A MATTER OF INTERPRETATION

AS CYBER POLICIES FACE THEIR FIRST REAL DAYS IN COURT, INSURERS REACT TO THE PRECEDENTS SET

BY RICHARD SHERIDAN

For the uninitiated, cyber insurance policies provide insureds first-party coverage for breach-response costs such as legal services, forensics, notification, and public relations. The policies also can provide coverage for income loss and extra expenses as the result of a business interruption arising from a cyber-related event. Additionally, cyber policies provide third-party coverage for claims that insureds may face resulting from cyber events. These claims may be lawsuits, regulatory proceedings, or arising from Payment Card Industry (PCI) assessments.

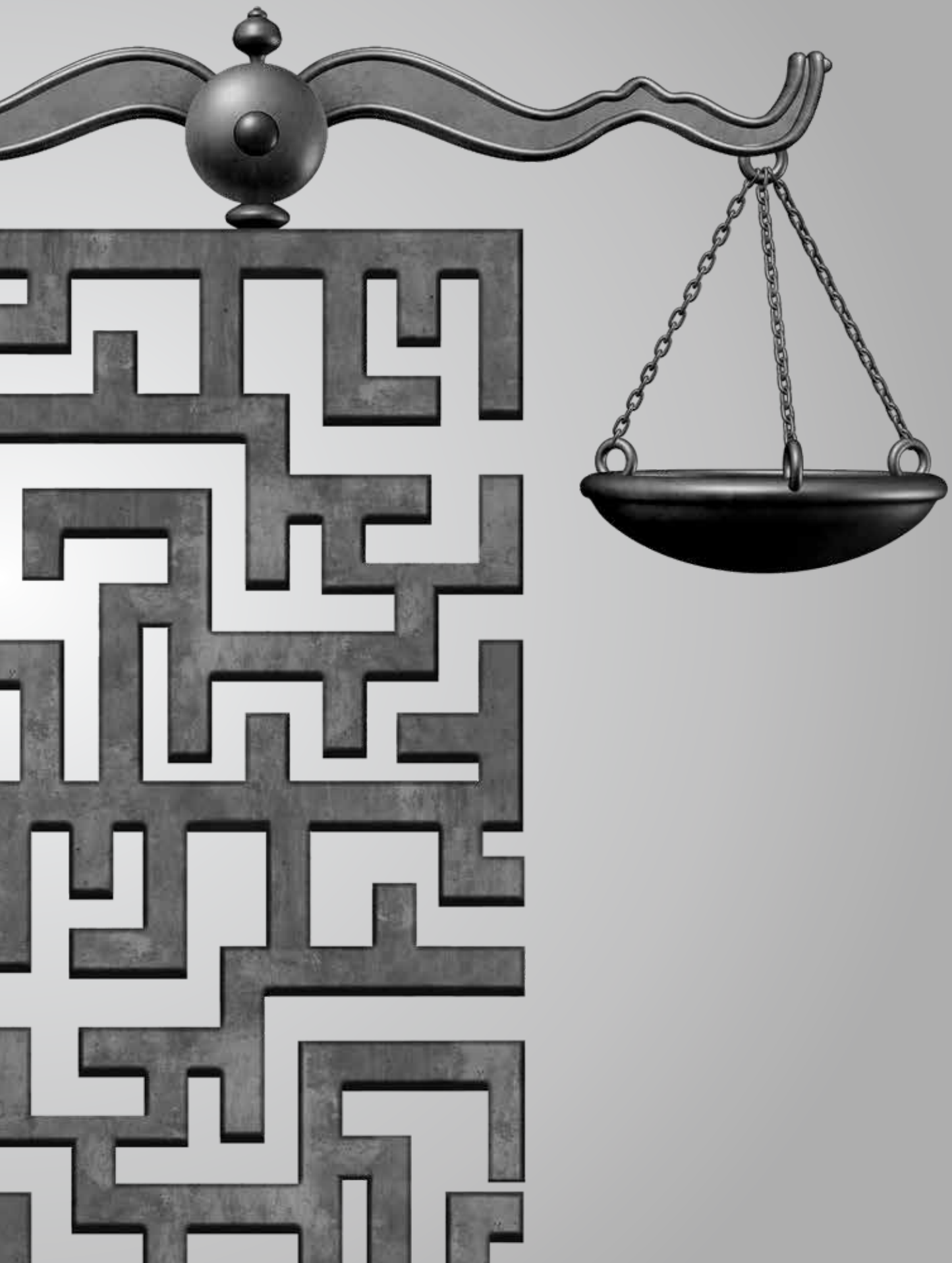
Courts have not yet had much opportunity to interpret cyber insurance products. There are several reasons for this. First, cyber policies are a fairly new product, and they have not been around long enough for many disputes to arise. Also, during the time these policies have existed, the coverage has evolved rapidly as the risks have changed, so there has been little incentive for carriers to seek precedents on policy provisions that may no longer be applicable.

For instance, a cyber carrier that denies coverage for a social engineering claim where one of an insured's employees is duped by an email into making a fraudulent payment—something that just five years ago was generally not covered under a cyber policy—would not be concerned about the precedential value of resolving that claim because cyber policies affirmatively offer coverage for those types of events. Additionally, the cyber insurance marketplace is very competitive, so carriers trying to gain market share in this industry may be reluctant to have the negative publicity that a litigated coverage dispute might garner.

FEE COVERAGE

Notwithstanding the above, there have been some litigated coverage disputes arising from cyber policies. In *P. F. Chang's China Bistro Incorporated v. Federal Insurance Company*, Federal (a subsidiary of Chubb) sold a cybersecurity policy to Chang's parent company, Wok Holdco LLC, with a policy period between Jan. 1, 2014 and Jan. 1, 2015. The policy was marketed by Chubb as one that would cover "direct loss, legal liability, and consequential loss resulting from cybersecurity breaches." On June 10, 2014, Chang's learned that hackers had obtained and posted approximately 60,000 customer credit card numbers on the internet.

Chang's notified Chubb the same day, and Chubb reimbursed Chang's $1.7 million in costs incurred to respond to the breach. In March 2015, Mastercard issued a fraud recovery assessment of $1.7 million, an operational reimbursement assessment of $163,000, and a case management



fee of $50,000 to Chang's credit card processor, Bank of America Merchant Services (BAMS), to cover the costs associated with fraudulent charges and the reissuance of cards. BAMS demanded that Chang's pay these amounts pursuant to Chang's contract with BAMS, and Chang's sought coverage from Chubb. Chang's reimbursed BAMS for the assessments from Mastercard and Chubb denied coverage, resulting in a lawsuit filed by Chang's.

The crux of the Arizona Federal District Court's decision in upholding Chubb's denial of coverage was that the policy excluded coverage for any loss "based upon, arising from, or in consequence of any…liability assumed by any insured under any contract or agreement," and for "any costs or expenses incurred to perform any obligation assumed by, on behalf of, or with the consent of any insured." In holding that these exclusions were applicable, the court noted that there was nothing in the record to indicate that Chang's would have been liable for the assessments absent its contract with BAMS.

In *Spec's Family Partners Ltd. v. The Hanover Insurance Co.*, the U.S. District Court for the Southern District of Texas found no coverage for about $9.5 million in PCI costs assessed under a merchant services agreement, citing a similar contract exclusion, albeit under a directors and officers policy. While this matter was reversed on appeal by the 5th Circuit Court of Appeals, the court did not find the exclusion inapplicable, but rather held that non-contractual claims had also been asserted.

New Hotel Monteleone LLC v. Certain Underwriters at Lloyd's of London et al. involves another litigated coverage matter under a cyber policy concerning coverage for PCI-related losses. In October 2014, the hotel suffered a security breach in which the payment cards of its customers were compromised, and its payment card processor demanded that the hotel reimburse it for the costs of fraudulent charges, replacement of cards, investigation costs, and costs in connection with the alleged violations of the PCI Data Security Standards (PCI DSS).

The hotel had purchased a CyberPro insurance policy from Ascent Underwriting, a managing general agent on behalf of Lloyd's, which contained an aggregate limit of liability of $3 million but a $200,000 sublimit of liability for "PCI fines and penalties," which were defined as "a written demand received by [the policyholder] by a credit card association for a monetary fine or penalty because of [the policyholder's] non-compliance with PCI DSS." When the hotel sought coverage under the policy for the items demanded by its payment card processor, Ascent took the position that those costs were subject to the $200,000 sublimit. The hotel sued, arguing that only the costs for the violation of PCI DSS should be subject to this sublimit, and only if those costs were subject to a written demand from a credit card association. A decision was not rendered in this matter, however, as the parties agreed to refer it to alternative dispute resolution.

Generally speaking, the specific issues that arose in *P.F. Chang's* and *New Hotel Monteleone* over coverage for PCI-related costs should not occur under cyber policies issued today. Following the *P.F. Chang's* case, most insurers that now offer the option to cover PCI exposure will carve back the exclusions for breach of contract or liability assumed under contract so that the exclusions don't apply to PCI-related costs. Cyber policies also now specifically delineate what PCI-related costs are covered, and are (or should be) clear as to whether they cover fines, fraud recovery charges, card reissuance costs, and any other PCI-related fees or costs. With the additional clarity that has developed in the market concerning PCI-related coverage over the last few years, it now seems unlikely that future disputes will arise over this type of coverage.

OTHER COVERAGE MATTERS

Another litigated coverage dispute involving a cyber policy occurred in *Columbia Casualty (CNA) v. Cottage Health System*. Cottage suffered a data breach in the fall of 2013 involving about 32,500 confidential medical records. A class-action lawsuit was filed against Cottage arising from this incident, and CNA agreed to fund a $4.1 million settlement under a complete reservation of rights.

CNA then filed a complaint seeking a declaration that it was not obligated to provide Cottage with a defense or indemnification and reimbursement for all expenses it had paid under the policy arising from the matter. In its complaint, CNA cited an exclusion for "failure to follow minimum required practices," which excluded claims arising out of the failure to continuously implement security procedures identified in the policy's application, and also cited the application itself as well as the conditions section of the policy. CNA referenced several questions in the application regarding Cottage's "risk control self-assessment," which Cottage answered affirmatively. The questions concerned the security controls that Cottage maintained, such as whether Cottage regularly checked for security patches to its systems, replaced factory settings, and performed due diligence and audited third parties it entrusted with sensitive data. Since the breach was the result of anonymous users being able to access personal health information from Cottage's servers (via a Google search), CNA argued that the exclusion applied because the breach would not have occurred had Cottage implemented the procedures and risk controls that it represented it did in the application. CNA's complaint was initially dismissed because it had failed to follow the policy's alternative dispute resolution provisions, but was refiled in California's courts. That lawsuit remains pending.

This dispute seems specific to cyber insurance because of the exclusion for "failure to follow minimum required practices." While this may have been an exclusion that many cyber policies contained at the time of this breach in 2013, most cyber policies do not have such an exclusion today. Instead,

insurers now might have to rely upon the policy conditions to seek to avoid coverage or rescind the policy based upon misrepresentations made by an insured in the policy application. This puts cyber insurers in the same shoes as other types of insurers seeking representations about risk management and loss control. For example, without this exclusion, this dispute is similar to one in which a property insurer seeks to avoid covering a warehouse fire based upon an insured's misrepresentation that it had fire prevention controls in place. So, in effect, this is really not an issue that would be specific to cyber insurance policies.

Another litigated coverage matter concerning a cyber policy is *Travelers Property Casualty Co. v. Federal Recovery Services Inc.*, filed in Utah Federal District Court in 2016. In that matter, Federal was sued by its client, Global Fitness, in a dispute where Federal allegedly intentionally refused to return bank account and credit card data to Global. That matter, however, was under an errors and omissions insuring agreement of the Travelers' policy—an insuring agreement that many cyber policies do not have—and was based upon the court finding that Federal's conduct was intentional and did not constitute an "error, omission, or negligent act," which was required to trigger the insuring agreement. Once again, although this case involved a cyber insurance policy, this matter did not really concern a cyber insurance issue.

THE REACTIONS

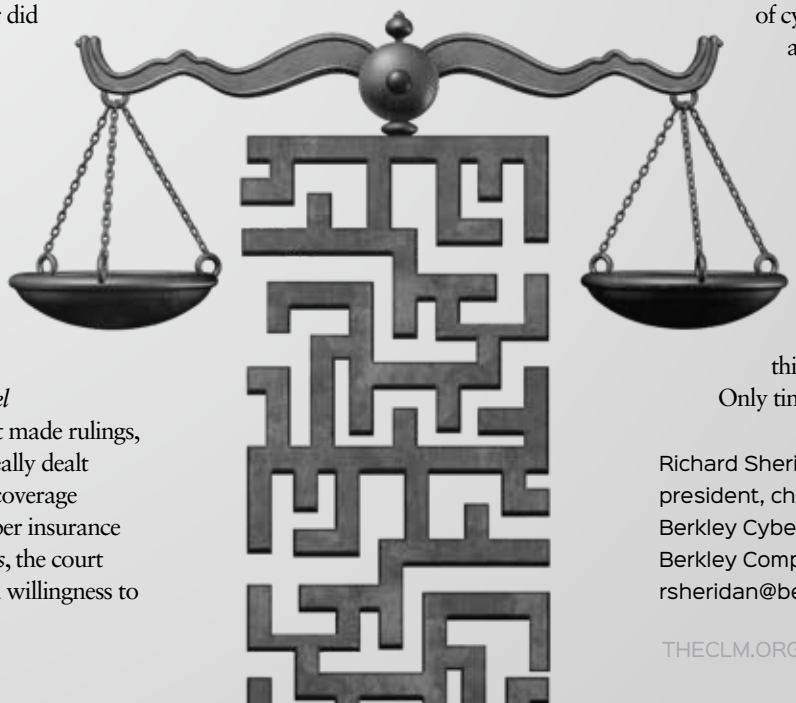
So what can be learned from the scant coverage litigation that has occurred under cyber policies? As far as how courts will interpret these policies, not a lot. The *Cottage* and *Hotel Monteleone* courts have not made rulings, and *Federal*'s court ruling really dealt with interpreting an E&O coverage agreement rather than a cyber insurance issue. At least in *P.F. Chang's*, the court demonstrated that there is a willingness to enforce the breach of contract exclusion in a cyber policy, and *Spec's* court seemed to support that ruling, although in that instance under a D&O policy.

But something can be learned from how cyber insurers have reacted to the litigation concerning coverage for PCI-related costs. Those disputes seem to have resulted in carriers providing a great deal more clarity around that type of coverage. As mentioned above, when cyber policies today provide PCI coverage, they usually contain a carve-back for the breach of contract exclusion so it doesn't apply to PCI assessments. Similarly, most policies now specifically delineate what costs will be covered by the PCI coverage offered so that disputes like the one that occurred in *Hotel Monteleone* should not continue to occur. Of course, some carriers may be slow to adopt these changes, so some disputes in these areas could continue to occur.

AT LEAST IN P.F. CHANG'S, THE COURT DEMONSTRATED THAT THERE IS A WILLINGNESS TO ENFORCE THE BREACH OF CONTRACT EXCLUSION IN A CYBER POLICY, AND SPEC'S COURT SEEMED TO SUPPORT THAT RULING, ALTHOUGH IN THAT INSTANCE UNDER A D&O POLICY.

Is there anything in the litigation that has occurred that may hint to what may be litigated in the future? Perhaps the issue regarding the applicability of a sub-limit in the *Hotel Monteleone* case. Many cyber policies can contain multiple sub-limited coverages not only for PCI, but also for coverages related to social engineering, cybercrime, and various aspects of business interruption. Many of these coverages are relatively new (at least to cyber) and carriers define them differently, so it is not difficult to imagine that, as in the *Hotel Monteleone* case, there could be different views as to how these varying types of sub-limits may apply.

While cyber carriers have demonstrated the ability to quickly modify their products—as demonstrated by how coverage for PCI-related costs has evolved following the litigation previously mentioned—perhaps the rapid evolution of cyber policies could serve as an impetus for future disputes. For instance, many cyber policies have greatly expanded the regulatory coverage that is offered in response to the recently implemented General Data Protection Regulation (GDPR) in the European Union. Could this lead to coverage litigation? Only time will tell. ■



Richard Sheridan is senior vice president, chief claims officer, for Berkley Cyber Risk Solutions, a W.R. Berkley Company.
rsheridan@berkleycyberrisk.com