July 2026 Cyber Threats Surge: Ransomware Attacks Double Year over Year as GenAI Data Exposure Widens

Key takeaways

- **Weekly cyber attacks reached 2,336 per organization in July 2026, up 3% from June and 16% year over year.**
- **Education remained the most attacked industry, averaging 4,848 weekly attacks per organization.**
- **Latin America recorded the highest regional attack volume, while Europe saw one of the sharpest increases at 18% year over year.**
- **GenAI adoption continued to expand, with organizations using an average of 8 tools and 1 in 36 prompts carrying a high risk of sensitive data exposure.**
- **Email remained a key entry point, with 1 in every 128 emails classified as phishing and another 20% falling into unwanted or risky categories.**
- **Ransomware activity surged to 964 reported victims, up 49% from June and 87% year over year.**

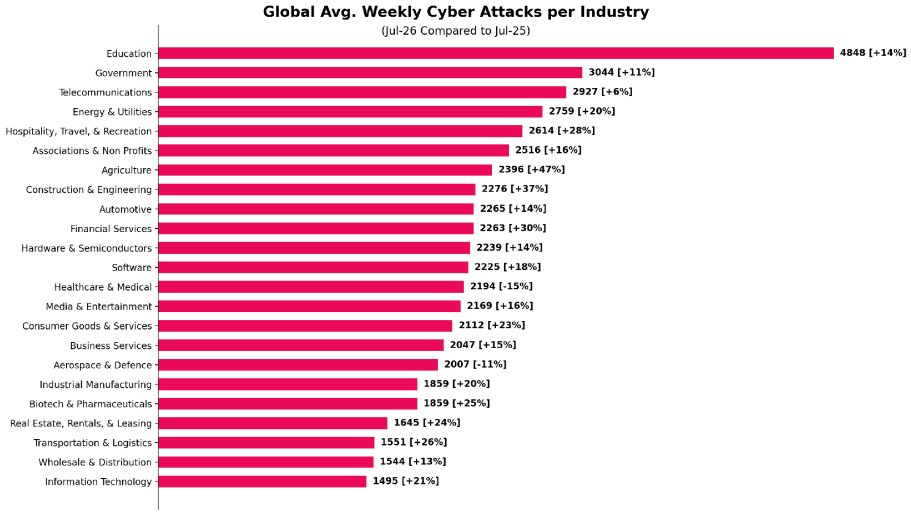
July's cyber threat landscape was shaped by pressure across multiple fronts. Global cyber attacks continued to rise, ransomware activity broke from the more stable pattern seen earlier in the year, and GenAI exposure became a clearer operational risk as employees used more tools and generated more prompts across the enterprise.

Cyber Attacks Keep Climbing

The global attack curve continued upward in July. Organizations faced an average of 2,336 weekly cyber attacks, up 3% from June and 16% from July 2025. While the monthly rise was more moderate than June's rebound, the broader trend remains clear: average weekly attacks per organization have increased by 13.7% since May, signaling sustained pressure rather than a temporary spike.

Education Remains the Top Target

Education remained the most targeted sector, averaging 4,848 weekly attacks per organization, up 14% year over year. Government ranked second with 3,044 weekly attacks, up 11%, followed by Telecommunications at 2,927, up 6%. Energy and Utilities moved into fourth place with 2,759 weekly attacks, up 20%, while Hospitality, Travel and Recreation entered the top five with 2,614 attacks, up 28%, possibly reflecting higher exposure during the summer travel period.



Latin America Leads in Volume as Europe Sees a Sharp Rise

Regionally, Latin America continued to face the highest attack volume, with 3,561 weekly attacks per organization on average, up 19% from July 2025. APAC followed with 3,316 weekly attacks, while Africa ranked third despite a 5% year-over-year decline. Europe stood out for its growth rate, with attacks up 18% year over year, while North America rose 9%.

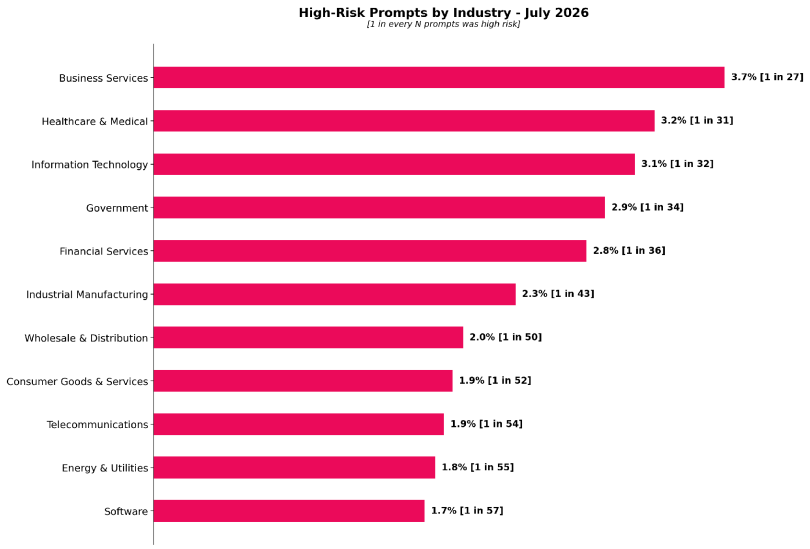
Region	Weekly Attacks per Organization	YoY Change
Latin America	3,561	+19%
APAC	3,316	+12%
Africa	3,237	-5%
Europe	2,051	+18%
North America	1,613	+9%

GenAI Risk Moves from Theory to Daily Business Reality

GenAI risk is becoming a daily business issue. The main concern is not only how AI tools are used, but what employees enter into them, from customer records and internal documents to infrastructure, legal, financial, or HR information. July's data shows how quickly that exposure can scale:

- **1 in every 36 prompts** from enterprise networks carried a high risk of sensitive data leakage.
- **88% of regular GenAI-using organizations** were affected by high-risk prompt activity.
- **22% of prompts** contained potentially sensitive information.
- **Organizations used an average of 8 GenAI tools**, while the average user generated 95 prompts during the month.

This makes GenAI both a governance and security issue, especially as adoption moves faster than policies, training, and controls. Exposure was highest in Latin America and North America, while Europe and APAC were slightly below the global average. By industry, Business Services and Healthcare and Medical recorded the highest risk, followed by Information Technology and Government.

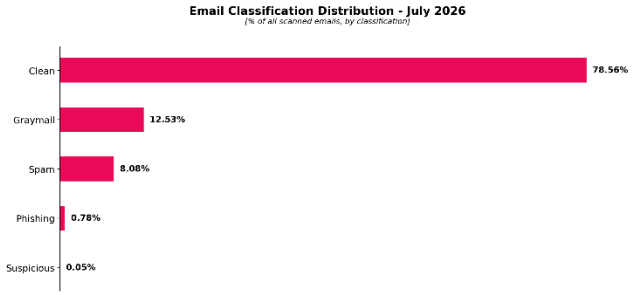


The type of information being exposed is also important. Personal data remained the most common sensitive category, appearing in 70% of organizations. Financial Data and Network and IT Infrastructure followed at 68% each, while Legal and Regulatory content appeared in 63% and Employee and HR data in 62%. The issue is not limited to one team, use case, or document type. It cuts across the core information organizations rely on every day.

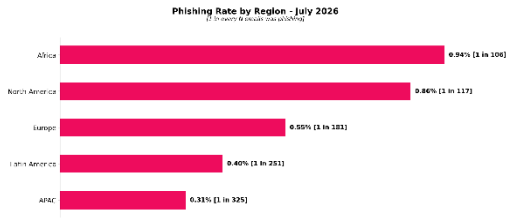
Data Category	% of Organizations
PII	70%
Financial Data	68%
Network & IT Infrastructure	68%
Legal & Regulatory	63%
Employee & HR	62%

Email Remains a Key Entry Point for Cyber Risk

Despite growing focus on newer attack surfaces, email remained a high-volume risk channel in July. One in every 128 emails, or 0.78%, was classified as phishing, while another 20% fell into unwanted or risky categories such as graymail, spam, and suspicious messages, adding to the daily burden security teams need to filter and investigate.



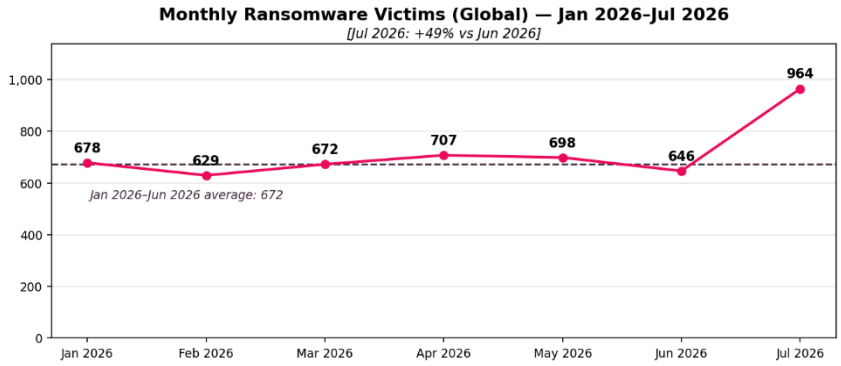
Africa recorded the highest phishing rate, with one in every 106 emails classified as phishing, followed by North America at one in every 117. Beyond the regional differences, the trend reinforces email's role as a common starting point for broader attack chains, from credential theft and malware delivery to business email compromise. In July, that escalation was most visible in ransomware activity.



Ransomware Breaks the Pattern

** This ransomware data draws from ransomware "shame sites" operated by double-extortion groups, which publicly disclose victim information. While these sources have inherent biases, they provide valuable insight into the ransomware landscape.*

The clearest shift in July came from ransomware. Reported attacks reached 964, up 87% from July 2025 and 49% from June. This marked a decisive break from the first half of 2026, when monthly ransomware activity averaged around 672 incidents.

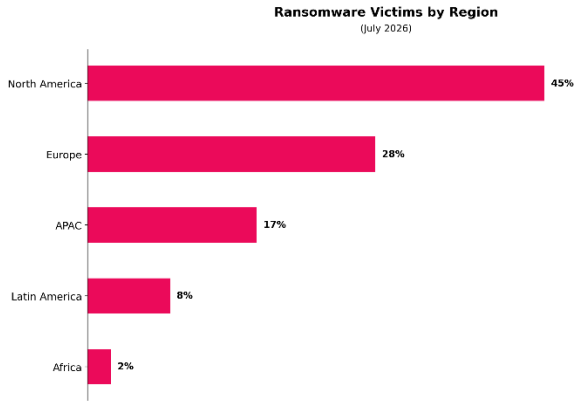


The increase was broad, touching multiple regions and industries, but Business Services remained the most affected sector, accounting for almost one third of reported victims.

Industry	Ransomware Victims
Business Services	32.5%
Industrial Manufacturing	14.4%
Consumer Goods & Services	13.4%
Healthcare & Medical	5.7%
Information Technology	5.2%
Financial Services	4.9%
Government	4.8%

Transportation & Logistics	3.6%
Automotive	3.0%
Education	2.9%

North America remained the most affected region, accounting for 45% of reported ransomware incidents. Europe followed at 28%, while APAC accounted for 17%.



Note: 5% of victims had an unknown region and are excluded from this chart.

At country level, the United States continued to dominate the victim count with 39.4% of reported attacks, followed by Germany, Canada, the United Kingdom, and Italy.

Country	Ransomware Victims
United States	39.4%
Germany	5.0%
Canada	4.4%
United Kingdom	3.5%
Italy	3.0%

The Gentlemen and Qilin Lead as the Ransomware Landscape Shifts

The Gentlemen and Qilin were the most prevalent ransomware groups in July, each responsible for **14%** of published attacks. **DeadLock** climbed to the top three, with **10%** and 97 reported victims.

- **The Gentlemen**: A fast-growing Ransomware-as-a-Service operation launched in mid-2025. The group combines ransomware operations with initial access brokering, helping it scale quickly in a short period of time.
- **Qilin**: An established Ransomware-as-a-Service group with victim disclosures dating back to 2022. Its mature affiliate model and renewed recruitment activity have helped it increase victim listings and regain momentum.
- **DeadLock**: A group first observed in July 2025. It has gained attention for using blockchain-based techniques to rotate command-and-control proxy addresses, alongside the use of legitimate remote management tools.

What July Tells Us

July's threat landscape was defined by accumulation rather than a single dominant risk. Global attacks kept rising, ransomware accelerated sharply, and GenAI exposure became more visible as part of routine business activity. For security teams, the message is clear: prevention cannot be limited to one layer or one threat category. Organizations need coordinated protection across network, cloud, endpoint, email, and AI usage, supported by the visibility to understand where sensitive data and attacker activity are moving next.