Insurance for Cyber-Related Claims: Issues Surrounding Coverage, Disputes, Reinsurance and Arbitration

Frank Lattal, FCIArb, Lattal ADR – Arbitra International

I. Introduction

The cyber insurance and reinsurance market has grown significantly in a relatively short period of time and its importance in commercial programs has matured from a niche product or an "add on" to one of the most critical components of risk management in the global property and casualty sector. The activity has been driven by the escalating frequency and severity of cyberattacks, along with reality of the implications of these events. There are huge potential losses at stake, not just financial, but reputational for sure, not to mention the large legal bills that could be generated after a significant data breach. Not surprisingly, the insurance market is experiencing rapid expansion, with premiums expected to grow from roughly $15 billion in 2024 to nearly $30 billion by 2027.[1]

The P&C industry saw a significant increase in claim volume from 2024 to 2025 with most notifications relating to data breaches.[2] The main drivers of insured losses are Ransomware, Data Breach, Business Email Compromise (BEC) and Distributed Denial of Service (DDoS).[3] Although ransomware attacks accounted for only 16% of notifications, they represented approximately 75% of total insurer payouts.[4]

Legal and coverage questions surrounding cyber insurance have arisen in short order. Coverage triggers, war exclusions, business interruption, ransomware consent-to-pay disputes, regulatory notification costs, aggregation clauses, and follow-the-fortunes obligations in reinsurance are all in a relatively early and general period of development. The absence of precedent—because outstanding legal issues remain unanswered or may have been resolved in

[1]See, Munich Re, Security.org, Cyber Insurance Statistics and Data for 2026, https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2026.html, see also, https://www.security.org/insurance/cyber/statistics/ (projecting the market toward approximately $29 billion by 2027).

[2]See, See NAIC, 2025 Cybersecurity Insurance Report (Nov. 10, 2025), https://content.naic.org/sites/default/files/inline-files/2025_Cybersecurity_Insurance%20Report.pdf. discussing ransomware, BEC, and credential abuse as primary claim drivers).

[3] A Distributed Denial of Service (DDoS) attack is a malicious attempt to crash or slow down a website, server, or network by overwhelming it with a massive flood of internet traffic

[4]See Deep Strike, Cyber Insurance Statistics 2025, https://deepstrike.io/blog/cyber-insurance-statistics-2025

confidential, non-precedential arbitrations—complicates legal development and the ability to analyze possible resolution with reliability.

It has been suggested that Cyber coverage is particularly fit for dispute resolution through arbitration because many of the attributes of the cyber insurance landscape mesh well with all that private commercial arbitration provides.[5] There is no doubt that many coverage disputes will be subject to arbitration clauses, especially when an the insurance program includes policies issued outside of the United States. At present, the world of cyber coverage arbitrations is somewhat opaque because of the general rule of confidentiality in commercial arbitrations and because the claim activity and legal theories are still in a developmental state. That said, there have been a number of cyber-related coverage disputes brought in the court system, mostly in the United States that provide some general guidance on how these disputes may resolve. [6]

Finally, there is a distinct role for reinsurance when it comes to cyber insurance as it provides an opportunity for direct insurers to manage risk exposure by sharing and mitigating large or unpredictable losses. As insurers use more reinsurance to expand their capacity for underwriting coverage the risk of reinsurance disputes grows significantly. The growth of reinsurance disputes in cyber is fueled by both a function of the volume of claims and the novelty of answers to the normal issues that arise between cedents and reinsurer. For cyber these include follow-the-fortunes obligations in ransomware payment scenarios, the war exclusion, aggregation and hours clause disputes in systemic events like CrowdStrike, and OFAC compliance allocation. These are not disputes that scale proportionally with premium volume — they arise from currently unresolved legal questions under existing reinsurance doctrine. These disputes are not theoretical future risks — they are active, and virtually all of them will be resolved through arbitration, as mandatory arbitration clauses are standard in reinsurance treaties across the U.S., London, and Bermuda markets.

II. Cyber Coverage Basics

A. "Silent Cyber"

[5] Andrew Nadolna, Adrienne Publicover & Daniel Garrie, Why Arbitration Clauses May Make Sense in Cyber Insurance Policies, 19 CARDOZO J. CONFLICT RESOL. 43 (2017), https://larc.cardozo.yu.edu/cjcr/vol19/iss1/5.
[6] See Section III.

Before the emergence of stand-alone cyber insurance policies, coverage was pursued through traditional property, general liability, crime, or errors-and-omissions policies. The policies neither clearly included nor clearly excluded cyber perils.[7] This phenomenon came to be known as "silent cyber" or "non-affirmative" cyber. Claiming cyber losses under these policies posed significant risk to both policyholders and insurers, as the absence of any language focused on cyber events cast doubt on the extent to which a policy might have an obligation to respond. Insureds could not reliably rely on that coverage existed and insurers could not reliably price or reserve for the risk.[8]

One development after the emergence of silent cyber coverage was response by regulators. For example, the New York Department of Financial Services issued Insurance Circular Letter No. 2 (2021), directing insurers to evaluate their exposure to silent cyber and to clarify coverage intent throughout their portfolios.[9] That circular observed that silent cyber risk can reside in a variety of combined and stand-alone non-cyber policies and recognized the need for affirmative clarification of coverage intent.[10] Further, in the London market the Prudential Regulation Authority and Lloyd's through Market Bulletins Y5258 and Y5277 required that all first-party property policies either affirmatively grant or affirmatively exclude cover for losses caused by a cyber event, beginning in 2020.[11] Regulatory developments like these along with the legal uncertainty posed by policies that were silent on cyber fueled a continuing migration of property and casualty policies to either a specific grant of cyber coverage grant or an express cyber exclusion, as well as moving systemic cyber exposure toward standalone cyber-specific policies.

B. Standalone Cyber Insurance Policies

A typical stand-alone cyber insurance policy is organized with both first-party and third-party coverage.[12] First-party coverages respond to losses the insured suffers directly as a

[7]See Marsh, Silent Cyber: What It Is and How You Can Cover Cyber Perils (Dec. 5, 2019), https://www.marsh.com/en-gb/services/cyber-risk/expertise/silent-cyber-how-you-can-cover-perils.html.

[8]See Guy Carpenter, Silent Cyber Explained (Nov. 2018), https://www.guycarp.com/insights/2018/11/silent-cyber-explained.html.

[9]See New York Department of Financial Services, Insurance Circular Letter No. 2 (2021): Cyber Insurance Risk Framework (Feb. 4, 2021), https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02.

[10]Id. (noting silent cyber residual exposure across E&O, burglary and theft, general liability, and product liability lines), ee Marsh, "Silent Cyber" Frequently Asked Questions (Nov. 2019), https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/silent-cyber-frequently-asked-questions.pdf.

[11]See Lloyd's Market Bulletins Y5258 and Y5277 (2019–2020); see also DAC Beachcroft, War Exclusions in Cyber Policies: An Overview (2023), https://www.dacbeachcroft.com/en/What-we-think/War-exclusions-in-cyber-policies-an-overview.

[12]See, Christensen Group, Cyber Insurance Coverage Explained (Feb. 23, 2026), https://www.christensengroup.com/article/the-value-of-cyber-insurance.

consequence of a cyber event, while third-party coverages respond to claims asserted against the insured by customers, counterparties, or regulators.[13] Although every insurance policy will differ in wording, structure, terms, and conditions, the dominant commercial product is a policy that includes both categories of coverage, with independent limits, sublimits, retentions, and waiting periods for each coverage grant.[14]

Typical first-party components include incident response and forensic investigation expense, data restoration, business interruption and extra expense for the insured's own operations, cyber extortion (including ransom payment where permitted), notification and credit-monitoring costs, digital asset recovery, and crisis management or public relations expense. Third-party components generally include network security and privacy liability, media liability, regulatory defense costs and insurable fines and penalties, and, increasingly, contractual liability arising from the insured's obligations to customers under data-protection agreements.[15]

A single cyber event may simultaneously trigger a sequence of coverages with different triggers, retentions, and sublimits.[16] A ransomware event, for example, may implicate incident response, extortion, business interruption, data restoration, notification expense, regulatory defense, and ultimately third-party claims brought by customers whose data was exfiltrated — each responding under its own terms and each potentially subject to its own coverage dispute.[17] Coverage for governmental fines and penalties is more limited: some jurisdictions prohibit insurance of punitive or intentional-conduct penalties, leaving insurability of particular regulatory exposures to the governing law of the policy and the nature of the underlying violation.[18]

Cyber policies are distinctive among commercial lines in the extent to which their economics depend on sublimits and time-based conditions rather than a single aggregate limit. It is common for the policy to carry an overall aggregate limit, with materially lower sublimits for extortion, regulatory defense, contingent business interruption, social engineering, reputational

[13]See ProWriters, First-Party vs. Third-Party Cyber Insurance (May 12, 2023), https://prowritersins.com/cyber-insurance-blog/cyber-liability-coverage/.

[14]See Vouch, First Party vs Third Party Cyber Insurance Coverage (2025), https://www.vouch.us/blog/first-party-vs-third-party-cyber-insurance, October 2025.

[16]See Vouch, supra note 9.

[17]See CrowdStrike, Cyber Insurance Explained (Aug. 12, 2025), https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/cyber-insurance/.

[18]See Christensen Group, supra note 7, See The Coyle Group, First Party vs Third Party Cyber Insurance (Feb. 5, 2026), https://thecoylegroup.com/first-party-vs-third-party-cyber-coverages/ (noting some jurisdictions prohibit insurance of punitive or intentional-conduct penalties).

harm, and related coverages.[19] The waiting period — a time-based threshold that must pass before business interruption coverage responds — functions as a time deductible.[20]

III. Cyber Insurance Coverage Issues

Coverage disputes over cyber insurance to date have centered around several recurring questions. It is not uncommon when focused on insured evolving technologies that today's analysis is framed by policy language drafted years before when the technology did not exist or was not understood. As stated earlier, a minimal amount of guidance exists in the way of precedent. To further complicate matters, notable matters have settled before the seminal issue(s) was decided and others have been resolved in confidential arbitration. So, it is not easy to analyze a large body of developing doctrine because none exist. That said, there is some guidance that may portend the future.

A. The War Exclusion

The most prominent coverage issue in the last several years has been the application of the war or "hostile/warlike action" exclusion to cyber events attributed to state or state-sponsored actors.[21] The issue arose most dramatically in *Merck & Co. v. ACE American Insurance Co*., in which Merck sought more than $1.4 billion in coverage under its "all risk" property program for losses caused by the 2017 NotPetya malware attack.[22] Merck's insurers denied coverage, contending that NotPetya constituted a "hostile or warlike action" by a government or sovereign power because U.S. and allied intelligence agencies had publicly attributed the attack to the Russian military.[23]

The New Jersey Superior Court rejected the insurers' position, finding that the exclusion's reference to "hostile or warlike action" had a plain meaning limited to traditional forms of armed

[19]See, Pierson Ferdinand LLP, Business Interruption Claims in Cyber Insurance: Policy Wordings, Misinterpretations, and Best Practices (Mar. 7, 2025), https://pierferd.com/news/business-interruption-claims-in-cyber-insurance, Skyscraper Insurance — "Cyber Policies: Are Your Sublimits Enough?"https://skyscraperinsurance.com/cyber-policies-are-your-sublimits-enough/

[20]See The Coyle Group, Cyber Insurance Waiting Period Explained (Dec. 9, 2025), https://thecoylegroup.com/insurance-by-coverage/cyber-insurance/cyber-insurance-waiting-period/.

[21]See Hunton Andrews Kurth, Boots on the Ground or Hands on a Keyboard: Merck and Insurers Battle Out the War Exclusion, https://www.hunton.com/hunton-insurance-recovery-blog/boots-on-the-ground-or-hands-on-a-keyboard-merck-and-insurers-battle-out-the-war-exclusion.

[22]Merck & Co. v. ACE Am. Ins. Co., No. UNN-L-2682-18 (N.J. Super. Ct. Jan. 13, 2022).

[23]The Record, Merck Wins Cyber-Insurance Lawsuit Related to NotPetya Attack (Jan. 17, 2022), https://therecord.media/merck-wins-cyber-insurance-lawsuit-related-to-notpetya-attack., See Marsh, Asking the Right Questions About War Exclusions in the Context of Cyber Operations (Jan. 2023), https://www.corporate.marsh.com/insights/publications/2023/january/asking-the-right-questions-about-war-exclusions-in-the-context-of-cyber-operations.html.

conflict between nations, and that the exclusion contained no language extending it to a cyber operation affecting a bystander corporation outside any theater of armed conflict.[24] The New Jersey Appellate Division affirmed in May 2023, holding that the insurers had failed to demonstrate the attack to be "hostile" or "warlike" within the meaning of the exclusion, and that the insurers had had every opportunity to draft language extending the exclusion to cyber operations but had not done so.[25] The matter settled in early 2024 on the eve of oral argument before the New Jersey Supreme Court, leaving the Appellate Division decision as the leading appellate authority on this question in the United States.[26] A similar dispute, *Mondelez International v. Zurich American Insurance Co.,* also settled in Illinois leaving the ultimate analysis of cyber "war" also unresolved.[27]

After NonPetya, the insurance industry responded. In August 2022, Lloyd's issued Market Bulletin Y5381 requiring that all stand-alone cyber-attack policies written under the CY and CZ risk codes include an exclusion for state-backed cyber-attacks at inception or renewal from 31 March 2023.[28] The Lloyd's Market Association promulgated four model clauses — LMA5564, LMA5565, LMA5566, and LMA5567 — that provide four tiers of coverage for state-sponsored cyber events.[29] LMA5564 is the strictest, excluding cyber losses caused by "war" or any "cyber operation"; LMA5565 and LMA5566 carve back coverage for cyber operations that are not "retaliatory" and do not have a "major detrimental impact" on a state's security, defense, or essential services; and LMA5567 (the most widely used of the four) additionally covers effects on "bystanding cyber assets" not physically located in an impacted state.[30] Revised "A" and "B" versions of each clause were issued in early 2023, with the "A" versions compliant with Market

[24]See Hunton Andrews Kurth, supra note 24.
[25]Merck & Co. v. ACE Am. Ins. Co., No. A-1879-21 (N.J. Super. Ct. App. Div. May 1, 2023); see K&L Gates, After Important Cyber Insurance Victory for Policyholders, Focus Turns to Insurers' Proposed Changes to War Exclusions (June 13, 2023), https://www.klgates.com/After-Important-Cyber-Insurance-Victory-for-Policyholders-Focus-Turns-to-Insurers-Proposed-Changes-to-War-Exclusions-6-13-2023.
[26]See Insurance Journal, Merck Settles Coverage Dispute With Insurers Over War Exclusion in NotPetya Attack (Jan. 5, 2024), https://www.insurancejournal.com/news/national/2024/01/05/754582.htm.
[27]See Dakota Digital Review, Cybersecurity & Insurance Law: Warlike-Action Exclusion & the Merck (Oct. 22, 2024), https://dda.ndus.edu/ddreview/cybersecurity-insurance-law-warlike-action-exclusion-the-merck/ (noting settlement of Mondelez International v. Zurich American Insurance in 2022).

[28]Lloyd's Market Bulletin Y5381, Cyber-Attack Exclusions (Aug. 16, 2022), https://assets.lloyds.com/media/35926dc8-c885-497b-aed8-6d2f87c1415d/Y5381%20Market%20Bulletin%20-%20Cyber-attack%20exclusions.pdf.

[29]Lloyd's Market Association, Cyber War Clauses, https://lmalloyds.com/specialist-areas/underwriting/wordings/cyber-war-clauses/.

[30]See Online and On Point, Four New Cyber War Exclusions from Lloyd's Market Association (Jan. 10, 2022), https://www.onlineandonpoint.com/2022/01/four-new-cyber-war-exclusions-from-lloyds-market-association/.

Bulletin Y5381 and the "B" versions omitting a contractual attribution mechanism and therefore requiring additional Lloyd's approval to use.[31]

The practical reality for practitioners is that the evolution of war wordings across markets for cyber coverage is a minefield challenge. A large commercial tower may now contain different war exclusions at various attachment points because of the absence of market consensus, a situation that is already generating coverage disputes and will continue to do so.[32] A policyholder may find itself in the position of having to address several different wordings of a "war" exclusion.

B. Business Interruption Trigger and "Direct Physical Loss" Disputes

A second recurring coverage issue concerns the nature of loss that triggers coverage. In *EMOI Services, L.L.C. v. Owners Insurance Co*.,[33] the Ohio Supreme Court unanimously held that a ransomware attack causing encryption of the insured's software did not produce "direct physical loss of or damage to" covered media within the meaning of an electronic equipment endorsement in the insured's businessowners policy. The court concluded that software is intangible and cannot experience direct physical loss or damage, so the endorsement was not triggered even though the insured's systems were inaccessible for a period of time and the insured ultimately paid ransom to recover them.[34] That decision was a strong statement that legacy first-party property language was a poor fit for cyber losses — and it underscores the importance of standalone cyber coverage for risks that fall outside the tangible loss requirement.[35]

Even under dedicated cyber policies, business interruption coverage is a frequent source of dispute.[36] The core issues are the triggering event, the waiting period, the period of restoration, and the method of measuring loss.[37] Whether a waiting period operates as a time retention

[31]See OnlyStrategic, Cyber War & Cyber Operation Clauses Updated by LMA, https://insurance.onlystrategic.com/Articles/featured/id/95298/ (distinguishing A and B versions).

[32]See Insurance Journal, Lloyd's Cyber War Exclusions: Confusing, Disruptive, but Necessary? (May 9, 2023), https://www.insurancejournal.com/news/international/2023/05/09/720020.htm.

[33] 170 Ohio St.3d 78, 2022-Ohio-4649.

[34]See Traub Lieberman, Ohio Supreme Court Finds That Ransomware Attack Did Not Result in Direct Physical Loss to Insured's Software, https://www.traublieberman.com/perspectives/ohio-supreme-court-finds-that-ransomware-attack-did-not-result-in-direct-physical-loss-to-insureds-software and Hinshaw & Culbertson LLP, Ohio Supreme Court Rules No Coverage For Ransomware Attack Under BOP Policy, https://www.hinshawlaw.com/en/insights/insights-for-insurers-alert/ohio-supreme-court-rules-no-coverage-for-ransomware-attack-under-bop-policy-because-computer-software-sustained-no-direct-physical-damage.

[35]See Kennedys Law, Getting Physical: Ohio Supreme Court Holds That Software Cannot Be Physically Damaged (Jan. 9, 2023), https://www.kennedyslaw.com/en/thought-leadership/article/getting-physical-ohio-supreme-court-holds-that-software-cannot-be-physically-damaged-and-endorsement-covering-software-must-be-triggered-by-physical-loss-or-damage-to-covered-property/.

[36]See Pierson Ferdinand LLP, supra note 19.

[37]See The Coyle Group, supra note 20.

(excluding losses incurred during the waiting period) or as a qualifying threshold (triggering coverage from hour one, provided the outage exceeds the waiting period) can have a decisive effect on recovery. Similarly, whether a policy responds only to a "security failure" or also to a broader "system failure" will determine whether non-malicious outages — software bugs, configuration errors, vendor failures — fall within the coverage grant. Contingent business interruption raises its own set of issues, particularly as cloud and vendor outages have emerged as systemic loss drivers.[38]

Recently another court focused on the "direct" requirement for coverage under a cyber policy for social engineering fraud after a phishing attack compromised a CFO's e mail account. In *Office of the Special Deputy Receiver v. Hartford Fire Insurance Company,*[39] a trial court refused to grant a summary judgment motion by the insurer that issued a cyber policy who argued that the loss was not a direct result of a computer crime because the payments were made by the insured's employees not a fraudulent actor. The court said the language in that Policy was "at most" ambiguous as to whether the insured had alleged a Computer Crime that directly caused Computer Fraud and that the payments were a direct response to the fraudulent e mails and therefore the computer crime could have directly caused the loss. This case settled on appeal but indicates that a court may look favorably on the allegation that action in respond to fraudulent e mails may be sufficient to meet the computer fraud trigger.[40]

C. Ransomware, Consent-to-Pay and the Shadow of Sanctions Law

A third category of dispute arises at the intersection of ransomware extortion, policy conditions, and sanctions law. Most cyber policies require that the insured notify the insurer promptly of a ransomware incident and obtain the insurer's consent before paying a ransom demand.[41] When a policyholder acts unilaterally — paying quickly to avoid operational catastrophe — the insurer may assert that the payment was "voluntary" rather than the result of an

[38]See Corvus Insurance, https://www.corvusinsurance.com/blog/cyber-coverage-explained-contingent-business-interruption-cyber.
[39] 2025 U.S. Dist. LEXIS 60484, 2025 LX 141418, 2025 WL 965093

[40] There are some cases that might suggest the opposite. *Apache Corp. v. Great American Ins. Co.*, 662 F. App'x 252 (5th Cir. 2016) (A loss resulting from a fraudulent e-mail did not trigger coverage under a crime policy's "computer fraud" coverage because the loss was not the "direct result" of computer use. The court held the email "was merely incidental to the occurrence of the authorized transfer of money"), Pestmaster *Services, Inc. v. Travelers Cas. & Sur. Co. of Am.*, 656 F. App'x 332 (9th Cir. 2016) ("Computer Fraud" occurs when someone "hacks" or obtains unauthorized access or entry to a computer to make an unauthorized transfer or otherwise uses a computer to fraudulently cause a transfer of funds — authorized transfers procured by deception don't qualify).
[41]See NAIC, Ransomware (Dec. 19, 2025), https://content.naic.org/insurance-topics/ransomware.

insured event, or that the insured breached cooperation or consent conditions.[42] In *G&G Oil Co. of Indiana, Inc. v. Continental Western Insurance Co.*, the Indiana Supreme Court declined to accept the insurer's position that a ransomware payment is categorically a "voluntary" transfer outside the coverage of a crime policy's computer fraud grant, holding instead that coverage depends on the factual nature of the extortion.[43]

Another dimension in this area is the increasing restriction on ransom payments imposed by sanctions and anti-money-laundering regimes.[44] The U.S. Treasury Department's Office of Foreign Assets Control (OFAC) has made clear that facilitating a ransom payment to a sanctioned entity — even inadvertently — can give rise to civil liability regardless of the payer's knowledge.[45] Insurers have responded by imposing screening conditions, requiring the use of approved negotiators, and, in some cases, excluding coverage entirely for ransom payments made to sanctioned parties or without required screening.[46] For the policyholder in extremis, an imprudent communication with a threat actor — for example, sharing the policy to obtain a demand within policy limits — can jeopardize coverage by undermining the cooperation obligation and raising the specter of collusion.[47]

D. Miscellaneous Cyber Decisions in 2026

There have been new cyber-related cases resolved in 2026.[48] First, in *Perry & Perry Builders, Inc. v. Cowbell Cyber and Obsidian Specialty Ins. Co*[49]., the court enforced a Cyber Crime Loss sublimit. In that case the policyholder was deceived into transferring money intended for a vendor to an unintended third party. The actual payments were wired in 2 transfers, and the policyholder argued it was entitled to 2 sublimits. This argument was

[42]See Security Boulevard, So You Think You Have Cyber Insurance? (Feb. 24, 2026), https://securityboulevard.com/2026/02/so-you-think-you-have-cyber-insurance-the-breach-is-only-the-first-incident-the-claim-is-the-second/ and See Hylant, Cyber Insurance, Ransomware and What Happens When You Can't Pay (May 15, 2025), https://hylant.com/insights/blog/cyber-insurance-ransomware-attacks-and-what-happens-when-you-legally-cant-pay.

[43]G&G Oil Co. of Indiana, Inc. v. Cont'l W. Ins. Co., 165 N.E.3d 82 (Ind. 2021).

[44]See Kaufman Dolowich, Ransomware Payments and Insurance Coverage, PIA Magazine (Feb. 2020), https://www.kaufmandolowich.com/wp-content/uploads/2020/02/PIAmagazine-February2020-Ransomware-Payments-and-Insurance-Coverage.pdf.

[45]U.S. Dep't of the Treasury, OFAC, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (Sept. 21, 2021).

[46]See Crestview Public Adjusters, How Cyber Insurance Claims Work for Ransomware Attacks (May 4, 2025), https://crestviewpa.com/how-cyber-insurance-claims-work-for-ransomware-attacks/.

[47]See Policyholder Pulse, The Dangers of Dialogue: Ransomware Attackers Want to See Your Cyber Insurance Policy (Mar. 27, 2023), https://www.policyholderpulse.com/ransomware-hardbit-cyber-insurance-policy/.

[48] See, https://www.whiteandwilliams.com/resources-news-White-and-Williams-LLP-Secures-Trio-of-Cyber-Coverage-Wins

[49] 2026 U.S. Dist. LEXIS 49409 (E.D. Tex. Mar. 9, 2026).

rejected and the court determined that the policy language clearly established one sublimit applied to all the insured's cybercrime losses during the policy period.

In *Gore, Kilpatrick & Dambrino, PLLC v. Spinnaker Ins. Co*[50]., a fraudster used a false identity to engage a policyholder law firm to assist in a debt recovery. The fraudster advised the firm that the debtor had agreed to pay the debt, and soon thereafter the policyholder received correspondence and a check. Unbeknownst to the firm, both the letter and check came from the fraudster who subsequently requested that the insured deduct its attorney's fees from the check and wire the remaining balance to him. The firm wired more than $158,000, but the check was later returned unpaid, revealing the transaction to be fraudulent.

The firm sought coverage under the Social Engineering Coverage Endorsement of its cyber policy which provided coverage where an insured is intentionally misled by an instruction transmitted via e-mail. The insurer denied the claim based on the position that the provision applied only where a fraudulent instruction purports to come from an existing client or business relationship, and no such relationship existed in the transaction and that the policy did not cover an entirely fictional transaction. The court agreed. It determined that the real entity that the fraudster purported to be was not a person who exchanged or was under contract to exchange goods or services with the insured for a fee and that the instruction to transfer money could not have been sent by an imposter purporting to be a client if the individual giving the instruction was the client. There was no coverage under the endorsement and therefore plaintiff's complaint failed to state a claim.

E. Application Misrepresentation and Rescission

An increasingly prominent basis for coverage dispute is alleged misrepresentation in the cyber insurance application. *In Travelers Property Casualty Co. of America v. International Control Services, Inc.,*[51] Travelers sought rescission of a cyber policy on the ground that the insured had represented in its application that multifactor authentication (MFA) was deployed across its environment when, in fact, MFA had not been enabled on the server through which threat actors gained entry.[52] Rather than denying the claim and defending a coverage action, Travelers

[50] 2026 U.S. Dist. LEXIS 69567 (N.D. Miss. Mar. 31, 2026).
[51] Travelers Prop. Cas. Co. of Am. v. Int'l Control Servs., Inc., No. 22-cv-2145 (C.D. Ill. filed July 6, 2022).
[52] See Reed Smith LLP, Insurance Applications Under Scrutiny: Lessons from Travelers v. ICS (July 21, 2022), https://www.reedsmith.com/en/perspectives/2022/07/insurance-applications-under-scrutiny-lessons-from-travelers-v-ics.

affirmatively sued to declare the policy *void ab initio*. The parties ultimately stipulated to rescission and dismissal with prejudice.[53]

The *Travelers* case has been influential well beyond its litigation posture. It signaled that cyber insurers are prepared to test application-based defenses aggressively, that sophisticated underwriting questionnaires — focused on specific security controls such as MFA, EDR, backup architecture, and patching cadence — will be treated as material representations, and that a policyholder's inaccurate or incomplete response may result not merely in a claim denial but in an attempt to rescind coverage.[54] Insurers have also asserted contract and subrogation theories against vendors whose security lapses contributed to widespread breaches affecting their insureds, as illustrated by the ongoing litigation arising out of the 2020 Blackbaud ransomware attack.[55]

F. Regulatory Notification Costs and the SEC Disclosure Regime

Another category of coverage inquiry concerns the scope of coverage for regulatory notification, investigation, and compliance costs — an area that has expanded dramatically in parallel with the proliferation of breach-notification statutes and the 2023 SEC cybersecurity disclosure rule.[56] New Regulation S-K Item 106 requires public registrants to describe their cybersecurity risk management, strategy, and governance in annual reports, and new Item 1.05 of Form 8-K requires disclosure of a material cybersecurity incident within four business days of the registrant's materiality determination.[57] These requirements create significant contemporaneous costs for incident-response counsel, disclosure counsel, forensic support, and SEC communications that are distinct from the third-party claims that traditionally defined regulatory defense coverage.[58] The interplay with parallel obligations under the European Union's General

[53]See Insurance Journal, Travelers, Policyholder Agree to Void Current Cyber Policy (Aug. 30, 2022), https://www.insurancejournal.com/news/national/2022/08/30/682564.htm, See Lockton, Travelers v. ICS Underscores Need to Respond Carefully to Cyber Insurance Application Questions (Sept. 15, 2022), https://global.lockton.com/us/en/news-insights/travelers-v-ics-underscores-need-to-respond-carefully-to-cyber-insurance-application-questions.

[54]See National Law Review, Practical Implications of Travelers v. ICS for Cyber Insurance Brokers, Carriers and Policyholders (Feb. 8, 2023), https://natlawreview.com/article/practical-implications-travelers-v-ics-cyber-insurance-brokers-carriers-and.

[55]See Risk & Insurance, Court Allows Insurers' Contract Claims to Proceed in Cybersecurity Dispute (2026), https://riskandinsurance.com/court-allows-insurers-contract-claims-to-proceed-in-cybersecurity-dispute/.

[56]SEC, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11216 (July 26, 2023), https://www.sec.gov/newsroom/press-releases/2023-139.

[57]17 C.F.R. § 229.106; see Gibson Dunn, SEC Adopts New Rules on Cybersecurity Disclosure for Public Companies, https://www.gibsondunn.com/sec-adopts-new-rules-on-cybersecurity-disclosure-for-public-companies/, SEC Form 8-K, Item 1.05; see Hunton Andrews Kurth, An Update on SEC Cybersecurity Reporting (Dec. 5, 2024), https://www.hunton.com/privacy-and-information-security-law/an-update-on-sec-cybersecurity-reporting.

[58]See PwC, SEC's Cyber Disclosure Rule, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/sec-final-cybersecurity-disclosure-rules.html.

Data Protection Regulation — which imposes a 72-hour breach-notification obligation on data controllers — further complicates coverage analysis for multinational insureds.[59]

IV. **Reinsurance**

Reinsurance disputes in cyber have lagged their primary-insurance counterparts, but the shape of the emerging issues is already clear. They fall into at least two broad categories, the aggregation question and follow-the-fortunes, driven by the uneasy interaction between systemic cyber risk and traditional reinsurance structures.

A. Aggregation, Loss Occurrence, and the Hours Clause Problem

Most property excess-of-loss and catastrophe reinsurance contracts contain aggregation provisions keyed to the concept of a single "loss occurrence" or "event," typically defined as the sum of all individual losses arising out of one disaster, accident, or series of related losses.[60] Many contracts also contain an "hours clause" limiting aggregation to losses occurring within a defined window — commonly 72 or 168 hours, though windows may be longer for specific perils — and allowing the reinsured to select the starting point for that window in order to maximize aggregation.[61] Aggregation clauses serve a parallel function, with courts recognizing at least three approaches — causation, effect, and liability-trigger — to the question of whether a collection of individual losses constitutes one occurrence.[62]

Cyber events may not clearly fit into structures built primarily for natural catastrophes or severity losses. A state-sponsored supply-chain attack, a ransomware campaign by a single threat actor group, a cloud service outage, or a mass exploitation of a single software vulnerability can generate tens of thousands of individual losses distributed across jurisdictions and industries, over time periods of days, weeks, or months.[63] Whether a multi-week ransomware spree by one affiliate group, or a cascade of losses across dozens of cloud customers, should be aggregated as "one event" could be an open question depending on the policy language and facts involved.

---

[59]See Regulation (EU) 2016/679 (General Data Protection Regulation) art. 33 (72-hour breach notification).

[60]See DLA Piper, Reinsurance Implications of the Supreme Court's Judgment in the FCA Business Interruption Test Case (Jan. 2021), https://www.dlapiper.com/en/insights/publications/2021/01/reinsurance-implications-supreme-court-judgment.

[61]See IRMI, COVID-19 Losses and Reinsurance Aggregation (Aug. 28, 2020), https://www.irmi.com/articles/expert-commentary/covid-19-losses-and-reinsurance-aggregation, See DAC Beachcroft, Landmark Commercial Court Decision on COVID-19 BI Loss Aggregation, https://www.dacbeachcroft.com/en/What-we-think/Landmark-Commercial-Court-decision-on-COVID19-BI-loss-aggregation.

[62]See IRMI, supra note 58.

[63]See DLA Piper, supra note 57 (noting that hours clauses typically permit aggregation within specified periods of 72 or 168 hours).

B. Follow-the-Fortunes - Follow-the-Settlements

The reinsurer's contractual obligation to follow the fortunes (or, more narrowly, the settlements) of the cedent is a bedrock principle of reinsurance law.[64] The doctrine precludes a reinsurer from relitigating the cedent's good-faith claim-handling and settlement decisions, subject to traditional exceptions for fraud, collusion, bad faith, and losses plainly outside the scope of the underlying coverage. Courts have extended the doctrine to allocation decisions as well, so long as the allocation is objectively reasonable.[65]

Recent appellate decisions have clarified the doctrine's limits. In *Public Risk Management of Florida v. Munich Reinsurance America, Inc.,*[66] the Eleventh Circuit held that courts will not imply a follow-the-fortunes obligation where the reinsurance agreement's plain and unambiguous terms are inconsistent with the doctrine.[67] For cyber, these limits are consequential. A cedent that pays a large ransomware business-interruption loss under a broad reading of its policy's "system failure" trigger, or that pays a NotPetya-style loss notwithstanding a war exclusion, should expect that reinsurers — particularly if the reinsurance treaty contains tighter exclusionary language or a narrower trigger — will probe both the coverage decision and the allocation to the treaty. Alignment of coverage language up and down the tower is thus an increasingly critical drafting exercise, and one that becomes more difficult as LMA and U.S. market wordings diverge in their treatment of state-backed cyber events.

V. Arbitration Issues

It has frequently been observed that cyber disputes are particularly well suited to arbitration and mediation.[68] Why? First, cyber claims often involve private and confidential information about the policyholder, its customers, networks, and strategies. Often proprietary investigation work product and privileged communications are involved. These disputes involve novel contract language that many participants would prefer to develop privately rather than in the reported public

[64]See IRMI, Understanding Reinsurance Terminology – Follow-the-Fortunes (Oct. 2001), https://www.irmi.com/articles/expert-commentary/understanding-reinsurance-terminology-follow-the-fortunes.

[65]Allstate Ins. Co. v. Am. Home Assur. Corp., 837 N.Y.S.2d 138, 43 A.D.3d 113 (N.Y. App. Div. 1st Dep't 2007),

[66]Pub. Risk Mgmt. of Fla. v. Munich Reinsurance Am., Inc., 38 F.4th 1298 (11th Cir. 2022).

[67]See, Shiffer on Reinsurance, https://schifferlc.com/2022/07/21/follow-the-fortunes-rejected-by-11th-circuit/

[68]See Daniel Garrie, Howard Miller & Yoav Griver, Arbitration, Mediation Can Solve Cyber Insurance Disputes, Law360 (Oct. 5, 2018), https://www.law360.com/articles/1088827/arbitration-mediation-can-solve-cyber-insurance-disputes, Andrew Nadolna, Adrienne Publicover & Daniel Garrie, Why Arbitration Clauses May Make Sense in Cyber Insurance Policies, 19 CARDOZO J. CONFLICT RESOL. 43 (2017), https://larc.cardozo.yu.edu/cjcr/vol19/iss1/5.

decisions.[69] Also, as discussed above, they often involve parties in multiple jurisdictions, including London, Bermuda, and continental Europe, for whom a neutral and enforceable forum is essential.

A. Arbitration in the United States

A recurring obstacle to arbitration of U.S. insurance disputes is the patchwork of state laws that, in express terms, prohibit or limit the enforceability of some arbitration clauses in insurance contracts. States including Louisiana, Kentucky, Washington, Missouri, together with the McCarran-Ferguson Act[70] (which reverse-preempts federal law to the extent it would invalidate, impair, or supersede state laws regulating the business of insurance) favor this trend. The federal policy favoring arbitration is reflected in the Federal Arbitration Act and, for international arbitration, in the New York Convention.[71] A circuit split has persisted for decades on the question whether the New York Convention is self-executing and therefore preempts state anti-arbitration laws under the Supremacy Clause despite the McCarran-Ferguson Act.[72]

In 2025, the Second Circuit joined the Fifth and Ninth Circuits in holding that the New York Convention, as implemented by Chapter 2 of the Federal Arbitration Act, preempts state insurance laws that would otherwise invalidate arbitration clauses in contracts subject to the Convention.[73] The Second Circuit decision is particularly significant because of New York's centrality to the U.S. insurance and reinsurance market and to international arbitration more broadly.[74] The decision reinforces the presumptive validity of international arbitration agreements under Article II of the New York Convention, and leaves a narrower — though still significant —

[69]See American Arbitration Association, B2B Cyber Breaches: How an Arbitration Clause Can Help, https://go.adr.org/B2B-Cyber-Breaches.html.

[70]McCarran-Ferguson Act, 15 U.S.C. §§ 1011–1015.

[71]Convention on the Recognition and Enforcement of Foreign Arbitral Awards, June 10, 1958, 21 U.S.T. 2517, 330 U.N.T.S. 38 [hereinafter New York Convention]; Federal Arbitration Act, 9 U.S.C. §§ 201–208 (implementing legislation).

[72]See Stephens v. Am. Int'l Ins. Co., 66 F.3d 41 (2d Cir. 1995); see Foley & Lardner LLP, S.D.N.Y. Finds Arbitration Clause in Insurance Contract Unenforceable, Following Second Circuit Precedent (2023), https://www.foley.com/insights/publications/2023/11/sdny-arbitration-clause-insurance-contract/.

[73]See Certain Underwriters at Lloyd's, London v. 3131 Veterans Blvd LLC, No. 23-1452 (2d Cir. 2025); see Debevoise & Plimpton LLP, Second Circuit Joins Other Circuits in Finding Insurance Arbitration Agreements Enforceable Under New York Convention (May 2025), https://www.debevoise.com/insights/publications/2025/05/second-circuit-joins-other-circuits-in-finding-in.

[74]See Faegre Drinker Biddle & Reath LLP, The Second Circuit Held That the New York Convention Preempts State Anti-Arbitration Insurance Laws (May 23, 2025), https://www.faegredrinker.com/en/insights/publications/2025/5/the-second-circuit-held-that-the-new-york-convention-preempts-state-anti-arbitration-insurance-laws.

set of domestic-only insurance disputes in which McCarran-Ferguson reverse-preemption may continue to operate.

C. International Arbitration: Bermuda Form, English Law, and the Seat of Arbitration

A practitioner advising on a substantial cyber program must consider the practical reality that excess insurance layers are routinely placed in outside the United States in London, Bermuda, Continental Europe, and Asia, and that the dispute resolution clause of those layers could be fundamentally different from that of the domestic U.S. primary market. A possible example is the Bermuda Form excess liability policy, which provides that disputes be resolved by arbitration in London (and, in some iterations, Bermuda), that the English Arbitration Act 1996 (or, in Bermuda-seated cases, the Bermuda International Conciliation and Arbitration Act 1993) governs the arbitral procedure, and that the substantive law of the contract is a modified form of New York law.

The rationale for this hybrid approach is well documented. At the inception of the Bermuda Form, the drafters believed New York substantive law was a reasonable choice because it was comparatively predictable and while in some respects insurer-friendly, was acceptable to the general policyholder community. At the same time, the drafters preferred London or Bermuda arbitration procedure based on the chance of expert tribunals, narrow scope for judicial review, and reduced exposure to U.S. discovery and jury awards. The practical result is that a Bermuda Form arbitration may require counsel to "operate" simultaneously in three legal jurisdictions to address the substantive insurance law, the procedure, and the common law.[75]

Several features of the Bermuda Form are worth highlighting in a cyber context. First, the English courts have been robust in policing the primacy of the seat: in *C v D*, the Court of Appeal upheld an anti-suit injunction preventing a U.S. collateral challenge to a London-seated Bermuda Form award, holding that by choosing London as the seat the parties had agreed that challenges to the award would be governed exclusively by English law.[76] The case is a strong statement when confronted with an attempt to create parallel proceedings in U.S. courts. Second, the U.K. Supreme Court's decision in *Enka Insaat ve Sanayi AS v OOO Insurance Company Chubb*[77]

[75] An excellent overall review of arbitration under the Bermuda Form was published by John Fellas in 2020. See, https://fellasarbitration.com/wp-content/uploads/2020/02/International-Arbitration-Under-The-Bermuda-Form.pdf

[76] C v D [2007] EWCA Civ 1282, Lexology, Bermuda Form: The Court of Appeal Upholds an Anti-Suit Injunction (Dec. 26, 2007), https://www.lexology.com/library/detail.aspx?g=13f023d9-7a9d-49fa-89e8-f728fc9c335b.

[77] Enka Insaat ve Sanayi AS v OOO "Insurance Company Chubb" [2020] UKSC 38

established that where a contract lacks an express choice of law for arbitration, the governing law of the main contract generally applies to the arbitration agreement. The Supreme Court ruled that in the absence of a chosen law, the arbitration agreement is governed by the law with which it has the closest connection, usually the seat of arbitration. Finally, the ruling affirmed that English courts could grant anti-suit injunctions to restrain foreign proceedings brought in breach of an agreement to arbitrate in London. The consequences for Bermuda Form disputes were significant enough to prompt refinement of arbitration clauses and, in the United Kingdom, the codification of a default rule in the Arbitration Act 2025 that the law of the seat governs the arbitration agreement absent express choice.[78] Third, the Bermuda courts, applying a well-established body of authority, will grant anti-suit injunctions to restrain parties from breaching arbitration agreements, as illustrated by *Allied World Assurance Co. Ltd v Bloomin' Brands, Inc.*[79] And finally, U.S. courts enforcing arbitration agreements under the New York Convention have ordered parties to arbitrate their Bermuda Form disputes in the designated seat even in the face of bankruptcy and jurisdictional complications, as in *MF Global Holdings Ltd. v. Allied World Assurance Co. Ltd*.[80]

Beyond the Bermuda Form, reinsurance treaties placed in the international market may call for the rules of a major international institution — London Court of International Arbitration (LCIA) or the International Chamber of Commerce (ICC), the Singapore International Arbitration Centre (SIAC), or the Hong Kong International Arbitration Centre (HKIAC). The 2025 International Arbitration Survey conducted by Queen Mary University of London and White & Case identifies the ICC, HKIAC, SIAC, LCIA, and UNCITRAL rules as the five most preferred sets of rules among international users, with selection driven principally by familiarity, institutional support, and the enforceability of awards under the New York Convention.[81][82] Recent amendments to the LCIA Rules have incorporated formal cybersecurity provisions and have confirmed tribunals' authority to dismiss claims that are manifestly without merit, both of which

---

[79]Allied World Assurance Co. Ltd v Bloomin' Brands, Inc. [2021] Bda LR 17 (SC)

[80]MF Global Holdings Ltd. v. Allied World Assurance Co. Ltd., 571 B.R. 80 (Bankr. S.D.N.Y. 2017); see Hunton Andrews Kurth, Bermuda Form Insurance Arbitration Series: Case Law Involving the Bermuda Form, https://www.hunton.com/hunton-insurance-recovery-blog/bermuda-form-insurance-arbitration-series-case-law-involving-the-bermuda-form.

[81]See White & Case, https://www.whitecase.com/insight-our-thinking/2025-international-arbitration-survey-experiences-preferences-enforcement.

[82]See Aceris Law, Comparing Model Arbitration Clauses: ICC vs. LCIA vs. SIAC (Nov. 22, 2025), https://www.acerislaw.com/comparing-model-arbitration-clauses-icc-vs-lcia-vs-siac/.

have practical significance for the cyber disputes these tribunals are increasingly being asked to hear.[83]

VI. Drafting the Arbitration Clause

The foregoing observations translate into a checklist of drafting considerations for cyber coverage and reinsurance arbitration clauses, if given the opportunity to do so. Counsel should give focused attention to the seat of arbitration, the institutional or *ad hoc* rules (with their implications for case management, cybersecurity, and interim measures), the method of arbitrator selection and the required qualifications, the governing law of the contract and the separate law of the arbitration agreement, the scope of confidentiality (both of the proceedings and of the award), the allocation of costs, and, if possible, the treatment of consolidated proceedings in a tower with multiple insurers. For U.S.-placed cyber programs with international reinsurance protection, clauses should also be drafted to avoid misalignment between the primary layer's dispute resolution regime and the reinsurance treaty's regime, if possible, which can create protracted and expensive sequencing of dispute resolution.

VII. Conclusion

Cyber insurance has matured over the last 20+ years from a niche specialty to an indispensable element of global risk management. The legal doctrines and guidance that govern coverage determinations are developing in real time simultaneously with the development of new technologies. War exclusions, business interruption triggers, ransomware consent-to-pay disputes, regulatory notification costs, aggregation, and follow-the-fortunes obligations are each the subject of active doctrinal development — some of which is taking place in confidential arbitration rather than in the published decisions. The resulting shortage of binding precedent, combined with the international character of large cyber programs, has made arbitration — both domestic and international — an attractive forum for cyber coverage disputes. For practitioners, the challenge is to draft, place, and defend cyber programs with a clear understanding of both the coverage architecture and the dispute-resolution architecture. As cyber losses continue to grow in scale and

[83] See Troutman Pepper Locke, International Arbitration Experts Discuss the New LCIA Rules (May 14, 2025), https://www.troutman.com/wp-content/uploads/2026/03/ARB032426cm.pdf?1774887687

sophistication, these subjects will only become more central to the work of the insurance, reinsurance and arbitration bar.