UT LAW CLE THE UNIVERSITY OF TEXAS SCHOOL OF LAW

PRESENTED AT

2016 Essential Cybersecurity Law

Ausgust 19, 2016
Austin, Texas

Top 10 Myths About Cybersecurity

Part II

Gavin George

Phong Tran

Lessons Learned on Insuring Cyber Risk from P.F. Chang's and State Bank of Bellingham: What to Look for in Placing Dedicated Network Security/Privacy Liability Insurance

07/11/2016
Micah E. Skidmore

With ever-increasing malware, spear phishing and ransomware attacks on corporate America and ever-contracting terms insuring "cyber" liability under traditional insurance, more and more risk managers are venturing into the market for dedicated network security and privacy liability or "cyber" insurance. Others remain dubious—preferring "traditional" coverage to policies that are little understood and even less tested by claims. Over the past several weeks, two judicial decisions have been issued addressing coverage for cyber risk under "traditional" and "cyber" policies. The score for policyholders: cyber insurance: 0; traditional insurance: 1.

In *P.F. Chang's China Bistro, Inc. v. Federal Insurance Company*, a federal district court judge in Arizona denied P.F. Chang's coverage under a specialized "CyberSecurity" policy for its liability for more than $1.9 million in credit card "assessments," representing the cost of fraudulent charges paid by Visa and MasterCard after hackers obtained some 60,000 credit card numbers from restaurant customers in 2014. Based on the contractual relationships between the relevant parties, Visa and MasterCard claimed the assessments first from card-processor Bank of America Merchant Services ("**BAMS**"), who in turn sought contractual indemnification from P.F. Chang's. According to the Court, P.F. Chang's was not entitled to payment for the assessments because the CyberSecurity policy's coverage was limited to "Privacy Injury," "sustained by a person because of actual or potential unauthorized access to such Person's Record . . . ." Because "BAMS did not sustain a Privacy Injury itself," its claim against P.F. Chang's did not trigger the policy's coverage. Moreover, according to the court, two separate exclusions for "liability assumed by any Insured under any contract or agreement" and "expenses incurred to perform any obligation assumed by, or on behalf of, or with the consent of any Insured," independently relieved Federal of any obligation to pay the assessments claimed against P.F. Chang's.

By comparison, in *State Bank of Bellingham v. BancInsure, Inc.*, a federal appeals panel affirmed summary judgment in favor of a bank seeking coverage for two fraudulent wire transfers, totaling $485,000, under a financial institution bond. Overruling arguments by BancInsure that the loss was not covered because of "employee-caused loss exclusions," the panel concluded that the "overriding cause" of the loss was "criminal activity"—not the employees' violations of policies and procedures. Based on Minnesota's "concurrent-causation" doctrine, State Bank of Bellingham was entitled to payment for its loss, notwithstanding the employees' negligent actions and their role in the loss, because "an illegal wire transfer is not a 'foreseeable and natural consequence' of the employees' failure to follow proper computer security policies, procedures and protocols."

Judging by these results, risk managers may question the necessity of so-called dedicated "cyber" insurance and find validation in reliance on "traditional" policies. In fact, while traditional coverage may provide an important source of recovery for loss and liability arising out of a data breach and should never be overlooked, the same can be said for "cyber" coverage when properly underwritten and negotiated. Some network security/privacy liability forms are very good. Others are awful. Although each policy is different, common issues arise. Here are five items, among

RELATED PRACTICES

Insurance Recovery

Privacy and Data Breach

RELATED INDUSTRIES

Healthcare

Also available as part of the eCourse
2016 Essential Cybersecurity Law eConference

First appeared as part of the conference materials for the
2016 Essential Cybersecurity Law session
"Top 10 Myths About Cybersecurity"