Cyber Risks & Liabilities

Cyber Insurance Market Trends to Watch in 2025

With the fast-changing nature of digital threats, cyber insurance can be an especially volatile and dynamic segment, and frequent market changes can make pricing predictions difficult to pin down. The CrowdStrike and Change Healthcare incidents highlighted the greater impact of just one cyberattack across multiple organizations and business sectors. Given the potential impact of systemic events like these, it's possible insurers will implement stricter underwriting guidelines in 2025 and may be less aggressive when it comes to lowering rates. While current price predictions indicate lower rates, mileage may vary by policyholder. Here are some key market trends to watch this year:

- **Ransomware threats**—Ransomware attacks have skyrocketed over the past decade, and blockchain analysis firm Chainalysis reported that 2024 could be the largest grossing year yet for ransomware payments. In 2025, it's expected that health care providers, schools, government agencies and other infrastructure-related organizations will be increasingly targeted in ransomware attacks.
- **Artificial intelligence (AI) exposures**—Cybercriminals can utilize AI technology to create and distribute malware, crack passwords, deploy social engineering scams, identify software vulnerabilities and analyze stolen data. This technology can enable such activities to be carried out faster and with greater success rates, which allows cybercriminals to cause major damage and even evade detection. Businesses should be particularly mindful of emerging AI-driven threats this year.
- **Supply chain vulnerabilities**—These vulnerabilities can stem from a variety of parties and practices within an organization, including third-party services or vendors with access to information systems, poor information security practices by suppliers, compromised organizational software or hardware, software security failures in supply chain management or among third-party vendors, and inadequate third-party data storage measures. Supply chain attacks are an increasing challenge for insureds, and technological research and consulting firm Gartner predicts that 45% of organizations will experience attacks on their software supply chain by 2025.
- **Data collection concerns**—A growing number of businesses have begun leveraging biometrics, pixels and other tracking technology to gather personal information from stakeholders for various HR, advertising and marketing processes; however, doing so poses several data privacy concerns. For instance, businesses that don't comply with applicable international, federal and state legislation when collecting, processing and storing stakeholders' data could face substantial regulatory penalties, costly lawsuits and associated cyber losses. As 2025 begins, businesses should be aware of heightened regulatory scrutiny and evolving privacy laws around data collection, especially as more states and countries strengthen their data privacy frameworks.

Contact us today for further cyber insurance guidance and solutions.

Plentiful Capacity for Cyber Reinsurance at Jan. 1 Renewals

The cyber reinsurance market saw a crop of new capacity for Jan. 1 renewals, according to industry leaders who confirmed reinsurance buyers saw better terms and conditions and lower risk-adjusted rates. "The cyber reinsurance market remained dynamic and innovative, with buyers exploring a range of blended solutions, from pro rata to event excess of loss and aggregate stop-loss structures," reported global risk advisory and reinsurance broker Guy Carpenter in a recent commentary. "Reinsurance buyers benefitted from improved supply and demand dynamics in 2024, driven by an oversupply of capacity, reduced demand and manageable large losses," said global insurance group Howden in a new report. The group said an additional $250 million in capacity came in from nine reinsurers entering the cyber reinsurance market—seven established carriers and two start-ups. Renewals "progressed smoothly," Howden added, citing that quota shares remain the preferred structure for buyers but more availability of excess of loss reinsurance.

“Perhaps indicative of the market conditions, or maybe reflective of reinsurers’ greater confidence in their understanding of the class, we have seen a greater willingness to offer risk excess of loss reinsurance products in support of cyber portfolios,” said Howden. “Given the ongoing spotlight on systemic events, an increasing proportion of cedents shifted their focus from proportional to nonproportional products more targeted at tail protection.” Part of reinsurers’ efforts to offer program structures aimed at systemic exposures included requiring more detail from primary insurers on the risk, the group added. “All of which translates into an increasingly mature and efficient marketplace,” said Howden. Contact us today for additional insurance industry updates.

Mitigating the Risk of Formjacking

Formjacking is a cyberattack method in which a threat actor injects malicious JavaScript into a website, often one that contains an online payment form. Once the targeted page has been compromised, the added code allows the hacker to collect sensitive data, such as credit card numbers, addresses and phone numbers. This data is sent to the cyberattacker’s domain after unsuspecting users enter their information and click “submit” to complete a transaction. Malicious actors can then use the stolen data in identity theft schemes, payment card fraud scams and account takeover attacks, or they can sell it to other criminals. Stolen information can also be used to create fraudulent accounts and distribute malware. The hacker’s code may be loaded through various methods, such as by exploiting a vulnerability in a business’s website, employing a phishing scam in which the cyber intruder gains access to a company’s checkout page, or compromising a third party’s app or JavaScript used by a business.

Formjacking attacks can have severe financial consequences, including lawsuits, fines and penalties, as well as expenses related to remediation. Moreover, formjacking can damage a company’s reputation, as clients, vendors and other partners may lose their trust in the business due to cyber incidents.

Although detecting malicious formjacking code and preventing attacks can be difficult, there are several measures businesses can take to identify potential issues and reduce the risk of it happening. Consider the following strategies:

- Practice cyber hygiene by keeping software, patches and extensions up to date. Establishing a content security policy and using firewalls and subresource integrity tags can also help prevent the injection of malicious data onto business websites and protect data.
- Scan and audit website code regularly to check its integrity. Monitoring and analyzing web logs and JavaScript behavior can help detect malicious activity, and checking where a browser is sending data is also key in stopping formjacking attacks.
- Utilize cyber defense techniques such as obfuscating JavaScript, which can make code more difficult for cyberattackers to understand. Implementing network segmentation can also limit network exposures and malicious actors’ lateral movement capabilities.
- Implement ongoing cybersecurity measures, such as thoroughly testing websites before they are publicly launched, executing penetration testing to discover vulnerabilities, and monitoring the supply chain to ensure vendors whose code is being used follow cybersecurity best practices.

Contact us today for more risk management tips.