March 2026 Cyber Threat Landscape Shows No Relief as Ransomware Rebounds and GenAI Risks Intensify

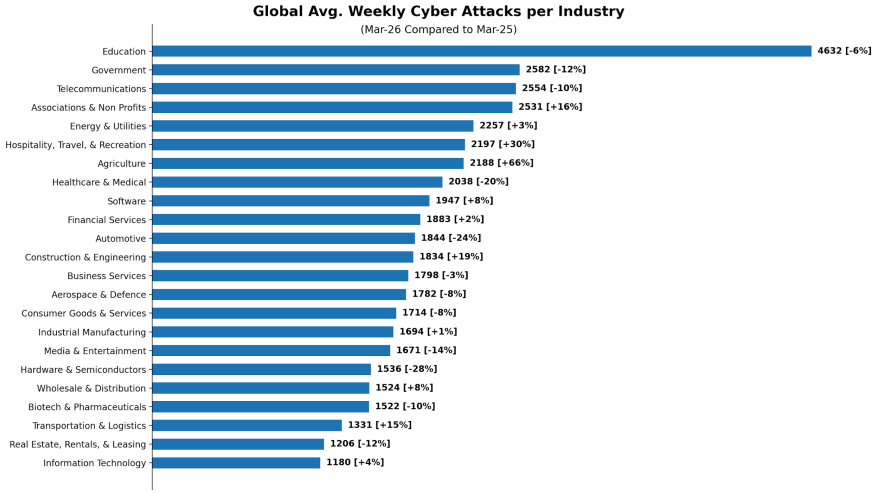
Global Attack Volumes Begin to Moderate

In March 2026, global cyber-attack activity showed early signs of moderation while remaining at historically elevated levels. The average number of weekly cyber-attacks per organization reached **1,995**, representing a **4% decrease month over month** and a **5% decline compared to March 2025**.

Despite this easing, the overall threat environment remains intense. Nearly 2,000 weekly attacks per organization continue to reflect sustained adversary pressure, driven by automation, broad attack surface expansion, and persistent exposure risks tied to cloud adoption and GenAI usage. Check Point Research data indicates that while short-term fluctuations are emerging, cyber threats have not returned to pre-surge baselines and remain a constant operational reality for organizations worldwide.

Critical Sectors Continue to Face Disproportionate Risk

The **Education sector** remained the most targeted industry in March, experiencing an average of **4,632 cyber-attacks per organization per week**, a **6% decrease year over year**. Large user populations, highly distributed access environments, and limited security resources continue to make educational institutions attractive targets, even as overall volumes decline slightly.



The **Government sector** ranked second, averaging **2,582 weekly attacks**, reflecting a **12% year-over-year decrease**. While the drop suggests some short-term relief, government organizations remain consistent targets due to mission-critical services and high-value data. **Telecommunications** followed closely, with organizations facing **2,554 weekly attacks**, down **10% year over year**, yet continuing to attract threat actors seeking large-scale disruption or supply-chain access.

An important outlier emerged in **Hospitality, Travel & Recreation**, which recorded a **30% year-over-year increase** in attacks. As these organizations prepare for spring and summer travel surges, attackers appear to be accelerating activity ahead of peak seasonal demand, exploiting increased transactional volume, customer data exposure, and operational dependencies.

Regional Threat Disparities Remain Pronounced

Regional analysis underscores continued imbalance in global cyber pressure, with attack reductions unevenly distributed. **Latin America** recorded the highest attack volume globally, averaging **3,054 weekly attacks per organization**, alongside a **9% year-over-year increase**. Notably, Latin America was the **only region to experience growth compared to February**, reinforcing its position as an expanding target amid rapid digitalization.

APAC followed with **3,026 weekly attacks**, reflecting a **4% year-over-year decline**, while **Africa** averaged **2,722 attacks**, experiencing the sharpest reduction at **-22% year over year**, though remaining among the most targeted regions overall.

Region	Weekly Attacks per Organization	YoY Change
Latin America	3,054	+9%
APAC	3,026	-4%
Africa	2,722	-22%
Europe	1,647	-7%
North America	1,384	-8%

Europe and North America both recorded moderate year-over-year declines, yet continue to face substantial baseline attack volumes, reinforcing that even mature markets are not immune to sustained cyber pressure.

GenAI Usage Continues to Elevate Data Exposure Risk

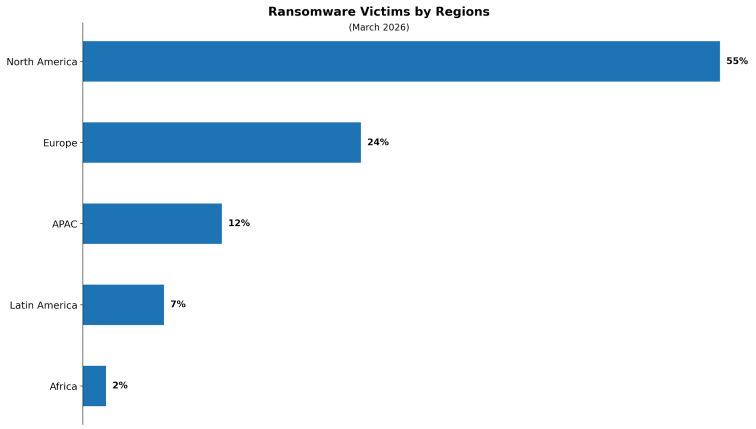
Enterprise GenAI adoption remained widespread throughout March 2026, intensifying data leakage risk despite reductions in overall attack volumes. Key GenAI exposure indicators in March include:

- **1 in every 28 GenAI prompts** posed a high risk of sensitive data leakage
- **91% of organizations** using GenAI tools regularly were impacted by this risk
- An additional **17% of prompts** contained potentially sensitive information
- Organizations used an average of **9 different GenAI tools**, signaling fragmented adoption
- The average enterprise user generated **78 GenAI prompts per month**

While GenAI usage expanded, the proportion of high-risk interactions increased compared to February, highlighting persistent governance and visibility gaps. Without centralized controls, organizations remain vulnerable to credential leakage, intellectual property exposure, internal data mis-sharing, and unintended third-party risk amplification.

Ransomware Activity Rebounds Month Over Month

In March 2026, **672 ransomware attacks** were reported globally. This represents an **8% decrease year over year**, yet a **7% increase compared to February**, indicating renewed attacker momentum following short-term declines earlier in the quarter.
North America remained the most affected region, accounting for **55% of reported incidents**, followed by **Europe at 24%** and **APAC at 12%**. Europe's share rose significantly from **17% in February**, suggesting a rebalancing of attacker focus toward high-value EU targets.



*This data is derived from ransomware "shame sites" operated by double-extortion groups. While inherently biased, these sources provide valuable insight into ransomware operations and trends.

Ransomware Targets Concentrate on High-Impact Industries

Business Services remained the most targeted sector, accounting for **35%** of ransomware victims, followed by **Consumer Goods & Services (14%)** and **Industrial Manufacturing (13%)**. Together, the top three industries represented **61% of all reported ransomware incidents**, underscoring attackers' focus on sectors where downtime and data exposure translate directly into financial leverage.

The mid-tier cluster, including **Financial Services, Government, and Healthcare & Medical**—accounted for a combined **14% of victims**, with each sector increasing its share compared to February, signaling broader distribution beyond traditional ransomware strongholds.

Industry	Ransomware Victims
Business Services	34.5%
Consumer Goods & Services	14.0%
Industrial Manufacturing	13.0%
Financial Services	5.2%
Government	4.6%
Healthcare & Medical	4.6%
Automotive	3.7%
Transportation & Logistics	3.6%
Information Technology	3.4%
Education	2.5%
Media & Entertainment	2.1%
Energy & Utilities	1.8%
Telecommunications	1.3%
Real Estate, Rentals, & Leasing	1.3%
Hospitality, Travel, & Recreation	1.0%

Ransomware Attacks per Country

Country-level analysis shows ransomware activity remains heavily concentrated in North America but continues to span multiple continents. The **United States** accounted for **51.8%** of reported attacks, followed by **Germany (4.8%)**, **France (4.5%)**, and the **United Kingdom (3.7%)**.

Country	Ransomware Victims
United States	51.8%
Germany	4.8%
France	4.5%
United Kingdom	3.7%
Canada	3.6%
Italy	3.4%
Spain	1.9%
Brazil	1.8%
Thailand	1.5%
Colombia	1.2%

The top impacted countries span North America, Europe, Asia, and Latin America, reinforcing ransomware's global reach despite regional concentration.

Leading Ransomware Groups Expand Their Influence

Ransomware activity in March remained fragmented yet dominated by a small number of high-output groups. **Qilin** led activity, responsible for **20% of published attacks**, followed by **Akira (12%)** and **DragonForce (8%)**. While the top three accounted for **40% of incidents**, a total of **47 different ransomware groups** publicly impacted organizations worldwide last month.

- **Qilin:** One of the most established ransomware-as-a-service (RaaS) operations, active since 2022. Formerly known as Agenda, Qilin operates a mature affiliate ecosystem with Rust-based encryptors, negotiation infrastructure, and dedicated support services. Since early 2025, the group has significantly expanded affiliate recruitment and victim disclosures.
- **Akira:** First observed in 2023, Akira targets Windows, Linux, and ESXi systems. The group has increasingly focused on business services and industrial manufacturing, deploying a Rust-based ESXi-focused encryptor with selective VM targeting and sandbox evasion mechanisms.
- **DragonForce:** A RaaS group operating a white-label "cartel" model allowing affiliates to run independent brands atop shared infrastructure. DragonForce's activity accelerated in March, following absorption of displaced RansomHub affiliates and high-profile social engineering campaigns targeting major UK retailers.

What March's Trends Reveal About the Threat Landscape

March 2026 suggests that cyber threats are entering a phase of compressed volatility rather than sustained escalation. Overall attack volumes declined modestly, yet ransomware activity rebounded month over month, GenAI-driven exposure intensified, and targeted sector pressure shifted rather than disappeared.

At Check Point Software, our research shows that temporary declines do not signal reduced risk. Attackers continue refining precision, timing, and targeting, exploiting seasonal cycles, emerging technologies, and operational blind spots. In this environment, reactive security models remain insufficient. A prevention-first,

AI-driven, multi-layered security strategy—spanning cloud, network, endpoint, and user environments—is essential to controlling exposure and building long-term cyber resilience. Staying ahead now requires anticipating attacker behavior, not merely responding to incidents after impact.