wiley

ALERT

Cyber Risks and Insurance 2025 Forecast

December 19, 2024

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 2025.

Q: So, let's get right into it – based on your experience this year, what do you think is in store on the ransomware front in 2025?

Nate Lovett: In recent years, ransomware attacks have grown substantially more sophisticated and targeted. Coordinated federal and international crackdowns knocked out several notorious ransomware gangs in 2023, only to have many of them reorganize and rebrand in 2024. Unfortunately, we do not see ransomware activity slowing down in 2025, particularly as threat actors increasingly deploy AI and other sophisticated measures to help them carry out attacks. With attacks becoming more targeted, we can expect threat actors to continue to target high-value sectors such as critical infrastructure, health care systems, telecommunications, financial services, and supply chain vendors, in particular.

The cyber extortion landscape has also seen a spike in incidents involving data exfiltration, with threat actors attempting to leverage a threat to disclose sensitive personal and/or business information as a secondary (or principal) basis to compel victims to pay. Even where a company makes payment in exchange for a threat actor's "promise" not to publish exfiltrated data, there is no guarantee that the data will be permanently deleted. Consequently, we have seen certain threat actors scour the dark web for data that was already leaked in an effort to re-extort victims.

During 2024, one of the main issues the cyber insurance industry faced was the rise of large-scale ransomware incidents that impact numerous downstream entities (for example, the Change Healthcare

Authors

Leslie A. Platt
Partner
202.719.3174
lplatt@wiley.law

Margaret T. Karchmer
Partner
202.719.4198
mkarchmer@wiley.law

Pamela L. Signorello
Of Counsel
202.719.3321
psignorello@wiley.law

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

William F. Knauss, III
Special Counsel
202.719.4521
wknauss@wiley.law

Nathan B. Lovett
Associate
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

Privacy, Cyber & Data Governance

incident). These large-scale incidents have caused cyber insurers to take a closer look at systemic risk, not just with respect to first party coverage, but also with respect to data breach class actions.

Q: Speaking of data breach class actions, what are you expecting in 2025?

Maggie Karchmer: As Nate observed, cyberattacks are growing in sophistication and severity. The result: more data breaches – including large-scale data breaches – and more class action litigation. Data breach has emerged as one of the fastest growing areas of class action litigation. The past two years saw a significant increase in data breach class action lawsuits, as well as some record settlements. The number of individuals impacted by data breaches has grown substantially, resulting in larger classes and higher settlement amounts. Financial services and health care companies are particularly in focus and, based on the sensitive nature of the data they hold, will continue to be.

Due to the large number and variety of consumers and other victims of these sophisticated data breaches, we likely can expect to see more multi-district litigation (MDL) in this context, like the MDLs currently pending in federal court in Massachusetts and Minnesota stemming from the MOVEit and Change Healthcare data breaches, respectively.[i] The MDL process has its own share of efficiencies as well as detractions, including that – for now – it operates outside of the Federal Rules of Civil Procedure and arguably lacks an effective mechanism for weeding out meritless claims, which defendants may be induced to resolve by way of aggregate settlement.

Courts continue to grapple with issues relevant to legal standing and class certification in the context of data breach class actions, including whether and how any concrete injury may be traced to a particular data breach (particularly where they have become so omnipresent). In point of fact, so far, courts have rarely granted class certification in these cases. However, as these matters come to increasingly involve the compromise of particularly sensitive data, the plaintiffs' bar conceivably could begin to experience more success establishing the requisite harm on a class-wide basis. In that event, settlements in this context could see a boost, though we are obviously hesitant to predict anything like that in the coming year (and particularly where the nature of the data at issue in any given breach technically should have no bearing on the traceability of a concrete injury to said breach).

Q: What can cyber insurers expect to see in the business interruption space?

Bill Knauss: Business interruption coverage in the cyber insurance context is unique because, unlike traditional business interruption policies that are typically triggered by physical damage to property and well-established property valuations, cyberattacks typically do not involve physical damage to property, and the financial impact resulting from compromised electronic data can be difficult to pin down. In our experience, resolving business interruption losses in the cyber insurance context is still dependent on a firm understanding of the coverage and the involvement of a knowledgeable forensic expert to identify the loss quantum.

There is comparatively little case law interpreting cyber insurance policies, including with respect to business interruption loss. However, we've seen two important rulings during 2024 that will inform our assessment of coverage for business interruption losses going forward: *Southwest Airlines v. Liberty Ins. Underwriters Inc.* and

Heritage Co. Inc. v. Hudson Excess Ins. Co.

In *Southwest*, the Fifth Circuit held that certain losses incurred by an insured following a computer system failure could not be categorically excluded from coverage under a cyber policy on the grounds that they were the result of "purely discretionary" business decisions.[ii] In doing so, the court applied a broad interpretation of the term "solely." However, other jurisdictions interpret the term more narrowly, and some of the holdings in *Southwest* may be distinguishable on the basis of policy wording.

In *Heritage*, the U.S. District Court for the Eastern District of Arkansas ruled in favor of Wiley's client, holding that policy language establishing the methodology for calculating "Business Income Loss" was unambiguous.[iii] Jess Gallinaro, a key player in the *Heritage* litigation, discusses the *Heritage* ruling in further detail below.

Q: How do you see the win for Wiley's client in *Heritage* impacting the resolution of business income loss claims?

Jess Gallinaro: The ruling in *Heritage* establishes important precedent on the proper methodology for calculating business income loss under not only Arkansas law, but also in the context of cyber insurance more generally. I am proud to be part of the Wiley team that secured the ruling in *Heritage*, along with my colleagues Ashley Eiler and Mallory Meaney.

In its ruling, the court agreed with our client's methodology for calculating "Business Income Loss" under the policy, which required subtracting expenses from total revenue *plus* only those normal operating expenses that were not paid using revenue actually earned during the interruption period. In this way, the court sought to uphold the purpose of business interruption coverage – that is, to protect the insured while also preventing the insured from being placed in a better position than if no loss or interruption of the business had occurred. Any other interpretation, such as the one proffered by the insured in that case, would allow the insured to sustain a windfall.

To date, there has been very little case law discussing the calculation of business income loss under a cyber insurance policy. This case is now one that insurers may cite to going forward to support their calculations of an insured's business income loss, particularly in those situations where insureds are seeking coverage for amounts that have not actually been lost (like non-continuing expenses) or are otherwise seeking a windfall from their insurance. While the amount of business income loss is usually a question of fact for trial, established case law setting forth the proper calculation of business income loss can serve to further narrow the disputes that arise in business income loss claims.

Q: What's on the horizon for third-party data sharing claims?

Pam Signorello: The Second Circuit's October 15, 2024, decision in *Salazar v. NBA*, interpreting the definition of "consumer" under the Video Privacy Protection Act (VPPA), may open back the floodgates on VPPA class action lawsuits involving website tracking.[iv] Prior to that decision, there was a split of authority as to who satisfied the standard for asserting a claim under the statute, with the Southern District of New York, in

particular, having dismissed a substantial number of VPPA lawsuits brought in the website tracking (e.g., pixel) context. Under *Salazar*, the standard for qualifying as a "subscriber of goods or services" (for the purpose of the VPPA's "consumer" definition) was arguably lowered (to include a subscriber to a digital newsletter), although the court was mindful to state upfront that its ruling was "narrow" and limited to the specific subscriber-related allegations made in that case.

With only a small fraction of (the hundreds of) website tracking claims (brought under the VPPA, federal and state wiretap statutes, and common law alike) having gone to settlement, and a substantial number of such cases now beyond the motion to dismiss stage, we likely will see decisions on class certification begin to issue in earnest in 2025. And plaintiffs should be up against some compelling arguments for denying class cert in this context, including in terms of ascertainability and typicality (see *Doe v. MedStar Health, Inc.*[v]*)*, as well as numerosity (see *Martinez v. D2C, LLC****[vi]***).

While 2023 was certainly a watershed year in terms of significant decisions issued by the Illinois Supreme Court interpreting the reach of that state's Biometric Information Privacy Act (BIPA) – *see Tims v. Black Horse Carriers, Inc.[vii]* (holding that five-year statute of limitations applies to BIPA claims); *Cothron v. White Castle Sys., Inc.[viii]* (holding that a claim for damages under BIPA accrues in each and every instance of a violation, while notably also observing that damage awards are discretionary under BIPA); and *Mosby v. Ingalls Mem'l Hosp.[ix]* (applying BIPA's "health care exception" to certain biometric information collected from employees of health care providers) – 2024 did not disappoint either. On August 2, 2024, Illinois Governor J.B. Pritzker signed into law the BIPA Reform Bill (Public Act 103-0769), which caps liability to one "violation" per person, providing defendants with a significant argument against potentially exorbitant BIPA damages under the *White Castle* decision. However, the retroactivity of the amendment remains the subject of heated debate, and the legal battle over whether pre-amendment claims are (un)affected should continue into the New Year.[x] Particularly if trial court decisions continue to diverge on the issue of retroactivity, we may be looking to another case to test the bounds of BIPA (and its recent amendment) with the Illinois Supreme Court in the coming year.

Q: Should we anticipate further cloud service provider outages and systemic cyber risks in 2025?

Mallory Meaney: With an increasingly interconnected digital world and insureds seeking cybersecurity control tools from a handful of top providers, the risk of a cloud service provider outage or a systemic cyber risk will continue through 2025 and beyond.

A number of recent, high-profile cloud service provider outages and systemic cyber risks disrupted business operations for key industries, including but not limited to transportation, health care, and banking. Cyber insurers and their insureds will continue to navigate the first- and third- party aspects of matters arising from those cloud service provider outages and systemic cyber risks for years to come.

As these cloud service provider outages and systemic cyber risks are certain to continue, it will behoove cyber insurers to reflect on trends and successful strategies in handling such matters to be better prepared for claims arising out of cloud service provider outages and systemic cyber risks in the future. Cyber insurers

should expect to see claims that involve sprawling, multi-district litigation, claims for business interruption loss that present coverage questions, and evaluations of whether subrogation is available and appropriate.

Q: Thoughts on the future of data privacy regulation under the incoming Administration?

Leslie Platt: A Republican-led Congress could pass federal comprehensive privacy legislation (possibly a weaker version of the "American Data Privacy and Protection Act"), which stalled due to major disagreements between lawmakers regarding the extent of consumers' control over their data, how to enforce privacy violations (by private right of action or otherwise), and whether a federal law should override existing state privacy laws. In that event, it is at least conceivable that some state privacy statutes conferring a private right of action (like BIPA and the CPRA), which have led to a wave of class action lawsuits against businesses, could be preempted. That being said, it is admittedly difficult to predict where privacy will fall relative to other issues that the incoming Administration has identified as immediate priorities. While privacy enforcement will continue under the FTC, the agency may do less rulemaking and issue less guidance under President Trump.

Q: How do you see your clients' insureds confronting cybersecurity challenges going forward?

Lydia Mills: The U.S. government directed federal agencies to adopt Zero Trust security architecture by the end of Fiscal Year 2024. Many state and local governments also are working toward implementing that cybersecurity model. Although the private sector will continue shifting resources to increase investment in cybersecurity solutions, universal adoption of Zero Trust before the end of 2025 is unlikely due to the upfront costs and perceived burden on application performance.

As my colleagues have noted, AI-driven cyber-attacks are poised to become more sophisticated and frequent. Threat actors are using AI to automate the discovery of vulnerabilities, quickly identify high-value targets, and accelerate attack timelines. In addition, the prevalence of generative AI has allowed threat actors to mimic a person's writing style, voice, and appearance, leading to an unprecedented increase in deepfake phishing attacks.

Threat actors are not the only ones using AI, however. As the technology matures, AI will play an increasingly significant role in cybersecurity measures. AI-powered security tools aim to quickly identify threats to reduce the potential impact of a cyberattack. AI can also be used to automate incident response tasks, such as blocking malicious IP addresses and isolating compromised systems. All other factors being equal, attacks that are stopped earlier (or thwarted altogether) will be less costly to recover from.

* * * * *

Over the past several years, as its insurance clients' exposures to cyber and privacy claims have grown exponentially, Wiley's insurance practice intentionally has committed itself to expand its team to match its clients' urgent needs in these significant areas. Wiley's deep cyber insurance bench is incredibly grateful to be positioned to navigate these challenges with its exceptional clients, alongside their significant business

partners and insureds, in the years ahead. We wish everyone more peace (than breach) this holiday season and a very happy and healthy New Year!

---

[i] See *In Re MOVEIt Customer Data Security Breach Litigation*, 699 F.Supp.3d 1402 (J.P.M.L. 2023); *In Re Change Healthcare, Inc. Customer Data Security Breach Litigation*, MDL No. 3108, 2024 WL 2884723 (J.P.M.L. June 7, 2024).

[ii] 90 F.4th 847 (5th Cir. 2024).

[iii] No. 4:22-cv-82-JM, 2024 WL 2325057 (E.D. Ark. May 22, 2024).

[iv] 118 F.4th 533 (2d Cir. 2024).

[v] No. 24-C-20-000591 (Md. Cir. Ct. Mar. 10, 2023).

[vi] No. 23-21394 (S.D. Fla. Oct. 1, 2024).

[vii] 216 N.E.3d 845 (Ill. 2023).

[viii] 216 N.E.3d 918 (Ill. 2023).

[ix] 234 N.E.3d 110 (Ill. 2023).

[x] See *Gregg v. Central Transp. LLC*, No. 24 C 1925, 2024 WL 4766297 (N.D. Ill. Nov. 13, 2024) (holding that BIPA Reform Bill applies retroactively); *Ballard v. Freedman Seating Company*, No. 2024 L 004606 (Ill. Cir. Ct. Oct. 2, 2024) (same); *Schwartz v. Supply Network, Inc.*, No. 23 CV 14319, 2024 WL 4871408 (N.D. Ill. Nov. 22, 2024) (holding that BIPA Reform Bill applies prospectively).