Opportunities abound to optimise your cyber liability insurance to your needs

September 2014 Issue

September 2014 | PROFESSIONAL INSIGHT | RISK MANAGEMENT

Financier Worldwide Magazine

7

BY

Hsiao C. (Mark) Mao

Kaufman Dolowich & Voluck LLP

Michael A. Bozzuto

Steven Bozzuto Insurance Agency, Inc.

The risk of cyber breaches is more prominent today than ever before. Mobile and telecommunications technology is evolving at a rapid pace, in both its breadth of use and the number of users. The technology boom has significantly increased the number of access points and opportunities available to hackers and thieves. Notable incidents of compromised security include the users and shoppers of Sony PlayStation, Target and Michael's. Recent news also highlighted programming bugs within Microsoft Windows and OpenSSL (i.e., the 'Heartbleed' bug), further demonstrating that cyber vulnerability is a constant risk of doing business, whether one is using proprietary or open-source software.

As the volume of insurance claims for cyber data breaches increase, the insurance industry is moving quickly to insulate insurance claims for 'cyber liability' from more traditional policies such as 'commercial general liability insurance policies' (CGL Policies). Similarly, many organisations have begun purchasing 'cyber liability insurance' (Cyber Insurance).

Nonetheless, many organisations still do not know they can mitigate their cyber risks with insurance. Even for those who have purchased Cyber Insurance, great confusion remains as to what such policies may or may not cover.

To date, there is still great diversity among the insurance products available to cover cyber risks. Two policies both claiming to be 'cyber insurance' may in fact provide different coverage. It is imperative that all organisations and their legal counsel carefully read and assess their policies, taking into full consideration the various cyber risks to which their business may be vulnerable. Organisations should not indiscriminately purchase Cyber Insurance and should instead select their various layers of coverage with great attention and deliberation.

Moving from CGL policies to cyber insurance

The recent explosion of internet and mobile technology has brought about increasingly common cyber breaches in the form of unauthorised access to personal, financial and health care information. Traditional CGL Policies were not designed to provide coverage for loss of sensitive electronic data and are typically purchased to cover tangible first and third property loss.

Nonetheless, organisations have tried with various levels of success to tender coverage for cyber breaches under CGL Policies. For example, in *Hartford Casualty Ins. Co. v. Corcino & Associates et al.* 2013 WL 5687527, at *2 (C.D. Cal. Oct. 7, 2013), the California Court found coverage under a CGL Policy for a hospital breach that compromised the medical records of nearly 20,000 patients. In that CGL Policy, "personal and advertising injury" was defined to include "[o]ral, written or electronic publication of material that violates a person's right of privacy".

On the other hand, in the case of the massive Sony PlayStation data breaches in 2011, Sony also tendered coverage under its CGL Policies. On 21 February 2014, a New York trial judge granted two of Sony's insurers' motions for summary judgment for no coverage under the CGL Policies. Although some expect Sony to succeed on appeal, the contrasting successes among differing cases demonstrate the need for organisations to secure appropriate Cyber Insurance in addition to their CGL Policies.

In fact, many organisations may have no choice now but to purchase appropriate Cyber Insurance. In the fall of 2013, the Insurance Services Office (ISO) – which most in the insurance industry consider to be the 'gold standard' for insurance policy language – issued a number of exclusionary endorsements for use with CGL Policies. These exclusionary endorsements have been approved by the vast majority of regulators in the US states and territories and provide for exclusions such as:

"Exclusion – Access Or Disclosure Of Confidential Or Personal Information And Data-Related Liability – Limited Bodily Injury Exception Not Included… This insurance does not apply to: Access Or Disclosure Of Confidential Or Personal Information… 'Personal and advertising injury' arising out of any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of non public information. This exclusion applies even if damages are claimed for notification costs, credit monitoring expenses, forensic expenses, public relations expenses or any other loss, cost or expense incurred by you or others arising out of any access to or disclosure of any person's or organization's confidential or personal information. (ISO CG 21 07 05 14 (2013))."

Regardless of the current development of case law on coverage for cyber claims made on CGL Policies, most insurance carriers are expected to specifically exclude cyber breaches from coverage in their CGL Policies. To mitigate their business risks associates with cyber breaches, organisations may have no choice but to purchase Cyber Insurance.

Are you comparing apples and oranges?

Even among Cyber Insurance policies, there is great variation in the coverage provided. Not only do the policies vary considerably in their language and provisions, some policies seek to better serve their insureds with additional features. Since case law on Cyber Insurance is still relatively scarce, it is even more important for organisations to review their coverage with both their insurance brokers and counsel.

Of the numerous policies we surveyed, there were indeed common characteristics. Most policies were specifically designed to protect against cyber risks, and those hybrid policies that provide for some cyber liability protection, typically provide for coverage for at least the following. Firstly, coverage for first and third loss arising from breach of the insureds' networks and databases. Breaches by hackers, identity thieves, viruses and trojans may fall into this category, subject to policy exclusions.

Secondly, coverage for regulatory defence expenses. In addition to various federal statutes that may apply, most states now have statutory reporting and disclosure requirements for insureds that discover a data breach. In cases where there may be a significant amount of personal information compromised, it would not be unusual for organisations to receive calls from both federal and state authorities. Cyber Insurance may provide coverage for regulatory investigations relating to the insureds' responses to such requirements, again subject to exclusions.

There were also some exclusions common to most policies: (i) breaches

that occurred prior to the policy period or a policy specified 'retroactive period', including breaches that the insured had knowledge or suspicion of prior to said period; (ii) intentional, dishonest and criminal acts by the insured; (iii) loss to subsidiaries, related entities and joint-venturers, unless they are otherwise specified as an insured; (iv) liability assumed by the insured under a contract; and (v) claims brought by an insured against the insured.

Perhaps most importantly, among the policies we sampled we found great variance in how covered cyber breaches and 'losses' were defined. Because the actual business and vulnerabilities of more traditional internet vendors may differ substantially from emerging technologies such as 'cloud companies' and 'big data', a careful selection of appropriate policy language is absolutely imperative.

Just as interesting are the various additional coverages that carriers are packaging with their Cyber Insurance. For example, subject to policy exclusions, some of the policies we sampled may provide coverage for: (i) 'errors and omissions' committed by the insured in the course of providing support services for their technology; (ii) 'advertising and media claims'; (iii) consequential damages in the form of loss of power and networks to third parties; and (iv) loss of intellectual property of third parties.

We found that carriers also varied in how they package Cyber Insurance with traditional forms of insurance. Carriers are often packing their Cyber Insurance with directors & officers policies, in addition to traditional CGL Policies.

In short, the insurance marketplace is rife with opportunities for those who are willing to spend the time to optimise their insurance to best fit their business needs.

Conclusion

Even for organisations that have purchased Cyber Insurance, many have not carefully reviewed their policies to assess what may or may not be covered. This can be particularly dangerous where the policies purchased are not optimised to fit the organisation's business needs.

For large organisations that need multiple layers of Cyber Insurance, it is even more important to conduct a thorough review to make sure that there are no gaps in coverage. Organisations should not passively rely on their professional advisers and should instead affirmatively assess and reassess their needs in light of the changing insurance environment. Indeed, Cyber Insurance brokers are likely to inform clients that where underwriters are still trying to figure out how to

best underwrite cyber risks, opportunities abound for organisations to optimise their Cyber Insurance to fit their needs for little – if any – additional costs.

Hsiao C. (Mark) Mao is a partner at Kaufman Dolowich & Voluck LLP and Michael A. Bozzuto is a commercial lines agent at Steven Bozzuto Insurance Agency, Inc. Mr Mao can be contacted on +1 (415) 926 7600 or by email: mmao@kdvlaw.com. Mr Bozzuto can be contacted on +1 (916) 673 2607 or by email: mike@bozzutoinsurance.com.