THOMSON REUTERS

Westlaw®

Digital disruption and the new normal: Reducing cyberexposures through collaboration

By Elizabeth S. Fitch, Esq., *Righi Fitch Law Group*

SEPTEMBER 22, 2017

Networks become more connected every day, and businesses are more dependent than ever on data-sharing.

The recent large-scale WannaCry ransomware attack demonstrated that even relatively unsophisticated attacks can cause very significant business disruption, data loss and financial impact for public and private sector enterprises worldwide.

And more extensive attacks, leveraging more powerful cyberweaponry, should be expected.

Although every organization relies on technology, many have failed to carefully evaluate whether their existing insurance policies provide adequate coverage for cyberexposures.

The cyberinsurance market is still in a state of relative infancy and is developing rapidly and inconsistently. Given this inconsistency, the absence of predictive modeling, and the failure or refusal of insurers to share loss information, collaboration among brokers, claims and underwriting and privacy counsel is critical to better understand the exposures.

It will also help to increase the availability of more comprehensive cyberinsurance coverages.

While post-breach collaboration is important to avoid misunderstandings that can lead to costly coverage battles, the focus of this commentary is on the importance of collaboration during the cyberinsurance procurement stage.

TRADITIONAL PROCUREMENT, UNEXPECTED LOSSES

An insured's procurement of cyberinsurance has followed the same path as the path taken to procure traditional insurance policies: Scope of coverage and premium are left to underwriters and brokers to negotiate. This has been a costly mistake that has caused many carriers to leave the market and others to experience unexpected losses.

The business interruption loss claimed by Southwest Airlines is a perfect example of unexpected consequences for an insurance carrier.

Southwest is seeking over $100 million in business interruption loss from its London insurance carriers due to its own router failure, which resulted in the cancellation of 2,300 flights.

Insurer AIG did not contemplate this loss when it issued the policy, but the policy language failed to limit coverage to system outages "caused by a cyberattack."

Had the AIG underwriter collaborated with its claims department, Southwest's broker and privacy counsel, it might have avoided being in the untenable position of having to pay out $100 million to Southwest.

The takeaway from the Southwest claim is that collaboration is vital to the cyberinsurance procurement process due to the complex and nonuniform nature of cyberpolicies.

The cyberinsurance market is still in a state of relative infancy and is developing rapidly and inconsistently.

There are four distinct areas that have most often led to confusion and exposure in cyberinsurance procurement: coverage for regulatory actions, fines and penalties; inadequate policy limits and misunderstanding of sublimits; coverage for Payment Card Industry assessments; and warranties and representations.

Coverage for regulatory actions, fines and penalties

The importance of regulatory coverage is best illustrated in *Federal Trade Commission v. Wyndham Hotels.*[1]

That case began when the Federal Trade Commission filed a lawsuit against certain corporate entities affiliated with Wyndham Hotels. The lawsuit claimed that Wyndham Hotels failed to provide reasonable security measures for its customers' information, such as credit card numbers, and allowed the unauthorized access of such data on multiple occasions.

The FTC alleged that this failure violated the Federal Trade Commission Act's prohibition on unfair and deceptive trade practices.

The 3rd U.S. Circuit Court of Appeals agreed with the FTC and found that the agency has authority to regulate cybersecurity. Ultimately, Wyndham had little choice but to settle with the FTC. Many cyberinsurance policies will not provide coverage for regulatory proceedings.

Traditional insurance products typically do not cover fines and penalties arising from regulatory proceedings. Generally speaking, coverage for fines and penalties is considered to be against public policy and thus uninsurable as a matter of law.

Many stand-alone cyberinsurance policies affirmatively provide coverage for the defense of regulatory actions arising from a data or security breach, as well as resulting fines and penalties — to the extent such are insurable under the law.

The scope of coverage provided by various policies varies greatly. Some policies contain very broad coverage, while others have a very narrow definition of "regulatory proceeding." Regulatory coverage is important for companies in the retail, hospitality and health care sectors, but is not necessarily critical for companies in sectors that are not as highly regulated.

Cyberinsurance sublimits

Cyberinsurance policies are unique in that many contain multiple sublimits that are not typically found in traditional insurance policies.

Due to the sheer number of sublimits — and oftentimes sublimits within sublimits — the insured can be easily confused. Greater confusion can occur where cybercoverage is conferred via an endorsement that does not have a separate declaration page outlining the limits available for the endorsed coverage.

Given industry knowledge that unsophisticated insureds do not carefully review policies, collaboration among the underwriter, broker and privacy counsel is important to protect the insured.

A broker learned this lesson the hard way in a highly publicized case involving Louisiana's historic Hotel Monteleone. The hotel purchased a cyberinsurance policy through Eustis Insurance Co., an insurance broker for Ascent Underwriting.[2]

In 2013, the hotel was the victim of a cyberattack that resulted in Payment Card Industry liabilities in excess of $200,000. After the incident, it purchased a cyberpolicy to protect itself against similar future losses.

Hotel Monteleone alleged that Eustis was tasked with finding it a cybersecurity policy that would have reasonably covered future fraud and reimbursement charges. The hotel was advised the policy would cover similar future losses and contained general limits of $3 million.

About a year later, Hotel Monteleone was again the victim of a cyberattack. When it made a claim for its losses, it learned that the policy contained a sublimit of $200,000 for PCI fines, penalties and assessments.

The hotel was denied coverage for the very type of insurance it had sought out after the first loss. It sued Eustis Insurance, and the case ultimately settled for an undisclosed amount.

PCI assessments

Every business that processes credit card transactions must sign a merchant services agreement with the bank or processor.[3] In that agreement, the business contractually agrees to comply with the Payment Card Industry Data Security Standards, or PCI-DDS.

Cyberinsurance policies are unique in that many contain multiple sublimits that are not typically found in traditional insurance policies.

Credit card breaches are often discovered after the business's merchant bank or card brand finds multiple fraudulent charges that were made at one common point.

If the business was the common point, it is contractually obligated to conduct a forensic investigation to determine the scope of the breach and whether it was PCI-DSS-compliant at the time. These forensic costs can be extreme.

Additionally, the payment card brands will seek to recoup their operational expenses, such as for card reissuance, notification or counterfeit fraud recoveries incurred in connection with the breach.

Also, any noncompliance with the PCI-DSS will result in fines that that vary depending on the breach and the size of the business.

Some insurers offer coverage for PCI fines and penalties only via a sublimit. Others have expanded the coverage to include fraud assessments, card reissuance costs or forensic investigation costs, either with full policy limits or via a sublimit.

An example of failing to procure coverage for PCI fines involves restaurant chain P.F. Chang's, which had a cyberinsurance policy through Federal Insurance Co.[4]

After Chang's purchased the policy from Chubb, Chang's experienced a breach in which hackers stole 60,000 credit card numbers.

Chubb marketed the policy purchased by Chang's as an insurance solution that addresses the full breadth

of cyberrisks, including "direct loss, legal liability and consequential loss resulting from cybersecurity breaches."

When Chang's sought $2 million in reimbursement for credit card-related costs, Chubb denied coverage. It claimed, among other things, that Chang's had no reasonable expectation of coverage.

Chang's then filed suit against Chubb. The court granted summary judgment in favor of Chubb because Chang's had previously made a separate contractual agreement with the credit card processing company to pay costs associated with the breach.

Chang's is appealing the decision. Though the policy was sold to cover the full breadth of cyberrisks, $2 million (not to mention the subsequent legal fees) was not covered because of insufficient PCI fines coverage.

Representations and warranties

Cyberpolicy representations and warranties often require insureds to warrant they are maintaining proper administrative and technical security controls. These warranty statements are often highly technical in nature. As a result, the insured understands neither the warranties nor the implications of making them.

> Collaboration with privacy counsel during the cyberinsurance procurement process can reduce risk and ultimately save money for the insurer, broker and client.

Columbia Casualty Co. v. Cottage Health Systems arose from a data breach that resulted in the release of 32,500 patient records.[5]

Cottage had prepared for an event like this by purchasing an insurance policy from Columbia. However, within that policy Cottage had answered affirmatively to a series of risk control assessment questions, which included questions about whether it had implemented and maintained certain protocols to help prevent breaches.

Columbia filed a complaint against Cottage asserting that a policy exclusion provided that the insurer would not be liable if a loss was caused by Cottage's failure to implement and maintain the protocols.

The court dismissed the complaint based on an alternative dispute resolution clause in the policy.

COLLABORATION DURING THE PROCUREMENT STAGE

Involving the insurer's claims professional in the procurement stage helps all stakeholders to understand the historical costs of those risks for the insured's industry.

In turn, this assists in the insured's cost-benefit analysis of scope of coverage compared with premium cost. Involving claims in the insurance procurement process also assists the underwriter in assessing risk and setting premium.

With input from claims, the underwriter is better poised to communicate the basis for premiums to the broker.

During the renewal process it is even more critical for the underwriter to consult with the claims division if the insured experiences a claim during the existing policy period. The claims professional can provide historical cost data about the claim and may have a much better understanding of the insured's business operations and risk because of what has been reported during the claim.

Collaboration with privacy counsel during the cyberinsurance procurement process can reduce risk and ultimately save money for the insurer, broker and client. Privacy counsel can drive the insured's adoption and implementation of a cyberrisk mitigation program, which will reduce risk of a cyberbreach.

On one end of the spectrum, web-based cyberrisk assessments tend to be "cookie cutter" and fail to take into account the unique business characteristics of the company being assessed.

On the other end, risk assessments performed by technology experts tend to be overly comprehensive and make sweeping recommendations for technical and administrative control overhauls without respect to operational and financial costs.

Privacy counsel can balance those interests and equip the company's executive team to make strategic decisions that further overall company goals while taking into account financial costs.

Assuming privacy counsel is a seasoned breach coach and trial lawyer, their unique perspective on perceived risk versus actual risk can foster better communications among the broker and underwriter — and in turn assist the client in balancing its unique business needs with cost of premium.

Brokers can leverage privacy counsel consultation as value added to sell policies. In return, the insurer and the insured client benefit from the reduced risk of business interruption and reputational harm.

CONCLUSION

Mitigating risk and exposure is the goal of every carrier, while avoiding reputational harm and business interruption is the goal of the insured. Although these goals are necessarily aligned, the speed at which cyberrisk has evolved — and continues to evolve — has left everyone in a state of frustrated confusion.

Without cooperation and fundamental change in the insurance procurement process, confusion will continue to permeate the cyberinsurance market.

Ensuring collaboration among the broker, underwriting and privacy counsel is the best way to effect the much needed change and is essential to minimizing financial risk and ensuring sufficient coverage.

NOTES

[1] *Fed. Trade Comm'n v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

[2] Complaint, *New Hotel Monteleone LLC v. Certain Underwriters at Lloyd's of London,* No. 15-11711 (La. Civ. Dist. Ct., Orleans Parish Dec. 10, 2015).

[3] *PCI Costs Coverage: What Insureds Really Need,* Biggs Insurance Services, http://www.biggsinsurance.com/pci-costs-coverage-what-insureds-really-need/ (last visited Sept. 10, 2017).

[4] *P.F. Chang's China Bistro Inc. v. Fed. Ins. Co.,* No. 15-cv-1322, 2016 WL 3055111 (D. Ariz. May 31, 2016).

[5] *Columbia Cas. Co. v. Cottage Health Sys.,* No. 15-cv-3432, 2015 WL 4497730 (C.D. Cal. July 17, 2015).

This article first appeared in the September 22, 2017, edition of Westlaw Journal Computer & Internet.

ABOUT THE AUTHOR

Elizabeth S. Fitch is an attorney and a founding member of **Righi Fitch Law Group** in Phoenix. She also is a member of the International Association of Defense Counsel, an invitation-only group of corporate and insurance defense attorneys and insurance executives. In her practice, she counsels companies and insureds on cyberliability and responding to data breaches. She is certified by the International Association of Privacy Professionals and serves as the chief information security officer for her law firm. She can be reached at beth@righilaw.com.