August 2026 Cyber Threat Landscape: GenAI Data Exposure Emerges as a New Enterprise Risk as Attacks, Phishing, and Ransomware Accelerate

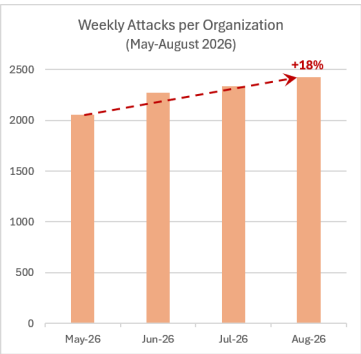
Key takeaways

- **GenAI usage continued to grow, with the average user generating 106 prompts in August, up from 95 in July and around 78 in June, while high-risk prompts remained present at 1 in every 43 prompts.**
- **Although August recorded the lowest high-risk GenAI prompt rate in several months, 86% of regular GenAI-using organizations were still affected by high-risk prompt activity, showing that data exposure remains a persistent governance challenge.**
- **By industry, Healthcare & Medical recorded the highest GenAI prompt exposure rate at 4% (1 in 25 prompts), followed by Software and Business Services at 1 in every 28 prompts.**
- **Weekly cyber attacks reached 2,422 per organization in August, up 4% from July and 22% year over year.**
- **Email phishing increased, with 1 in every 112 emails classified as phishing, up from 1 in 128 in July.**
- **Ransomware activity reached 1,042 reported attacks, almost doubling year over year and rising 8% from July.**

August showed that cyber risk is intensifying on multiple fronts at once. Global attacks continued to rise, ransomware volumes accelerated, and phishing remained a consistent entry point for threat actors. GenAI added a more nuanced but equally important signal: while August recorded the lowest rate of high-risk for data exposure in GenAI prompts in several months, enterprise AI usage continued to expand sharply, with the average number of prompts per user rising from around 78 in June to 95 in July and 106 in August. This suggests that most of the growth is coming from acceptable business use, but sensitive data exposure through prompts remains a persistent risk that organizations can no longer treat as experimental or peripheral.

Cyber Attacks Keep Climbing

The global attack curve continued to move upward in August, with organizations facing an average of 2,422 weekly cyber attacks. This marks a 4% increase from July, and a 22% increase compared with August 2025.

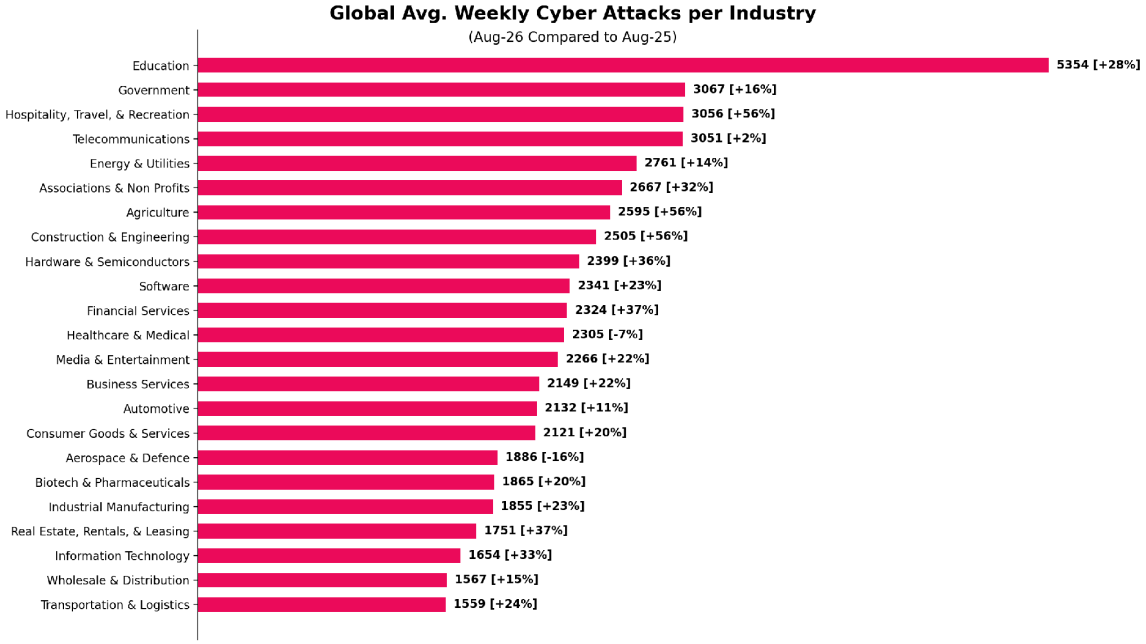


The broader four-month trend underlines the scale of the challenge: since May, the global average has climbed from 2,055 to 2,422 weekly attacks per organization, pointing to sustained pressure rather than a short-term seasonal spike.

Education Remains the Top Target as Travel-Related Sectors Rise

Education remained the most targeted sector, averaging 5,354 weekly attacks per organization, up 28% year over year. Government followed with 3,067 weekly attacks, while Hospitality, Travel, and Recreation rose to third place with 3,056 weekly attacks, up 56%. Its move into the top three, ahead of

Telecommunications, suggests attackers may be taking advantage of the operational pressure and increased customer activity linked to the peak summer travel season.



Latin America Leads in Volume as Europe Records the Sharpest Increase

Regionally, Latin America continued to face the highest attack volume, with 3,577 weekly attacks per organization on average, up 25% from August 2025. Africa ranked second with 3,335 weekly attacks, followed closely by APAC at 3,325. Europe stood out for its growth rate, recording the highest year-over-year increase at 28%, while North America rose 18%.

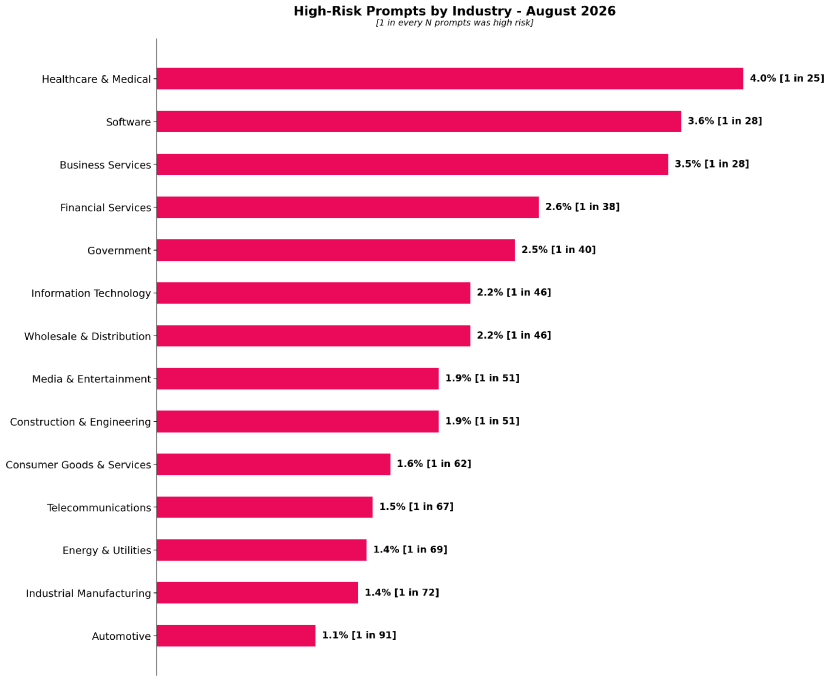
Region	Weekly Attacks per Organization	YoY Change
Latin America	3,577	+25%
Africa	3,335	+3%
APAC	3,325	+16%
Europe	2,155	+28%
North America	1,744	+18%

GenAI Risk Remains a Daily Business Reality

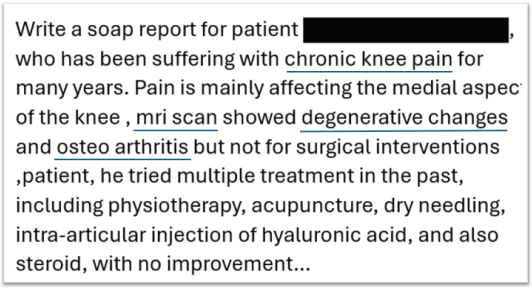
GenAI risk is now part of everyday business operations, but the August data points to a shift in the risk profile rather than a simple increase in high-risk activity. High-risk GenAI prompts fell to their lowest level in several months, at 1 in every 43 prompts from enterprise networks posing a data exposure risk. At the same time, overall usage continued to climb, with the average user generating 106 prompts during the month. This means the expansion in GenAI activity appears to be driven largely by acceptable usage, while problematic data exposure prompts have not disappeared: 86% of organizations using GenAI regularly were still affected by high-risk prompt activity, and the wide usage of various AI tools, 7 different tools on average per organization, create a critical governance gap which enhances the potential risk.

For CISOs and business leaders, the message is clear: the risk is not only whether employees are using approved or unapproved AI tools, but what information they enter into them. As teams rely on multiple GenAI applications and generate higher volumes of prompts, sensitive data can move into environments that lack sufficient visibility, governance, or control. This also increases exposure to prompt manipulation and indirect prompt injections, where hidden instructions embedded in external content can influence AI behavior and potentially expose information.

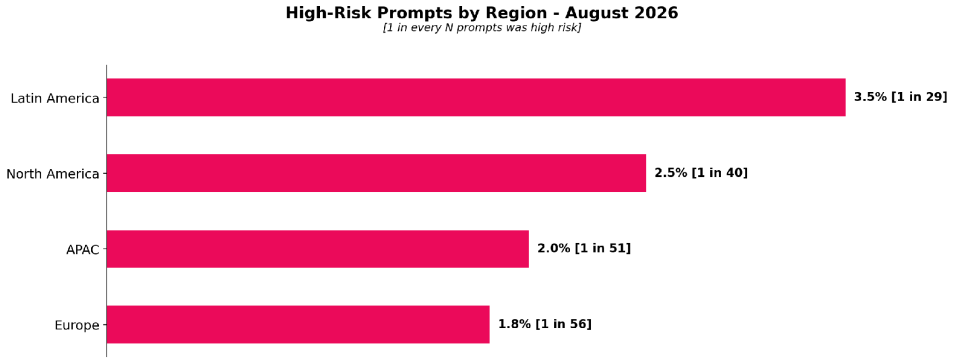
By industry, Healthcare & Medical recorded the highest rate of high-risk GenAI prompt exposure at 4%, or 1 in every 25 prompts, climbing one spot from July. Software followed at 3.6%, or 1 in 28 prompts, while Business Services reached 3.5%, also equivalent to 1 in 28 prompts.



The sensitive data exposure rate for Healthcare & Medical organizations is particularly alarming when considering this is mostly relating to extremely private information, and with users on the medical staff who are less tech-savvy and work under high pressure, potentially neglecting advised usage guidance.
Such an example can be seen below, written in ChatGPT web service, and includes the full patient's name, symptoms, examination results and diagnosis.



Regionally, Latin America recorded the highest high-risk GenAI prompt rate at 1 in every 29 prompts, or 3.5%, above the global average of 2.3%. North America followed at 1 in 40 prompts, APAC at 1 in 51, and Europe at 1 in 56. Regional differences are significant, but high-risk GenAI exposure across all regions confirms this is a global governance challenge as enterprise AI adoption accelerates.

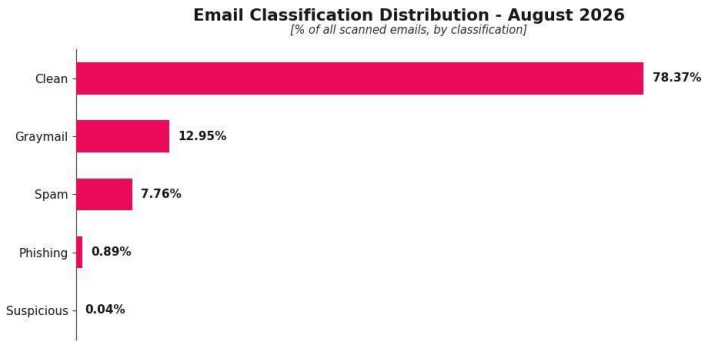


The type of information being exposed also shifted in August. Network and IT Infrastructure became the most common sensitive data category, appearing in 67% of organizations where GenAI prompts contained sensitive data. Financial Data followed at 65%, Legal and Regulatory at 64%, Employee and HR at 59%, and PII at 57%. This shows that GenAI exposure cuts across core business information, from technical infrastructure to financial, legal, employee, and personal data.

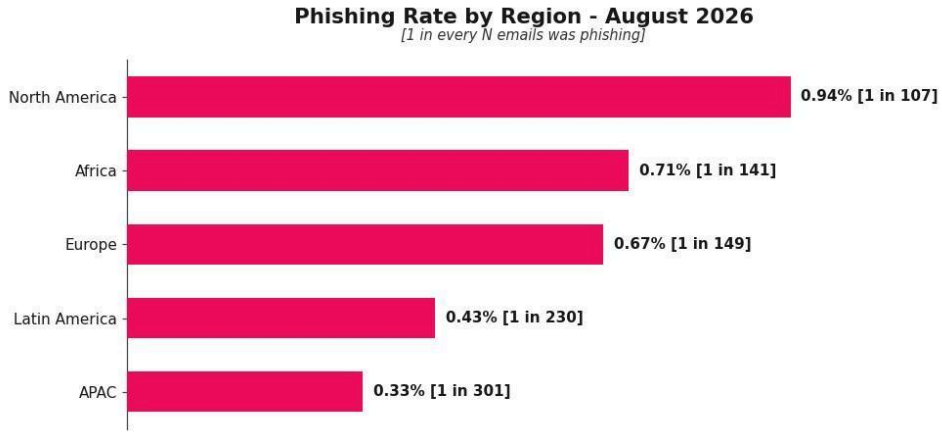
Data Category	% of Organizations
Network & IT Infrastructure	67%
Financial Data	65%
Legal & Regulatory	64%
Employee & HR	59%
PII	57%

Email Phishing Risk Increases

Email remained one of the most reliable entry points for cyber risk in August. One in every 112 emails, or 0.89%, was classified as phishing, up from 1 in 128 in July. Among phishing emails, 72% contained links and 14% contained attachments, confirming that malicious links remain a dominant delivery method. However, not all phishing relies on clickable payloads. Some emails used pure social engineering, such as requesting phone calls, sharing instructions, or encouraging direct engagement between the attacker and the victim.



North America recorded the highest phishing rate, with 1 in every 107 emails, or 0.94%, found to be malicious. By industry, Associations and Nonprofits saw the highest phishing rate at 1.87%, or 1 in 54 emails, around twice the global average. Construction and Engineering followed at 1.74%, and Real Estate, Rental, and Leasing at 1.13%.



Ransomware Activity Continues to Accelerate

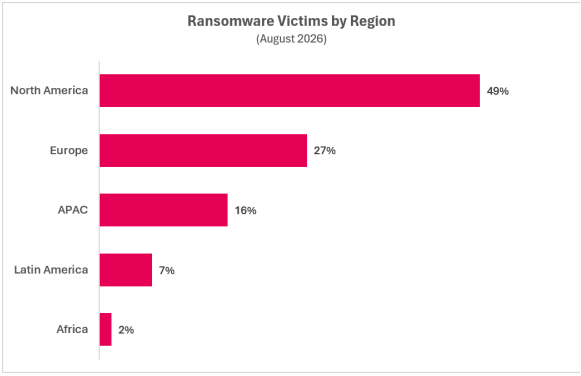
** This ransomware data draws from ransomware "shame sites" operated by double-extortion groups, which publicly disclose victim information. While these sources have inherent limitations, they provide valuable insight into the ransomware landscape.*

Ransomware activity continued to accelerate in August. A total of 1,042 ransomware attacks were reported, almost double the level recorded in August 2025 and 8% higher than in July. Business Services remained the most targeted industry, accounting for 36% of reported ransomware attacks, followed by Industrial Manufacturing at 13% and Consumer Goods & Services at 12%.

Industry	Ransomware Victims
Business Services	36%
Industrial Manufacturing	13%
Consumer Goods & Services	12%
Financial Services	8%
Healthcare & Medical	7%
Transportation & Logistics	4.1%
Information Technology	4.1%

Government	3.7%
Automotive	3.3%
Education	2.3%

North America remained the most affected region, accounting for 49% of reported ransomware incidents, followed by Europe at 27% and APAC at 16%. At country level, the United States was the most impacted country, accounting for 45% of reported ransomware attacks. Germany and Italy followed, both close to 5% of reported victims, with Canada, the United Kingdom and France also among the top affected countries.



Qilin Leads as Orova Enters the Top Three

Qilin was the most prevalent ransomware group in August, responsible for **15%** of published attacks, followed by **The Gentlemen** with **10%**. **Orova** entered the top three for the first time, accounting for **4%** of published attacks.

- **Qilin**: An established Ransomware-as-a-Service group with a consistent record of victim disclosures dating back to 2022. Its mature affiliate model and renewed recruitment efforts have helped it maintain strong momentum in recent months.
- **The Gentlemen**: A fast-growing Ransomware-as-a-Service operation launched in mid-2025. The group combines ransomware operations with initial access brokering, enabling affiliates to scale attacks quickly.
- **Orova**: An emerging ransomware group that surfaced publicly in May 2026 and has quickly gained visibility. Its activity appears access-driven rather than sector-driven, with victims concentrated among small and mid-sized businesses.

What August Tells Us

August reinforces a clear reality for security teams: prevention must now extend across every layer of the enterprise, including the fast-growing AI usage layer. Attacks are rising, ransomware remains highly active, phishing continues to open the door to compromise, and GenAI is creating a new path for sensitive data to leave the organization's control. The priority is no longer visibility alone, but preventing exposure before it becomes impact through coordinated protection across network, cloud, endpoint, email, and AI usage.