The evolving cyber insurance market: How IT companies, financial institutions, and other nontraditional players can offer cyber insurance coverage to their customers

14 November 2017

In this hoganlovells.com interview, Hogan Lovells counsel Robert Fettman discusses the evolution of cyber insurance, the level of regulatory oversight applied to covered entities, and ways that noninsurance companies can offer their clients cyber insurance coverage.

How has cyber insurance evolved?

Fettman: The cyber insurance market is relatively young. Its early roots can be traced to the late 1990s, leading up to the Y2K Millennium Bug, which got people thinking about how they could insure against potential digital exposures. The initial products were pretty rudimentary, had a lot of exclusions, were targeted to very specific technology risks, and largely limited coverage to liability to third parties. First-party loss suffered by the insured was typically not included in the early products.

Cyber insurance started picking up steam in the mid-2000s. Coverage broadened to cover first-party liability such as costs associated with a data breach and the insured's response thereto. While cyber insurance policies these days are broader than ever and are becoming increasingly standardized as the market continues to mature, coverage terms between carriers can still vary greatly. Cyber insurance coverage can run the gamut from coverage for business interruption, theft of digital assets, losses arising from disclosure of sensitive information through human error to lawsuits alleging IP infringement and damage to a company's reputation, to name just a few. The types of coverages are constantly evolving. There is an ever-growing list of hazards that people are looking for cyber insurance to cover.

What challenges have insurance carriers faced while evolving their cyber policies?

Fettman: For insurance carriers to be able to develop a viable cyber insurance product, they need to have access to credible actuarial data that would help drive their pricing. The difficulty they encounter is trying to come up with sound projections for what losses might result in the future from cyber risks, which in some cases may not even exist today.

What you see then are insurance companies compensating for their lack of credible historic loss run data by undertaking an assessment of the applicant's risk management procedures — its overall risk culture — and relying somewhat on the confidence they will get from diligencing the

insured's cyber risk profile. And to some extent that ends up driving the scope of coverage and premium cost.

What aspects of cyber insurance are regulators focusing on?

Fettman: Understandably, insurance regulators are paying close attention to what's happening in the cyber insurance market, though they are not necessarily looking to shape or prescribe how cyber insurance is written. Regulators are really focusing on how financial institutions, insurance companies, and other repositories of personal information are protecting customer data, related privacy concerns, and how cyber events are disclosed to the public and the regulators.

The National Association of Insurance Commissioners (NAIC) has been focusing on cyber insurance for several years now. In 2014, the NAIC formed the Cybersecurity (EX) Working Group to serve as the central focus for regulatory activities relating to cybersecurity. In 2015, the NAIC put out cybersecurity regulatory guidance that included 12 principles identifying the risks and best practices in protecting consumer information, and more recently adopted an insurance data model security act, which creates rules directed at insurance companies and other regulated entities — such as insurance brokers and agents — covering data security, investigation, and breach notification.

What does New York's first-in-the-nation cybersecurity regulation require covered entities to do?

Fettman: The New York State Department of Financial Services (NYDFS) jumped to the lead in getting cybersecurity regulation passed. A comprehensive set of regulations went into effect in New York on March 1, 2017 with a number of rolling deadlines for coming into compliance with various requirements. The regulations essentially require insurance companies, banks, and anyone licensed by the NYDFS to assess their cyber risk profiles and design cybersecurity programs in a robust fashion. More recently, following the cyber breach at Equifax, the NYDFS has been trying to also include credit monitoring agencies as a covered entity subject to the regulations.

Among other requirements, covered entities will need to have a chief information security officer who will oversee and implement a cybersecurity program and provide periodic reporting to key stakeholders. The New York regulations also require covered entities to have policies and procedures to: annually penetrate and test a company's systems for vulnerability, limit access privileges to nonpublic information and implement an incident response plan and cybersecurity training for employees. Covered entities are required to report to the NYDFS any cybersecurity event, including unsuccessful hacks. This has given the industry some pause because on any given day, hackers are attempting to get into companies' IT systems and websites. When does it amount to a reportable breach? Some of the open issues surrounding the regulations' scope hopefully will become clearer as they are implemented on a rolling basis through 2017 and 2018.

Are nontraditional players able to offer their clients cyber insurance as part of a bundled service offering?

Fettman: Financial institutions, technology companies, and other large organizations that provide IT services or maintain customer data on behalf of customers are thinking about how they can ensure that their clients are adequately protected. Because insurance is highly regulated, it cannot be sold by an entity that is not properly licensed — whether as an insurance company, if it is underwriting risk, or as an insurance producer, if it is only selling insurance policies to end users but not retaining any of the underwriting exposure.

Companies that are looking at getting involved in offering cyber insurance to their clients have to carefully navigate and understand the complex patchwork of state insurance law as it relates to the sale and solicitation of insurance. Even something as simple as recommending that a customer obtain a particular cyber insurance product from a particular insurance company could potentially run afoul of a state's insurance licensing requirements. The more granular discussions or materials that a company provides to its customers are, the greater the potential for such actions to implicate insurance licensing laws.

What options are available to financial institutions, technology companies, and other large organizations that are not licensed as insurance producers that want to get involved in their clients' cyber insurance programs?

Fettman: Financial institutions and technology companies have gotten involved in different ways when it comes to cyber insurance. Some recognize that they don't want to be an insurance producer, so they will make suggestions to their customers that they get insurance without going into any detail — to avoid being captured by insurance producer licensing laws.

Others might want to have a licensed agency within their group so that they can participate in the insurance programs on a commission basis. That entity would offer insurance products directly to the institution's customers and earn commissions (on a risk-free basis) from the insurance company issuing the policy, which would typically be unaffiliated.

For those that want to get further involved, they may actually look to participate in some of the underwriting profits and losses of insurance programs. One way of doing that is to form a captive insurance company that can then retain all or a portion of the risk that is being offered to their customers by a so-called "fronting" insurance company.

That's the gamut of participation by nontraditional or noninsurance companies that dabble in the cyber insurance space.

About Robert Fettman

Robert Fettman has represented many of the largest insurers and reinsurers from around the world in all types of insurance transactional and regulatory matters. Robert has worked on many of the largest Life and P/C insurance acquisitions (including the largest P/C acquisition in history), representing both U.S. and non-U.S. public and private companies within the insurance industry, as well as nonsector clients, including private equity firms and pension funds. He also regularly

advises clients on insurance regulatory compliance, market conduct examinations, disciplinary proceedings, multistate insurer and agency licensing, insurance product development, surplus lines, statutory investments, and transactions within insurance holding company systems. Clients also turn to Fettman for advice on insurance regulatory developments at the NAIC and U.S. state, federal (Dodd-Frank, ACA), and international levels (IAIS).

> Read the full article online