7 Predictions For Cyber Risk And Insurance In 2026

By **Pamela Signorello, Jessica Gallinaro and Lydia Mills** (January 21, 2026)

Pamela Signorello

Jessica Gallinaro

Lydia Mills

Forecasting the future of cyber risk and coverage is a challenging task in such a rapidly evolving landscape. Nevertheless, recent trends suggest that 2026 will present organizations and their insurers with complex and costly new threats.

1. AI adoption is transforming business, but it also is creating new vulnerabilities and attacks like prompt injection, data poisoning and AI-powered phishing.

While companies continue to explore how they can implement artificial intelligence to help grow their business, the limitations and cracks that come with using AI are still being discovered. Even well-intentioned use can result in inaccurate outputs, flawed decision-making or inadvertent disclosure of sensitive data.

Threat actors have begun exploiting companies' AI systems through techniques like prompt injection and data poisoning, manipulating the models to perform in unexpected or unintended ways.

They are also leveraging generative AI to supercharge traditional cyberattacks such as deepfakes, phishing and social engineering. With the help of AI, these attacks are becoming more convincing, scalable and cost-effective, making detection increasingly difficult and expanding the pool of potential targets.

Although these types of risks are not necessarily new, there has been a tremendous spike in their frequency, and no sign of their slowing anytime soon. Despite these developments, there has yet to be a marketwide response to these new threats in the cyber insurance market.

As companies seek coverage for more AI-related losses, insurers will likely implement form exclusions or impose sublimits in response.

2. Website tracking lawsuits under CIPA will remain high, and the lack of uniformity in case law and AI adoption will fuel more filings in 2026.

The past year continued the rising trend of demand letters, arbitration and litigation targeting companies for alleged privacy violations tied to the use of online tracking tools, such as pixels, cookies, chat features and session replay. At the center of many of these cases is the California Invasion of Privacy Act, a wiretapping statute dating back to 1967.

Several trends suggest that CIPA-related activity will continue — or even accelerate — in 2026.

Courts remain divided on the applicability of CIPA in the website tracking context, and the lack of uniformity will only fuel new filings.

Pro se claimants have also begun to issue demand letters or institute arbitration proceedings, leveraging the statutory penalties provided for under CIPA to obtain quick settlements.

The current hyperfocus on AI and the adoption of AI tools in various business applications may contribute to a new wave of CIPA claims, such as claims alleging that a website's AI-powered virtual assistants "eavesdropped" on and/or repurposed the visitor's communications without consent.

California lawmakers attempted to address this trend by introducing S.B. 690, which would create a commercial business purpose exception for routine website technologies used for ordinary business purposes.

The California Senate unanimously passed the bill in June 2025, but it stalled in the Assembly. Now, the earliest S.B. 690 can be reconsidered is 2026, in which case it would not take effect before 2027. Even then, S.B. 690 would only apply prospectively, meaning that, if enacted, it would not affect any lawsuits filed before then.

3. Amendments to the CCPA introduce mandatory cybersecurity audits and risk assessments that will become key documents in litigation and enforcement.

California continues to lead the privacy landscape in terms of privacy regulation and enforcement with its recent amendments to the California Consumer Privacy Act, or CCPA, that were approved in September 2025 and became effective Jan. 1.

As part of these changes, California has now implemented cybersecurity audit and risk assessment obligations for companies doing business in the state.

Under Title 11 of the California Code Regulations, Section 7122(a), the new annual cybersecurity audit required for businesses that meet defined thresholds, must be conducted by an internal or external "qualified, objective, independent professional" who uses accepted audit standards.

The report must be given to an executive management team member who can attest, under penalty of perjury, that the business completed the audit and did not attempt to influence the auditor.

The report, which must be retained for at least five years, also must discuss in detail the gaps and weaknesses in the company's cybersecurity policies, procedures and practices, and the company's plan to remediate them.

These, presumably, nonprivileged audit reports called for by the CCPA's amendment may become key documents in litigation and regulatory enforcement — and in responses to questions following a breach — for years to come.

4. States are partnering with private firms for privacy enforcement and expanding focus to midsize companies, signaling a growing compliance risk for companies of all sizes.

In the absence of comprehensive federal privacy law, states are increasingly taking privacy regulation into their own hands.

Amid the onslaught of recent state privacy litigation, such as the comprehensive privacy

laws enacted by eight states in 2025, state attorneys general are emerging as the main privacy regulators, forming dedicated privacy units and collaborating across state lines.

As part of this new wave of privacy enforcement, attorneys general are partnering with private law firms. By using private firms as outside counsel, attorneys general are able to pursue more complex privacy litigation without the usual resource constraints, making it an effective tool for the enforcement of state privacy laws.

With the rise of state privacy regulations, the increase in nuclear settlements and judgments, and the lowered resource depletion of attorneys general offices, the new wave of privacy enforcement will likely reach beyond large companies to midsize and smaller companies.

Businesses should expect more aggressive enforcement and invest in compliance programs accordingly.

5. Kids' privacy is taking center stage nationally and among states.

A growing emphasis on children's privacy is emerging, with states increasingly adopting measures aimed at protecting kids' personal data and limiting their access to certain content and services.

In a demonstrably coordinated move, on Aug. 25, 2025, a bipartisan coalition of 44 state and territorial attorneys general issued a letter to the CEOs of several prominent, U.S.-based companies addressing children's safety, particularly in the context of minors' anticipated interactions with AI products like chatbots. The letter implied that the states are prepared to use existing consumer protection, child safety and unfair-practice laws to hold companies accountable for harm to minors.

Under the circumstances, companies will do well to review their age-gating, user-verification, parental control, and content moderation and filtering processes, and more generally to adopt a conservative posture when designing experiences where minors may interact with AI.

In light of the national spotlight on children's online safety, 2026 likely will bring with it an unusual amount of state enforcement activity in this context, including the risk of simultaneous multistate actions against companies whose AI features engage with minors.

Add this to the growing mix of private class actions over children's data, and 2026 will be highly kid-centered on the privacy front.[1]

6. Courts are debating what counts as direct loss in social-engineering fraud cases, trending toward more scrutiny and possible AI-related exclusions in policies.

The concept of direct loss under cyber insurance has become a pivotal point of contention, especially in cases involving social engineering fraud. As insureds increasingly face sophisticated cyber threats that exploit human behavior — i.e., AI-generated impersonation — whether the resulting financial harm qualifies as a direct loss under insurance policies has taken center stage.

This issue was at the heart of Office of the Special Deputy Receiver v. Hartford Fire Insurance Company, an Illinois federal case involving multimillion-dollar losses after a

spear-phishing attack resulted in the compromise of the CFO's email account.[2]

The cyber insurance carrier denied coverage under the policy's computer fraud insuring agreement, arguing that the loss was not the direct result of a computer crime as required by the policy because the insured's employees were the ones who issued the payments, not the fraudster.

On March 31, 2025, the U.S. District Court for the Western District of Illinois, however, rejected this argument, finding that, as the transfers were "a direct response" to the fraudulent emails issued from the CFO's account, the computer crime could be said to have directly caused the loss.

Other jurisdictions interpret the term "direct" more narrowly.[3]

The Office of the Special Deputy Receiver ruling, however, reflects a growing trend where courts recognize that cyber deception resulting in losses due to manipulated human behavior may be sufficiently direct to trigger computer fraud coverage, unless policies are explicitly drafted to address such scenarios.

7. Recent court rulings expanding the scope of coverage provided for third-party claims involving funds transfer fraud are ripe for further evaluation.

With the rise of funds transfer fraud schemes, insureds are increasingly seeking to expand the scope of coverage under third-party insuring agreements.

Specifically, insureds have argued that a breach of contract claim against them by the intended recipient of the diverted funds should qualify as a claim for a security breach, notwithstanding that the contract claim is not predicated on the security breach of an insured's computer systems but rather on the insured's failure to pay.

Two 2025 cases — Kane v. Syndicate 2623-623 Lloyd's of London, decided by the New Mexico Court of Appeals, and Connelly Law Offices PLLC v. Cowbell Cyber Inc., decided by the U.S. District Court for the Western District of Washington — found ambiguity in the word "for" in this context, rejecting insurers' arguments that the parties had agreed to limit coverage associated with funds transfer fraud.[4]

As claims associated with an insured's failure to pay amounts due after experiencing a funds transfer fraud proliferate, more coverage litigation applying causation principles in this context is expected.

Conclusion

In 2026, cyber risk and insurance will be shaped by the rapid adoption of AI, ongoing privacy litigation and evolving regulatory requirements. As organizations increasingly integrate AI into their operations, they will contend with new vulnerabilities and a shifting legal landscape that demands greater vigilance and adaptability.

AI-driven attacks and privacy lawsuits — especially under CIPA — will remain prevalent, while new mandates like the CCPA's cybersecurity audits will raise the bar for compliance. This means companies will face not only more sophisticated threats but also heightened scrutiny from regulators and courts, making robust cybersecurity and privacy programs essential for risk mitigation.

State regulators are expanding enforcement, including actions focused on children's privacy and midsize companies. The broadening scope of enforcement signals that no organization is immune, and even smaller businesses must prepare for increased oversight and potential multistate actions.

Courts are broadening coverage for social engineering and funds transfer fraud, but insurers are likely to respond with tighter policy language, exclusions and more coverage litigation in turn.

By investing in forward-looking strategies and staying abreast of regulatory changes, businesses and their insurers can better position themselves to navigate the challenges and opportunities that 2026 will bring.

Pamela Signorello is a partner, Jessica Gallinaro is of counsel and Lydia Mills is an associate at Wiley Rein LLP.

[1] See, e.g., Diaz v. Paramount Skydance Corp., Case No. 25-2945 (C.D. Cal.) (filed Nov. 4, 2025); S.K. v. Disney Worldwide Services Inc., Case No. 25-8410 (C.D. Cal.) (filed Sept. 5, 2025).

[2] Office of the Special Deputy Receiver v. Hartford Fire Insurance Company, No. 22-cv-03709, 2025 U.S. Dist. LEXIS 60484 (N.D. Ill. Mar. 31, 2025).

[3] See, e.g., Whitney Equip. Co. v. Travelers Cas. & Sur. Co. of Am., 431 F. Supp. 3d 1223 (W.D. Wash 2020) ("Washington cases interpret 'direct' in the context of insurance coverage as 'without any intervening agency or step: without any intruding or diverting factor.'").

[4] See Kane v. Syndicate 2623-623 Lloyd's of London, No. A-1-CA-41254 (N.M Ct. App. June 16, 2025); Connelly Law Offices PLLC v. Cowbell Cyber Inc., No. 25-cv-00302-JHC (W.D. Wash. Aug. 7, 2025).