"The Cyber Insurance Conundrum"

By: Elizabeth S. Fitch

I. Introduction

Insurance brokers are exposing themselves to risks by selling cyber insurance endorsements and policies without fully understanding them or their client's cyber risk profile. Relying on the long standing relationships and competency of their brokers, Companies assume that the cyber policy recommended by their broker provides the necessary financial protection. Oftentimes, this reliance is misplaced. When the cyber insurer rightfully denies coverage, insureds are looking to their insurance brokers to make them financially whole and are in turn triggering a new wave of litigation: errors and omission claims against insurance brokers.

II. Duties Imposed on Cyber Insurance Brokers and Agents

Jurisdictions have uniformly adopted a general duty to act with reasonable care, skill, and due diligence in procuring requested insurance for clients. Most jurisdictions have also imposed a "duty to advise," in which, the broker is held responsible for failing to offer the insurance coverage for which the insured *"should have been"* advised. The duty to advise places a heightened burden on insurance agents and brokers to have a complete, working knowledge of cyber insurance policies. Each client will require a unique analysis for a cyber policy or cyber coverage that will best suit their needs. This requires brokers to familiarize themselves with the risks faced by clients and to negotiate for a policy that is sufficient to encompass the risks in case of a cyber breach.

III. Challenges Facing Cyber Insurance Brokers

Brokers are in a highly precarious position with respect to liability exposure arising in connection with the counseling and placement of cyber insurance products. One challenge facing insurance brokers is the rapid evolution of the exposures and the insurance product. Cyber insurance is in a state of relative infancy and is developing with rapid inconsistency. There are over 50 carriers offering stand-alone cyber insurance products and almost all carriers offer some level of cyber insurance via endorsements to traditional products. These stand-alone cyber insurance policies are lengthy and complex and can be heavily endorsed. Most policies contain multiple insuring agreements – a combination of third-party "liability" coverage and first-party "direct" coverage.

Another challenge brokers face with respect to cyber insurance placement relates to the adequacy of limits. Companies often heavily rely on insurance brokers to advise them as to "how much" insurance they should purchase. Many cyber insurance products contain multiple different limits, with sub-limits and even sub-limits *within* sub-limits. The absence of predictive modeling means that insurers and brokers alike are forced to look at other factors to evaluate risk and the adequacy of aggregate limits and sublimits.

IV. Liabilities/Exposures of Cyber Brokers

There are four distinct categories against brokers that are likely to evolve: (1) failure to procure coverage for regulatory actions, fines, and penalties; (2) failure to recommend an adequate policy limit and to inform the insured of sub-limits; (3) failure to procure coverage for Payment Card Industry assessments; and (4) failure to discuss ramifications of insured's failure to comply with the representations and warranties in the application.

Coverage for Regulatory Actions/Fines/Penalties:

The importance of regulatory coverage is best illustrated in *Federal Trade Commission v. Wyndham Hotels*.[1] The Federal Trade Commission ("FTC") filed a lawsuit against certain corporate entities affiliated with Wyndham Hotels, claiming that Wyndham Hotels failed to provide reasonable security measures for its customers' information, and allowed the unauthorized access of such data on multiple occasions. The FTC alleged that this failure violated the FTC's Acts prohibition on unfair and deceptive trade practices. The Third Circuit Court agreed with the FTC, and found that the FTC has authority to regulate cyber security. Ultimately, Wyndham had little choice but to settle with the FTC.

Many stand-alone cyber insurance 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. Some policies contain broad coverage, while others have a narrow definition of "regulatory proceeding." Therefore, it is incumbent upon the cyber insurance broker to procure a policy that includes the broadest form of coverage for the types of regulatory proceedings that may be triggered as a result of the insured's operations.[2]

[1] F.T.C. v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 608 (D.N.J. 2014).
[2] John Jo & Alicia Gilleskie, Cybersecurity Insurance –One size does not fit all, Smith Anderson, http://www.smithlaw.com/updates-alerts-Cybersecurity-Insurance.html.

Cyber Insurance Sub-Limits

Cyber insurance policies are unique in that many contain multiple sub-limits and oftentimes sub-limits within sub-limits. Due to the sheer number of sub-limits the insured can easily become confused. Given industry knowledge that unsophisticated insureds do not carefully review the policies, the brokers' duty to act with reasonable care may require the broker to not only understand the sub-limits, but also to properly counsel the insured on the financial implications of the sub-limits.

In 2013, Hotel Monteleone was the victim of a cyber-attack, which resulted in PCI liabilities in excess of $200,000.[3] After the incident, the hotel purchased a cyber insurance policy through Eustis Insurance Co. ("Eustis") to protect itself against similar future losses. The broker advised the hotel that the policy would cover against similar losses in the future, and contained general limits of $3 million. Approximately one year later, Hotel Monteleone was again the victim of a cyber-attack. When the hotel made a claim for their losses, the hotel learned to its detriment that the policy contained a sub-limit of $200,000 for PCI Fines, Penalties, and Assessments. The hotel was denied coverage for the very type of insurance it sought out after the first loss, and in turn sued Eustis. The case ultimately settled for an undisclosed amount.

Payment Card Industry Fines, Penalties, and Assessments:

Businesses that process credit card transactions are required to sign a "Merchant Services Agreement," contractually agreeing to comply with the PCI-DSS (Payment Card Industry Data Security Standards). Credit card breaches are often discovered after the business's merchant bank or card brand finds multiple fraudulent charges used at one common point. Should the business be the common point, the business itself will be contractually bound to conduct a forensic investigation to determine the scope of the breach, and whether the business was PCI-DSS compliant at the time. The payment card brands will be looking to recoup their operational expenses, such as for card re-issuance, notification, or counterfeit fraud recoveries incurred in connection with the breach. Any non-compliance with the PCI-DSS will result in fines, based on the breach and size of the business. Some insurers offer coverage for PCI fines and penalties only via a sub-limit. Other insurers have expanded the coverage to include fraud assessments, card re-issuance costs, or forensic investigation costs, either with full policy limits or via a sub-limit.

[3] New Hotel Monteleone, LLC v. Eustis Insurance, et al. Copy of Complaint available at http://www.lockelord.com/newsandevents/publications/2016/02/-/media/B5069EE57D164752B1B2B070256558CB.ashx

An example of failing to procure coverage for PCI fines involves P.F. Chang's ("Chang's") which had a cyber insurance policy through Federal Insurance Co. ("Chubb"). After Chang's purchased the cyber insurance policy from Chubb, Chang's experienced a breach in which hackers obtained 60,000 credit card numbers belonging to its customers. Chubb marketed the policy purchased by Chang's as "a flexible insurance solution designed by cyber risk experts" that "covers direct loss, legal liability, and consequential loss resulting from cyber security breaches." When Chang's sought $2 million on reimbursement for credit card related costs, Chubb denied the coverage. Chubb claimed that Chang's had no reasonable expectation of coverage. Chang's filed suit against Chubb. The court granted summary judgment in favor of Chubb. The case is currently being appealed by Chang's. The policy that was sold to Chang's was sold to cover the full breadth of cyber risks, and yet, $2,000,000 (and not to mention the subsequent legal fees) was not covered because of insufficient PCI fines coverage.

Representations and Warranties:

Cyber policy representations and warranties often require insureds to represent and warrant they are maintaining proper administrative and technical security controls. These warranty statements can be highly technical in nature. As a result, the insured neither understands the warranties themselves nor the implications of signing the warranties.

Columbia Casualty Company v. Cottage Health Systems ("Cottage") arises out of a data breach that resulted in the release of 32,500 patient records. Cottage had prepared for an event like this by previously purchasing an insurance policy from Columbia. However, within that policy Cottage had answered affirmatively to a series of risk control assessment questions, which included implementing and maintaining certain protocols to help prevent breaches. Columbia filed a complaint against Cottage asserting that an exclusion within the policy provided that Columbia would not be liable if a loss was the result of failing to implement and maintain the protocols. (The court dismissed the complaint based on an alternative dispute clause in the policy.) This coverage dispute might have been avoided had Cottage been advised of what was in the representations and warranties, and then simply followed them.

V. Defending Brokers and the Standard of Care:

As with most claims against professionals, to prove a malpractice claim against a broker requires expert testimony that the broker fell below the applicable standard of care. Given the ongoing and rapid evolution of cyber exposures and inconsistency in insurance policies, the standard of care is not easy to define. The standard of care for brokers placing traditional coverages is relatively well defined due to

standard ISO provisions, historical data, predictive modeling, and legal opinions to guide an experienced broker to evaluate proper coverage for his/her client. In contrast, the absence of data for cyber exposures and coverages is a two edge sword. On the one hand, the absence of data makes it difficult for a broker to evaluate and assess proper coverage for a particular client. On the other hand, this absence of data means that cyber brokers are left to their own devices to evaluate proper coverage. Since there are no well-established factors to evaluate proper coverage, the standard of care is also subject to interpretation.

Conclusion

The cyber insurance industry is evolving rapidly in response to higher levels of claims and increasing level of threats. Insurers (especially those with lots of cyber experience) are refining their underwriting tools, making increasing valuable risk management services available to their insureds. There is no question that brokers are in a conundrum. No policy is a one-size fits all in the cyber insurance world. At a minimum cyber insurance brokers should be asking the right questions to ensure the business is covered for potential losses from a cyber breach. Retail insurance brokers can mitigate their errors and omissions risks aligning with specialty brokers that have extensive backgrounds placing cyber insurance. Wholesale brokers can join retail brokers during their client meetings to assist in educating their clients and/or prospects and also include direct meetings with cyber underwriters, after preparing the client in advance prior to meeting directly with insurers.