Global Cyber Claims Report | Marsh

- Executive summary
- Our taxonomy
- 2025 key trends
- Industry breakdown
- Conclusions

The defining trend for global cyber claims in 2025 was complexity

While some regions recorded slightly fewer notifications year-over-year, and a large number of correlated events in mid-2024 affected the comparison, adjusted totals for 2024 and 2025 are broadly comparable. More notable is how incidents now combine multiple loss drivers — privacy exposure, extortion, prolonged business interruption, third-party failure, and litigation — within single events. These multi-vector incidents produce larger, more legally complex, and longer-running claims.

The practical implication is that cyber resilience must be enterprise-wide, integrating security, privacy, vendor governance, legal, crisis management, and insurance design, and must be built to manage high-severity, aggregation-driven events rather than only to reduce incident counts.

Context and high-level trends

A modest year-over-year dip in some regions masked persistent high activity: much of the apparent decline results from normalizing for a cluster of correlated events in 2024.

This graph above covers the last five years of claims volume. For privacy reasons, we have indexed the volume to a baseline of 2021 levels = 100, allowing for normalized year-over-year comparisons.

In the following graph, we have identified correlated events in 2024. When removed, it shows that 2024 attritional levels were roughly on par with 2025.

Cyber claims are evolving

Contemporary claims increasingly combine privacy liabilities, business interruption, third-party impacts, regulatory action, and extortion, multiplying cost drivers, litigation risk, and recovery timelines.

Even in regions where notification volumes declined, incidents tended towards the more severe and legally complex. Losses increasingly reflect operational disruption, data misuse, regulatory scrutiny, extortion dynamics, and dependencies on external vendors.

Organizations may want to evaluate both frequency and aggregation risk across ecosystems and geographies, recognizing that a single technical compromise can cascade into multiple forms of exposure.

selected option

1. Privacy issues
2. Extortion claims
3. Non-malicious incidents
4. Insider and third-party risks
5. Severity distributions

Privacy issues dominate all claims

Privacy risk was a dominant theme across claims in several key regions in 2025.

In Europe, a substantial share of cyber notifications included privacy components; in the US and Canada, privacy litigation expanded beyond classic breach cases into non-breach actions tied to website tracking, device telemetry, and data use practices. Privacy exposure now reaches beyond incident response into compliance, governance, and civil litigation.

Notably, 2025 saw a rise in tech E&O claims related to non breach privacy statutes and litigation connected to "track and trace" or similar telemetry/analytics tools. Organizations should review how they use website tracking and analytics tools, and make sure related disclosures, consent practices, and vendor arrangements keep pace with the changing privacy risk environment.

Industry breakdown

Claims were widely spread across industries in 2025, but several key industries remain near the top as in previous years. Below is the breakdown of the top ten industries by 2025 claims volume, and a breakdown of the specific risk areas present in the top four.

Artificial intelligence (AI) layers into classes of cyber risk

In 2025, we collected a handful of claims that mentioned AI, either as an affected service, a third-party source, or other mention in the nature of the claim. However, AI is not becoming a new class of risk, but rather fits into existing classes we already track.

Currently, those risk classes appear to be:

- **Errors and misconfigurations** – This is perhaps the most exigent area where AI risk currently looms. As organizations race to deploy and reap the rewards of AI, mistakes and blind spots occur. Additionally, third-party services and suppliers may roll AI-enabled services into their platforms, introducing new risk without explicit knowledge of downstream effects.
- **Non-breach impersonation** – The first frontier of attacker AI usage has been an increase in both the volume and quality of social engineering. This leads to more convincing lures and a growing financial fraud industry. So much so that Marsh — along with key partners across the financial, cybersecurity, and retail sectors — has been working as part of the Fight Financial Fraud MITRE initiative to improve reporting and defenses against this increasing threat.
- **Network breaches** – Developments in early 2026 have indicated this may be the year where AI-driven network breaches truly arrive. Whether or not that occurs at scale, it is already true that AI has lowered the bar for attack expertise, and provided tools for attackers to scale. Given an expected increase in volume of attempts, it is all the more important for organizations to build resilience into their cybersecurity programs. Security through obscurity is not a winning strategy in an AI-scaled adversary environment.

Conclusions and looking ahead

2025 showed a clear shift: incidents became more complex and costly. Many claims combined privacy exposure, extortion, prolonged business interruption, and litigation within single events, driving larger, lengthier, and more complex losses. Non-malicious incidents (errors, misconfigurations, and passive data collection) and non-breach privacy actions grew in prominence, while extortion evolved from encryption to data theft and leak strategies that inflate downstream costs. The tail of severity expanded: median losses held steady, but the 75th percentile and above accounted for a larger share of total cost.

In 2026, expect more of the same, amplified. Aggregation-driven events will remain the principal danger as interdependent supply chains and third-party services spread impact across sectors and geographies. Privacy litigation and regulatory scrutiny are likely to increase, particularly around non breach data practices. Extortion will continue to monetize exfiltration and reputation risk rather than simply encryption-based payments. AI will raise the baseline risk by lowering attackers' entry costs and introducing new error modes in deployments and vendor services, while also improving the scale and plausibility of social engineering campaigns.

As cyber losses become more complex and severe, organizations should reassess whether insurance limits remain adequate for today's risk environment, especially given the potential for multi-faceted and high-severity claims. Incident and claims preparedness should also be a priority, including maintaining access to out-of-band communications, such as Marsh Central, and clear response protocols. Regular tabletop exercises, whether in person or facilitated through digital tools, such as Marsh Central, can help teams respond more effectively under pressure. Organizations should also review and actively manage third-party dependencies, while staying current on evolving privacy requirements and enforcement trends.

Interested in learning more?

Fill out the form to speak with a Marsh representative.