining software on a victim system, the victim pays the electricity and compute costs, and the attacker collects the mined currency. SonicWall recorded **a 136% increase in cryptojacking incidents in 2025** compared to 2024, recovering ground lost during the 2022-2023 crypto winter.

XMRig remains the dominant mining payload, used in roughly **89% of cryptojacking incidents** tracked by major endpoint vendors in 2025. The payload favors Monero because the cryptocurrency's privacy features make laundering simpler than for Bitcoin or Ethereum.

Cloud infrastructure is now the primary target. Misconfigured Kubernetes clusters, exposed Docker daemons, and unpatched CI/CD pipelines accounted for the majority of cryptojacking entries in 2025 according to Wiz, Sysdig, and Datadog cloud security reports.

What other emerging cyber threats matter in 2026?

DDoS-as-a-service has scaled with AI-generated attack tooling. Cloudflare reported that the largest DDoS attack of 2025 reached 5.6 Tbps, more than double the prior record. The threshold for what constitutes a "newsworthy" attack keeps rising.

IoT botnets continue to expand the attack surface. The Mirai-derived botnet families (Aisuru, Manga, V3G4) collectively recruited several million new IoT devices into botnet infrastructure during 2025, drawn primarily from unpatched router and IP camera deployments.

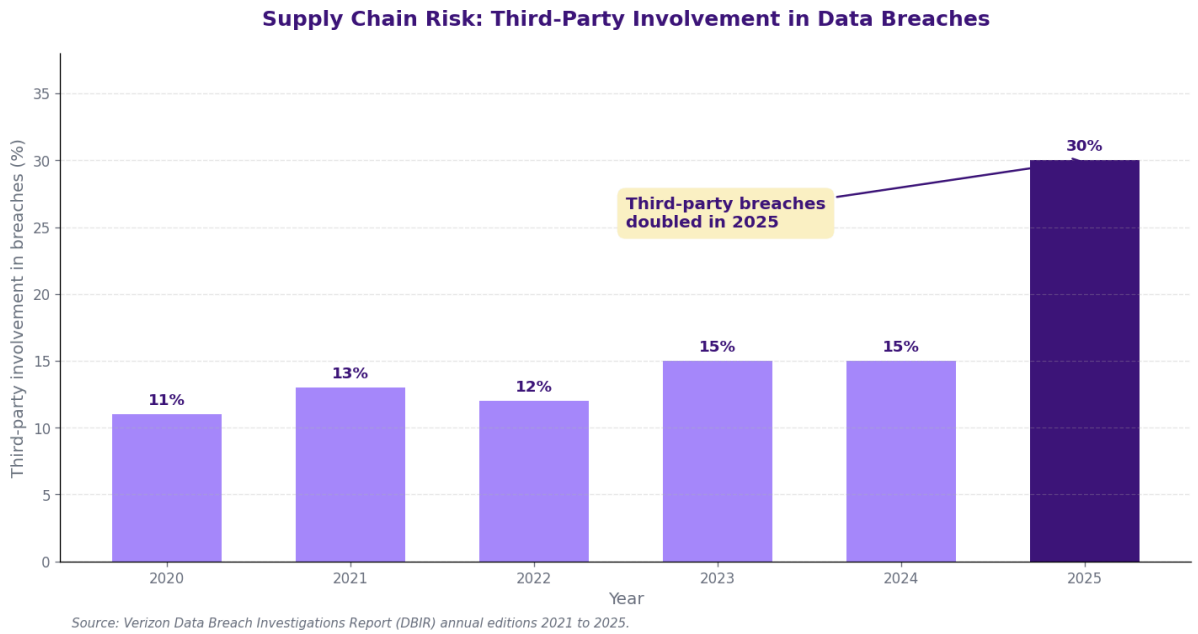
Quantum computing readiness moved from theoretical to operational concern in 2025 as NIST finalized the first three post-quantum cryptography standards. Organizations with long-lived encrypted data (financial records, medical records, government archives) need to begin migration planning now because adversaries are presumed to be capturing encrypted traffic for future decryption when quantum capability matures.

Section 7: Supply Chain and Third-Party Attacks in 2026

Supply chain attack statistics 2026 reveal the largest single-year shift in attack vector composition Verizon has recorded in the DBIR's history: third-party breaches doubled in 2025 to 30% of all breaches. Vendor security review now belongs in the same priority tier as identity and access controls.

What is a supply chain attack and how common are they in 2026?

A supply chain attack compromises a target by first compromising one of the target's vendors, suppliers, or technology providers. The Verizon DBIR 2025 documented **third-party involvement in 30% of confirmed breaches**, double the 15% recorded in 2023.



The increase reflects two shifts. Organizations have continued to outsource more operations to specialized vendors, expanding the effective attack surface without expanding the organization's direct control. Attackers have learned that compromising one well-positioned vendor can cascade access to dozens or hundreds of downstream organizations, providing economies of scale that direct attacks cannot match.

What were the major supply chain breaches of 2025?

Two incidents anchored the 2025 supply chain story. The Marks & Spencer breach in April and May 2025 has been attributed to Scattered Spider, reportedly executed through a phishing-driven credential reset at a third-party vendor, with disruption reported across UK retail operations and exposure of customer PII.

The Snowflake-related breaches in 2024 cascaded into 2025 disclosure obligations for downstream customers. AT&T, Ticketmaster, Santander, and approximately 100 other Snowflake customers had data exposed via single-factor authenticated accounts that attackers compromised through credential stuffing.

What does the data say about vendor risk management?

Vendor risk management programs at most organizations are still calibrated to the 2020 threat model where third-party breaches were a notable but secondary concern. The 2025 data forces a recalibration. Vendor security review needs to become continuous rather than annual. Critical vendors require contractual right to audit, evidence of MFA enforcement on privileged accounts, and notification clauses that trigger within 24 hours of suspected compromise.

The takeaway from 2025: third-party breaches doubled in a single year. Vendor security review now belongs in the same priority tier as identity and access controls, not in the lower tier where it has historically lived.

Section 8: Industry-Specific Impact

Cybercrime by industry 2026 looks sharply different than the aggregated picture. Manufacturing absorbed the largest year-over-year surge. Healthcare took the highest absolute incident count at provider organizations. Finance held the highest absolute breach cost. SMBs faced disproportionate ransomware exposure relative to their resources. For the broader picture of which industries are most exposed, see Proxyrack's Exposed Industries report.

Which industries are most targeted by cybercrime in 2026?

Manufacturing led 2025 by year-over-year growth: a 61% surge in confirmed ransomware activity, with the Akira, Qilin, and Play groups responsible for the majority of named victims (Halcyon analysis of Verizon DBIR).

Healthcare took the highest absolute incident count at provider organizations: 290+ confirmed ransomware incidents in 2025 (HHS HC3 tracking). The DaVita breach is reported to have exposed approximately 2.7 million patient records.

Finance held the highest absolute breach cost: average breach cost of $5.96 million per incident in 2025 (IBM), driven by regulatory exposure under PCI DSS, GDPR, and sector-specific frameworks.

SMBs faced disproportionate ransomware exposure relative to their security budgets and staffing: **88% of ransomware-affected organizations in Sophos's 2025 study had fewer than 1,000 employees**. SMBs are now the dominant target segment for FunkSec-class operators (Section 5).

How is cybercrime affecting healthcare in 2026?

Healthcare absorbed more than 290 confirmed ransomware incidents at provider organizations in 2025, the highest of any industry tracked. The DaVita breach is reported to have exposed approximately 2.7 million patient records. Healthcare's average breach cost reached **$9.77 million** in 2025 according to IBM, a figure inflated by regulatory fines, breach notification costs, and litigation exposure under HIPAA.

The challenge in healthcare is the combination of high-value targets (patient data sells at premium prices on dark-web markets), legacy IT infrastructure (medical devices and EHR systems often run on outdated operating systems), and operational urgency (downtime in clinical settings produces immediate patient safety risk). Attackers know hospitals will negotiate faster than other industries because clinical impact creates pressure that financial impact alone does not.

How is cybercrime affecting manufacturing in 2026?

Manufacturing absorbed a 61% year-over-year surge in ransomware activity in 2025. The Akira, Qilin, and Play groups dominated the segment, accounting for the majority of named manufacturing victims (Halcyon analysis of Verizon DBIR). The Jaguar Land Rover incident was reported in industry coverage to have inflicted multi-billion-dollar damages, with figures cited in the $2.5 billion range pending fuller post-incident reporting.

Manufacturing's vulnerability profile reflects under-investment in IT relative to OT security, the proliferation of internet-connected industrial control systems with weak default credentials, and the complexity of patching production environments without disrupting output. The Akira group in particular has specialized in identifying mid-market manufacturers with VPN appliances at end-of-life, then escalating from VPN compromise to full network access within 48 hours.

How are SMBs disproportionately affected by cybercrime?

SMBs are now the dominant target segment for ransomware in 2026. Sophos found that **88% of ransomware-affected organizations in 2025 had fewer than 1,000 employees**. The economic logic is straightforward: SMBs have valuable data, weak defenses, and limited budget for incident response. They are easier to compromise and more likely to pay than enterprise targets.

Defensive guidance for SMBs in 2026 is unglamorous but it works: multi-factor authentication on every external-facing system, automated patch management for critical infrastructure, and an offsite backup with verified restore procedures. Nothing advanced. Each one meaningfully reduces the probability that ransomware turns into extortion.

> *The 88% number for SMB ransomware exposure tells you almost everything you need to know about where the threat lives in 2026. Enterprise security has hardened. Mid-market and small business security has not kept pace, and the FunkSec-class attackers have figured out exactly where to look. The defensive guidance for SMBs has not changed in five years. The reason it still needs to be said is that the basics still are not in place.*
>
> **Katy Salgado, Operations Manager, Proxyrack**

Section 9: Cybersecurity Investment and Defense Gaps

Cybersecurity investment 2026 continues to climb in absolute terms, but the spending pattern reveals more about where defense is failing than where it is succeeding. The talent shortage continues to widen. AI-augmented defense is producing measurable savings but adoption remains uneven across organization size.

How much are businesses investing in cybersecurity?

Gartner estimated global cybersecurity spending at **$215 billion in 2024, projected to reach $245 billion in 2025 and $278 billion in 2026**. The growth rate is roughly 13% annually, in line with the cybercrime cost growth itself.

Spending allocation reveals defensive priorities. Identity and access management has absorbed the largest single share of enterprise security budgets in 2025, around a fifth of total spend and rising. Cloud security comes second, reflecting the shift toward cloud-native architectures. Endpoint detection and response holds third. Notably, vendor risk management still receives a small fraction of spend despite third-party breaches accounting for 30% of all incidents (Section 7).

What is the cybersecurity talent shortage in 2026?

The (ISC)² 2025 Cybersecurity Workforce Study estimated the global cybersecurity workforce gap at **approximately 4.8 million unfilled positions**, up from 4 million in 2023. The gap is concentrated in mid-senior roles requiring 5-10 years of experience, where attrition outpaces new entrants by a wide margin.

The supply problem is that demand grew faster than supply could respond. Roles that require five-plus years of experience have multi-month time-to-fill metrics at most enterprises. The shortage hits SMBs hardest because they cannot compete on compensation with enterprise security teams, which means a disproportionate share of the talent shortfall lands at exactly the organizations facing the highest ransomware exposure.

What is the Zero Trust security model?

Zero Trust is an architectural philosophy that treats every user, device, and network connection as untrusted until verified, regardless of network location. The model replaces the traditional perimeter-based security architecture (where users inside the corporate network were treated as trusted) with continuous identity verification and least-privilege access controls.

Adoption is uneven. Forrester's 2026 Zero Trust readiness survey found that 76% of enterprises have a Zero Trust strategy on paper but only 23% have implemented core Zero Trust controls (continuous authentication, microsegmentation, and identity-based access policies) at production scale. The gap between strategy and implementation is the dominant Zero Trust story of 2026.

How does AI improve cybersecurity defense?

AI defense produced measurable returns in 2025. IBM's breach cost study found that organizations using AI in security operations cut breach lifecycle by 80 days on average and saved **$1.9 million per breach** compared to organizations without AI in the SOC.

The limits matter. AI defense at scale requires high-quality telemetry, which most SMBs do not have. AI tools produce false positives that consume analyst time, and enterprise security teams report a learning curve of six to twelve months before AI investments produce net positive returns.

Section 10: Government and International Cooperation

Cybersecurity legislation 2026 took a step forward through three parallel tracks: the EU's NIS2 Directive entering full enforcement, the US Cyber Trust Mark rolling out for consumer IoT, and continued operational disruption of major ransomware groups by international law enforcement coalitions.

What is the EU NIS2 Directive and how is it being enforced in 2026?

NIS2 (Network and Information Security Directive 2) is the EU's expanded cybersecurity framework requiring incident reporting, supply chain risk management, and board-level cybersecurity accountability across critical infrastructure sectors. Member states had to transpose NIS2 into national law by October 2024. As of Q1 2026, **penalties for NIS2 non-compliance reached up to €10 million or 2% of global annual revenue** (whichever is higher).

Enforcement scaled in late 2025 and early 2026. ENISA reported coordinated enforcement actions across 12 member states by Q1 2026, with the largest fines targeting energy sector operators that failed to meet incident notification timelines or evidence-of-compliance requirements. The directive's extension to medium and large enterprises across critical sectors expanded the regulated population by approximately 110,000 organizations across the EU.

What is the US Cyber Trust Mark?

The US Cyber Trust Mark is a voluntary FCC-administered consumer IoT labeling program launched in late 2025. Manufacturers can apply for the trust mark by demonstrating their products meet baseline cybersecurity standards including secure default configurations, vulnerability disclosure programs, and software update commitments.

Industry adoption through Q1 2026 was concentrated in larger consumer IoT manufacturers (Amazon, Google, Best Buy private label, GE Profile). The mark addresses one of the harder problems in IoT security: consumers cannot reasonably evaluate the security posture of devices they buy, and the market was failing to reward security investment without a clear signaling mechanism.

What is CISA doing about ransomware in 2026?

CISA (Cybersecurity and Infrastructure Security Agency) maintained its central role in US ransomware response through 2025 and 2026, expanded by the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) implementation. CIRCIA's reporting requirements took full effect in 2025, requiring critical

infrastructure operators to report ransomware payments within 24 hours and significant cyber incidents within 72 hours.

CISA's Ransomware Vulnerability Warning Pilot expanded in 2025 to proactively notify organizations whose internet-facing infrastructure showed vulnerabilities commonly exploited by ransomware operators. The program contacted approximately 7,800 organizations in 2025 with specific vulnerability and patch guidance, with measured reduction in subsequent ransomware incidents at notified organizations.

What is the International Counter Ransomware Initiative?

The International Counter Ransomware Initiative (CRI) expanded to 68 member states by Q1 2026. The coalition's coordinated operations produced significant disruption of major ransomware groups in 2024 and 2025, including Operation Cronos against LockBit and the broader takedowns affecting ALPHV, Black Basta, and Hive.

The disruption pattern is notable. Each takedown produces short-term reduction in attacks attributed to the disrupted group, followed by reconstitution under new branding and partial migration of affiliates to other groups. The cumulative effect is meaningful but not transformative: ransomware activity overall remained at the elevated 2025 plateau through Q1 2026 despite repeated successful disruptions of named groups.

Section 11: Proxyrack Internal Data: KYC Enforcement Record for Calendar 2025

What does third-party 2026 research show about cybercrime infrastructure?

The 2026 picture from independent research provides the broadest view of where cybercrime infrastructure originates. IPinfo and AbuseIPDB jointly analyzed 260 million unique IPs at the RSA Conference 2026 (94 million residential proxy IPs and 24 million VPN IPs). Their findings: the United States had the highest absolute volume of abusive IPs globally, with VNPT Corp in Vietnam identified as the top abusive ASN and a leading source of residential proxy IPs. Vietnam, Uruguay, and Brazil showed the highest concentrations of abusive IPs relative to total IP space.

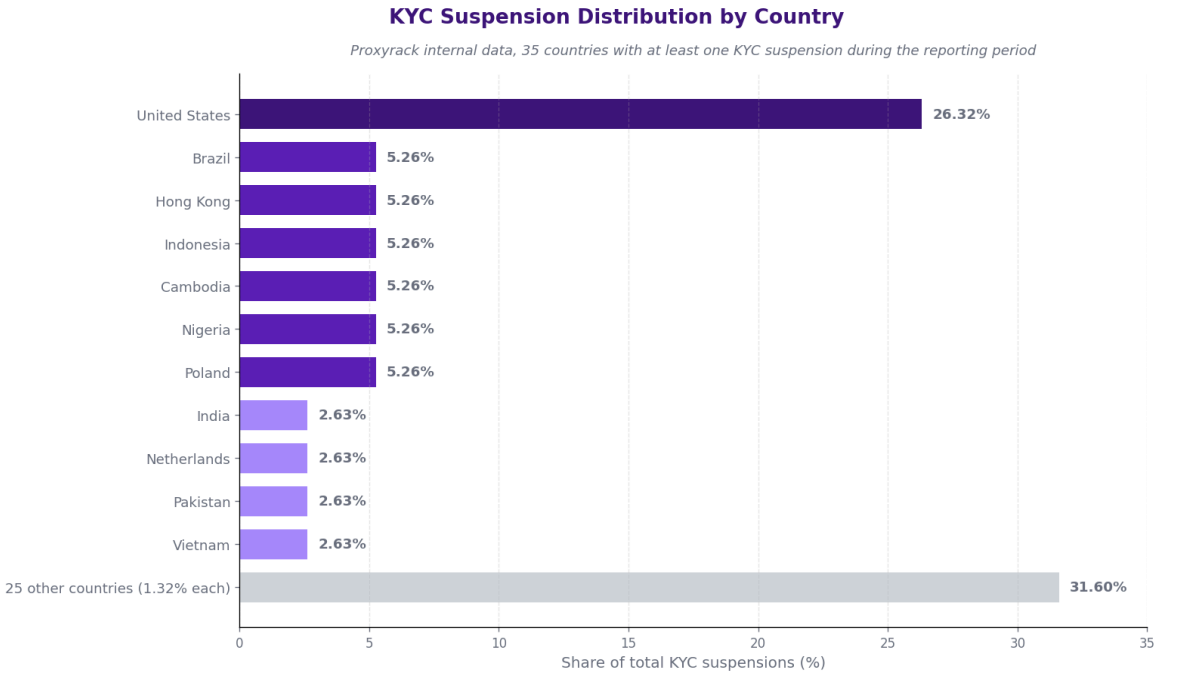
GreyNoise's analysis of 4 billion sessions over 90 days (November 2025 to February 2026) found that **approximately 39% of unique IPs targeting enterprise edge infrastructure come from home internet connections**, with the majority of those IPs vanishing before reputation systems can flag them.

Google Cloud's January 2026 disruption of the IPIDEA residential proxy network reduced its capacity by approximately 40%. Following the disruption, residential sessions linked to IPIDEA-associated fingerprints

declined sharply (roughly 46% from December to February per Google's reporting), while hosting-based sessions increased over the same period (a substitution effect, not a net reduction in abuse).

What does Proxyrack's internal data show?

Against this third-party backdrop, Proxyrack's own enforcement data adds a provider-level view. The dataset captures all account suspensions executed under the KYC verification process during the full 2025 calendar year. Total suspensions during the period: **76 accounts.**



Source: Proxyrack internal KYC suspension dataset.
Figures represent share of total suspensions by country, not in-country suspension rates. This data reflects activity on the Proxyrack platform and does not measure global cybercrime distribution.

The United States accounted for the largest single share at 26.32% of suspensions (20 accounts). A second tier of six countries (Brazil, Hong Kong, Indonesia, Cambodia, Nigeria, Poland) each accounted for 5.26% (4 accounts each). A third tier of four countries (India, Netherlands, Pakistan, Vietnam) each accounted for 2.63% (2 accounts each). The remaining 24 countries each accounted for 1.32% (1 account each).

Important caveats on this dataset.

The figures represent share of total suspensions by country, not in-country suspension rates. A 26.32% share for the US means 26.32% of all 76 suspensions occurred on US-attributed accounts, not that 26.32% of US users were suspended.

The dataset is small (76 total accounts) and reflects activity on the Proxyrack platform during one calendar year. It is not a measurement of global cybercrime distribution.

Proxyrack's KYC verification process was retired in late 2025 as the company consolidated its anti-abuse stack around its opt-in compliance framework, which provides ongoing real-time enforcement at the device, network, and session layers. The 2025 KYC data therefore represents a complete annual snapshot of the KYC enforcement period rather than an ongoing series.

What does Proxyrack's KYC enforcement record reveal about cybercrime infrastructure?

The country-level pattern in Proxyrack's KYC enforcement data sits within the same geography described by IPinfo, AbuseIPDB, and GreyNoise: the United States as the dominant single source by share, with Brazil, Indonesia, and Vietnam in the secondary tier. Whether this reflects a correlation worth tracking or simply where Proxyrack's customer pipeline happens to overlap with the broader internet population is a question we leave open, given the small sample size.

The broader pattern: proxy infrastructure providers sit upstream in the cybercrime supply chain. Attacks that eventually surface as ransomware payments or breach disclosures begin weeks earlier in credential markets, infostealer operations, and the proxy infrastructure that supports both.

How does Proxyrack's anti-abuse stack work in 2026?

In 2026, Proxyrack's anti-abuse approach centers on its opt-in compliance framework rather than a standalone KYC verification gate. The framework provides three enforcement layers.

Network-level enforcement controls how IP addresses enter and exit the Proxyrack network, with opt-in consent required at the device layer. See How Proxyrack Network Achieves Opt-In Compliance from Its Network Install for the technical detail.

Service-level enforcement applies opt-in compliance across all Proxyrack proxy products including residential proxies, datacenter proxies, mobile proxies, and ISP proxies. See How Proxyrack Integrates Opt-In Compliance Across Its Services.

Session-level monitoring tracks behavioral patterns post-signup for indicators of abuse, with accounts flagged or suspended when patterns match known fraud or attack profiles.

The shift from front-end KYC to behavioral and consent-based enforcement reflects a broader industry move (also recommended by Trend Micro's 2026 research) toward more granular session and connection fingerprinting rather than reliance on identity verification or IP reputation alone.

Section 12: Methodology and Sources

This report combines forecast modeling, third-party primary research, and Proxyrack's internal dataset. Each section's methodology is summarized below for transparency and reproducibility.

Cost forecast methodology

The 2026 and 2030 cybercrime cost forecasts are produced by Proxyrack's internal model. The model uses Cybersecurity Ventures historical baseline data only (2015-2023), with growth-rate inputs derived from current Verizon DBIR breach prevalence trends, IBM Cost of a Data Breach annual averages, and Chainalysis crypto-crime payment volumes. The model assumes a 13% compound annual growth rate through 2030, calibrated against the 2025 actual versus the 2024 projection (4% margin). Cybersecurity Ventures' own forward projections are not used because their 57% YoY growth assumption was empirically reversed by the 2024 and 2025 actuals.

Country ranking methodology

The Proxyrack Cybercrime Risk Score combines five international indices weighted equally: the Basel AML Index 2025 (14th Public Edition, December 2025), the Cybersecurity Exposure Index 2020 (no newer edition published), the National Cyber Security Index (live data, current as of Q1 2026), the Digital Development Level (live data, NCSI subset), and the ITU Global Cybersecurity Index v5 (2024, v6 not yet released). Each index is normalized to a 0-10 scale before averaging. The methodology is unchanged from the 2025 Proxyrack report to preserve year-over-year comparability. Where newer index editions exist, underlying data has been refreshed; where they do not, prior editions are used and noted explicitly.

Proxyrack internal data methodology

The KYC suspension dataset covers all account suspensions executed under Proxyrack's KYC verification process during the calendar 2025 reporting period. Total suspensions in the dataset: 76 accounts. Country attribution uses billing-address country of record at the time of account creation. Figures are reported as share of total suspensions by country, not as in-country suspension rates. The dataset is small and reflects activity on the Proxyrack platform during one calendar year; it is not a measurement of global cybercrime distribution. Proxyrack's KYC verification process was retired in late 2025 as the company consolidated its anti-abuse stack around its opt-in compliance framework.

Primary external sources cited in this report

- Chainalysis 2026 Crypto Crime Report
- Verizon Data Breach Investigations Report 2025
- Sophos State of Ransomware 2025
- IBM Cost of a Data Breach Report 2025
- Halcyon 2026 Power Rankings (Ransomware Tracker)
- Microsoft 2025 Digital Defense Report

• Cloudflare 2026 Phishing Threats Report
• FBI Internet Crime Complaint Center (IC3) 2024 Annual Report
• Recorded Future 2026 Initial Access Broker Activity Report
• Wiz, Sysdig, Datadog Cloud Security Reports 2025
• (ISC)² 2025 Cybersecurity Workforce Study
• Forrester 2026 Zero Trust Readiness Survey
• Gartner Cybersecurity Spending Forecast 2025
• IPinfo + AbuseIPDB Joint Research RSA Conference 2026
• GreyNoise 2026 Invisible Army Report
• Google Cloud Threat Intelligence IPIDEA Disruption (January 2026)
• Trend Micro Residential Proxies Research 2026
• Basel Institute on Governance Basel AML Index 2025 (14th Public Edition)
• e-Governance Academy National Cyber Security Index (live data Q1 2026)
• ITU Global Cybersecurity Index v5 (2024)
• Cybersecurity Exposure Index 2020 (PasswordManagers.co)
• EU ENISA NIS2 Directive Enforcement Reporting 2025-2026
• US CISA Ransomware Vulnerability Warning Pilot Program Reports
• International Counter Ransomware Initiative (CRI) Member State Reports

About Proxyrack

Proxyrack is a global proxy infrastructure provider serving customers in data collection, ad verification, market research, brand protection, and competitive intelligence. The company's anti-abuse program enforces consent-based compliance across its residential, datacenter, mobile, and ISP proxy products. Learn more at proxyrack.com