LAW.COM
An ALM Website
October 27, 2016

Is Cyberinsurance Really Worth It? Using ADR to Resolve Cyberattack Disputes

By Daniel Garrie and Andrew Nadolna

While strengthening a company's cybersecurity posture can make a considerable difference, companies must also prepare for the unfortunate inevitability of a successful cyberattack. Recognizing this risk, companies have turned to cyberinsurance as a tool for mitigating their cybersecurity risks. Unfortunately, uncertainty still exists regarding how courts will interpret this relatively new type of insurance policy. Accordingly, contractual alternatives such as arbitration or mediation are often the most efficient means for resolving cyber coverage disputes.

Photo: iStock

Cyberinsurance, as an industry, is experiencing rapid growth. With 25 to 50 percent annual increases in premiums, 2015 set a record with $2.75 billion in gross premiums written. This is expected to double by 2020 and may get as high as $20 billion by 2025. One feature of this rapidly expanding market is that not all exposures have been properly identified, turned into language and priced into the policy. Terms and conditions are negotiable and the forms are revised frequently. This means there is little value in court precedents in interpreting these policies and from the cases so far it is clear that there have been unintended consequences from policy wordings to date.

Before delving into case law, it is important to understand what cyberinsurance is and what it insures against. A cyberinsurance policy is generally an amalgamated form of different types of insurance, including: errors & omissions coverage, network security coverage and privacy coverage. While policies can be heavily tailored, they generally feature several of the following types of coverage: loss/corruption of data, business interruption, public relations/crisis management, cyberterrorism, etc.

Of great importance is the fact that insurers can write specific baseline requirements for cybersecurity compliance into their policies, which provides sometimes-necessary guidance to companies who are developing or revising their cybersecurity posture. Further, insurers are able to provide services to companies before, during and after a cyberattack. These services can be invaluable in mitigating and remediating the harms associated with such an attack.

While cyberinsurance offers tremendous benefits to those who seek to mitigate their risks, due to its

relative youth as an industry, there are many cases where cyber claims will be disputed. For example, in *P.F. Chang's Inc. v. Federal Insurance Co.*, P.F. Chang's discovered a data breach in June 2014. The breach involved 33 restaurants and compromised the credit card data of roughly 60,000 customers. Upon learning of the breach, P.F. Chang's reported it immediately to Federal Insurance Company (Chubb). The company sought coverage under their cyberinsurance policy for payments to credit card companies resulting from fraudulent payments associated with the breach.

The policy covered "direct loss, legal liability, and consequential loss resulting from cybersecurity breaches," but the Court nevertheless held that the data breach fell outside the policy coverage. Relying on case law involving commercial general liability policy coverage for data breaches, the court found that liability is generally excluded for "the assumption of another's liability, such as an agreement to indemnify or hold another harmless." Because P.F. Chang's was seeking coverage for the assumption of the credit card companies' liability, the Court ruled that this was excluded under the policy and Chubb did not have to pay for vendor related, fraudulent payment costs.

The case of *P.F. Chang's* illustrates that cyberinsurance is still in relative infancy compared to other forms of insurance. The market has yet to determine what should and should not be in an insurance agreement, and, more importantly, what the terms of an insurance policy necessarily mean. Most forms have now been amended to cover the exposures at issue in the *P.F. Chang's* case. But there continues to be new kinds of exposures that are fought over in court. This lack of steady footing in stable forms will continue to lead to a large amount of costly and time-consuming litigation. While the courthouse door is always an option, insurance providers and purchasers should begin looking at contractual options, such as arbitration, to expedite the dispute resolution process, and ensure a relatively quick and confidential outcome.

Why is ADR better than litigation in resolving cyberclaim coverage disputes? Depending on the specifics of a dispute, mediation or arbitration can save anywhere from a handful of months to several years. This is particularly true because the parties can set their own discovery procedures, which are almost always faster, easier and more direct than discovery in the traditional litigation context. Moreover, cyber insurance involves complex technical and insurance issues that judges will often need significant time and resources to understand. By contrast, mediation or arbitration allows the parties to select a neutral with technical cyber experience and/or relevant insurance experience to help navigate the nuances associated with cyber-related disputes. Additionally, since these disputes can often be highly visible, ADR allows the parties to keep the dispute out of the courtroom and away from the media and public eye. Companies considering purchasing cyber policies should strongly consider adding arbitration or mediation clauses to allow for the more efficient resolution of coverage disputes.

Daniel B. Garrie *Esq. is an arbitrator, forensic neutral and technical special master at JAMS, a private alternative dispute resolution (ADR) provider. He is also the executive managing partner of Law & Forensics and head of the computer forensics and cybersecurity practice groups.*

Andrew Nadolna *is a mediator and arbitrator with JAMS. He has 25 years of experience in the insurance industry as a claims executive and litigator.*

Michael Mann*, who contributed to this article, is a senior analyst at Law and Forensics. He received his J.D. from the New York University School of Law.*