wiley

ALERT

Wiley's Cyber Risks and Insurance 2026 Forecast

December 1, 2025

As we prepare to close the books on another eventful year in the cyber and privacy space, Wiley's Cyber Insurance team is already making predictions for 2026.

Q: With the increase in the use of generative AI, how have the types of exposures specific to this new technology evolved, and how will they be addressed in 2026?

Jessica Gallinaro: There's no doubt that many companies are exploring how they can implement AI to help their businesses, from increasing their own efficiency and productivity to enhancing their customers' experiences. But with any new innovation comes new potential exposures. Because generative AI is a kind of technology that many companies have not utilized before, they may not appreciate the limitations of the technology or the nuanced differences between the tools offered by various providers. As a result, even the most well-intentioned use of AI can lead to errors in AI-generated content, failures of AI decision-making tools, or disclosures of sensitive information, all of which expose companies to potential liability. Threat actors are also infiltrating companies' AI models and using them to execute new kinds of attacks, such as prompt injections or data poisoning, that manipulate the models and cause them to perform in an unexpected or unintended way.

In addition, many threat actors are relying on generative AI to escalate familiar attacks like deepfakes, social engineering, and phishing by making them more convincing and also by increasing their reach. People can no longer easily spot a social engineering scam using good judgment alone, now that threat actors can use AI to craft highly personalized messages with information scraped from

Authors

Pamela L. Signorello
Partner
202.719.3321
psignorello@wiley.law

Jessica N. Gallinaro
Of Counsel
202.719.4189
jgallinaro@wiley.law

Nathan B. Lovett
Partner
202.719.7295
nlovett@wiley.law

Mallory Meaney
Associate
202.719.4575
mmeaney@wiley.law

Lydia A. Mills
Associate
202.719.4735
lmills@wiley.law

Practice Areas

Cyber Insurance

Insurance

social media and the internet. And threat actors can use AI models to deploy these attacks more quickly and cheaply than before, meaning more people have become potential targets. So, while these types of risks are not necessarily new, there has been a tremendous spike in how frequently they occur now, and there is no sign of a downswing anytime soon.

We have yet to see a market-wide response to these new threats in the context of cyber policies. As companies seek coverage for more AI-related losses, it is possible that we may ultimately see more carriers add form exclusions for such losses. For now, though, carriers should be mindful of potential trigger issues, as well as carve-outs or exclusions for amounts incurred by companies to harden their systems following an attack.

Q: Do you expect the surge of website tracking technology claims, specifically those alleging violations of CIPA, to continue?

Nate Lovett: The past year was again marked by a tidal wave of demand letters, arbitration, and litigation targeting companies for alleged privacy violations tied to the use of online analytics tools, such as pixels, cookies, chat features, and session replay. One of the most frequently cited statutes in these cases is the California Invasion of Privacy Act (CIPA), a wiretapping statute that dates back to 1967.

Several trends suggest CIPA-related activity will remain steady – or even accelerate – over the next year. The growing body of case law interpreting CIPA in the website tracking context continues to be mixed, and the lack of uniformity will fuel new filings. Pro se claimants have also started to throw their hats in the ring with demand letters or arbitration geared toward quick settlements, leveraging statutory penalties under CIPA. Moreover, the current hyperfocus on AI and adoption of AI tools in various business applications will likely contribute to a new wave of CIPA claims – e.g., claims alleging that a website's AI-powered virtual assistants "eavesdropped" and/or repurposed the visitor's communications without consent.

In response to the surge, California lawmakers introduced Senate Bill 690 (SB 690) that seeks to amend CIPA to provide a "commercial business purpose" exception. If enacted, SB 690 would clarify that routine website technologies do not constitute unlawful wiretapping or eavesdropping when used for ordinary business purposes. The proposed legislation passed the California Senate in June 2025 by unanimous vote, but stalled in the Assembly, which converted SB 690 to a two-year bill. Now, the earliest SB 690 can be reconsidered is 2026, and it would not take effect before 2027. Prior to its passage in the Senate, SB 690 was amended to apply prospectively, not retroactively, meaning that, if enacted, it would not affect any lawsuits filed before its enactment or prior to its effective date.

While SB 690 would significantly curb the current pace of claim activity, the delay and uncertainty surrounding its enactment mean that CIPA cases will continue to be filed at a rapid pace for the foreseeable future.

Q: Anything else noteworthy happening in California in the privacy space?

Pam Signorello: Always. Amendments to the California Consumer Privacy Act were approved in September 2025 and become effective on January 1, 2026. They include, among other things, cybersecurity audit and risk assessment obligations for companies doing business in California. Of particular note, there is a new annual cybersecurity audit requirement for businesses that meet defined thresholds. The audit must be conducted by a "qualified, objective, independent professional" (internal or external) who uses accepted audit standards, and the audit report must be delivered to an executive management team member who is ultimately responsible for attesting under penalty of perjury that the business completed the audit and did not attempt to influence the auditor. Among other things, the audit report (which must be retained for at least five years) must discuss "in detail" the gaps and weaknesses in the company's cybersecurity policies, procedures, and practices and how the business plans to address them and in what time frame.

In the absence of a comprehensive federal privacy law, I expect California to continue to be a leader among states in terms of privacy regulation and enforcement. I also think it's fair to predict that the (non-privileged) audit reports called for by the CCPA's amendment will be key documents in litigation and regulatory enforcement (and in responses to questions following a breach) for years to come.

Q: What can we expect to see in terms of privacy enforcement at the state level?

Lydia Mills: States are increasingly taking privacy regulation into their own hands in the absence of an overarching federal privacy legislative scheme. Amidst the onslaught of recent state privacy legislation, such as the comprehensive privacy laws that went into effect in eight states this year, states' Attorneys General have been increasingly empowered to serve as the main privacy regulators. States such as California, Texas, and Virginia have even begun forming privacy-centered units focused on enforcement of and compliance with state privacy laws, including by means of interstate collaboration.

As part of this new wave of privacy enforcement, Attorneys General are now pairing with private law firms to bring lawsuits against large corporations, alleging violations of the various data privacy laws. For instance, in Texas, Attorney General Paxton recently partnered with a law firm and obtained a billion-dollar settlement in a consumer privacy lawsuit. Similarly, Michigan, Nebraska, and Utah attorneys general have recently filed suit against various companies in collaboration with various law firms. By partnering with private firms as outside counsel – often, if not always, under contingency fee arrangements – Attorneys General are able to pursue more complex privacy litigation without the resource constraints that usually plague them. As such, it is likely that we will see even more Attorneys General working with outside counsel as a part of their enforcement toolbox and, subsequently, more enforcement litigation.

So far, states' Attorneys General primarily have focused on large companies with deep pockets; however, with the rise of state privacy regulation, an increase in nuclear settlements and judgments, and lowered resource depletion in Attorneys General offices, it is likely that the new wave of privacy enforcement will continue to expand to midsize and smaller companies. In the coming year, companies should continue to evaluate and invest in their compliance programs with an eye towards this expanding privacy battleground.

Q: Is there any emerging privacy focus of particular interest among states?

Pam Signorello: There is a growing emphasis on children's privacy, 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 August 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, unfair-practice, and related laws – not necessarily new federal AI legislation – to hold companies accountable if harm to minors occurs. In other words, the AGs have signaled that they will not wait for Congress to act; they are prepared to bring state-law enforcement actions now. The AGs' letter outright warns: "If you knowingly harm kids, you will answer for it."

On the heels of the AGs' coordinated move, in September, the Federal Trade Commission announced that it had launched its own inquiry into several companies that operate consumer-facing AI chatbots concerning potential harm to minors who use their "chatbots acting as companions."

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

In light of the national scale of this regulatory 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 multi-state actions against companies whose AI features engage with minors. Add this to the growing mix of private class action litigation over children's data, and 2026 could be the Year of the Child on the privacy front. *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).

Q: What are some of the key developments in case law involving cyber insurance policies?

Bill Knauss: In the evolving landscape of cyber insurance, the concept of "direct loss" 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 (think AI-generated impersonation), the question of whether resulting financial harm qualifies as a "direct loss" under insurance policies has taken center stage. This issue was at the heart of a case decided in Illinois federal court captioned *Office of the Special Deputy Receiver v. Hartford Fire Insurance Company*.

Office of the Special Deputy Receiver involved a legal dispute as to whether certain losses constituted a "direct loss" under a cyber insurance policy. In this case, an insured company experienced multimillion-dollar losses after a spear-phishing attack resulted in the compromise of the CFO's email account. The cybercriminal tricked the insured's employees into wiring funds to a fraudulent account by sending phony emails impersonating the CFO.

The cyber insurance carrier denied coverage under the policy's Computer Fraud insuring agreement. The Computer Fraud coverage applied to claims for loss "incurred . . . as a direct result of Computer Crimes." The Policy defined "Computer Crime" to mean "the intentional, fraudulent, or unauthorized input, destruction, or modification of electronic data or computer instructions into Computer Systems by any entity which is not an Insured Organization or person who is not an Insured Person . . . ." The insurer argued that the loss was not the "direct result" of the Computer Crime because, while the fraudster did gain access to the CFO's account, it was the insured's employees who actually issued the payments based on the fraudulent emails.

In the ensuing coverage litigation, the court rejected the insurer's argument that "finding direct loss here would improperly substitute a proximate cause analysis for a direct loss analysis." Instead, the court held that the transfers were "a direct response" to fraudulent emails issued from the CFO's account, which was "adequate" to show that Computer Crimes directly caused the loss.

To be clear, other jurisdictions interpret the term "direct" more narrowly. *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.'") 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. We recently discussed this case in further detail on Wiley's *The Cyber Periscope* podcast – give it a listen here!

Q: What third-party cyber insurance issue is ripe for further evaluation from the courts in 2026?

Mallory Meaney: Despite first-party sublimits applicable to recover funds unwittingly paid by insureds in funds transfer fraud schemes, insureds have attempted to expand the scope of third-party insuring agreements that cover claims "for" a security breach to include breach of contract claims from the insured's payees that were the intended recipients of funds diverted in funds transfer fraud schemes. Such breach of contract actions by payees for an insured's failure to pay lack the causal connection to the security breach that precipitated the funds transfer loss scheme to constitute a claim for a security breach. Indeed, an action for failure to pay an invoice or otherwise meet a payment obligation cannot constitute an action for the security breach of an insured's computer systems as the payee's concern is not that the insured's systems were breached but rather that it did not receive payment due.

Two decisions issued this year, by a Washington federal court and the Court of Appeals of New Mexico, took pains to transform third-party claims for insureds' failure to pay amounts due into claims "for" a security breach. *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). In so holding, the courts rejected the plain meaning of the word "for," found ambiguity in the commonly understood word, and failed to consider the language in light of the entire policy, in which the parties had agreed to limit coverage associated with funds transfer fraud.

As demands associated with an insured's failure to pay amounts due following funds transfer fraud on an insured is an all-too-common scenario, insurers may take steps to show that these recent cases were wrongly decided and distinguishable, including through litigation of this issue to ask that courts honor the plain meaning of the language, apply appropriate causation principles, and consider the applicable language together with the policy as a whole.

* * *

Wiley's deep cyber insurance bench is navigating these complex cyber and privacy challenges with its clients, alongside their significant business partners and insureds. Please join us in discussion throughout the new year on Wiley's podcast dedicated to exploring issues and developments relevant to the cyber insurance professional community: *The Cyber Periscope*. In the meantime, we wish everyone a memorable holiday season!