Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# The Role Of Cyberinsurance In Risk Management

*Law360, New York (April 7, 2016, 11:32 AM ET) --*
On March 22, 2016, the Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies of the U.S. House of Representatives Homeland Security Committee held a hearing on the role of cyberinsurance in risk management. The hearing focused on how the cyberinsurance market, which could triple in size to $7.5 billion in annual premiums by 2020, can encourage companies to improve their security safeguards and protect themselves against cyber attacks. The subcommittee's chairman, Rep. John Ratcliffe, R-Texas, remarked, "Just as the process of obtaining home insurance can incentivize homeowners to invest in strong locks, smoke detectors and security alarms, the same could be true for companies seeking to obtain cyberinsurance." The hearing explored how cyberinsurance can generate "market-driven methods" for improving security protections not only for large businesses, but also for medium and small companies.


James R. Woods


Marcus A. Christian

The insurance industry has been a catalyst for corporate change in the past. For example, the industry helped corporate boards of directors improve corporate governance through introducing directors and officers liability insurance decades ago. Similarly, cyberinsurance promises to help companies strengthen their cybersecurity protections. In part, the cyberinsurance market will influence corporate behavior through the desirability, availability, extent and cost of coverage.


Jeyshree Ramachandran

Companies recognize that cyberinsurance is advantageous. Matthew McCabe, the senior vice president of Marsh LLC, testified on the benefits of cyberinsurance, which include reimbursing the costs a business pays to respond to a cybersecuriy incident, covering the fees and damages from ensuing litigation and reimbursing companies for revenues lost or expenses incurred due to a disruption related to a cyber incident. Given these benefits, businesses increasingly seek to add cyberinsurance to their enterprise risk management programs. According to a Matthew McCabe, the number of his Marsh LLC's U.S. based clients purchasing cyberinsurance in 2015 exceeded the prior year by 27 percent.

However, as with other types of insurance, not all companies that want cyberinsurance will be able to obtain it. And premiums will vary according to organizations' respective cybersecurity postures. Companies with well-developed safeguards, including up-to-date written

information security programs (WISPs) and data breach response plans (DBRPs), together with active board of director governance of cybersecurity risk, will enjoy broader cybersecurity coverage at lower premium costs. These market incentives will motivate companies to adopt and implement sound cyberrisk management policies. Indeed, if a company does not have a WISP, DBRP or board oversight of cybersecurity risk, it may have difficulty obtaining cyberinsurance at any cost.

The subcommittee's hearing reinforced the need to implement effective WISPs, DBRPs, strong board governance programs and other best practices. They must become ingrained in a corporation's culture. In particular, hearing testimony highlighted four components of effective cyberrisk cultures: (1) executive leadership, meaning what boards of directors should do to build corporate cultures that manage cyberrisk well; (2) education and awareness, meaning what training and other mechanisms are necessary to foster a culture of cybersecurity; (3) technology, meaning how technology can improve cybersecurity protections; and (4) information sharing, meaning who within the company needs what information to enhance cybersecurity risk investments. Further, the hearing underscored the need to adopt a cybersecurity framework, such as the National Institute of Standards and Technology framework. Daniel Nutkis, CEO of the Health Information Trust (Hitrust) Alliance, testified that Hitrust has a risk management framework that provides a set of requirements tailored specifically for the health care sector. HIitrust CSF, the risk framework, is the most widely adopted privacy and security framework in health care. These sorts of frameworks and guidelines can help companies identify best practices and implement them to obtain favorable cyberinsurance policies.

Also discussed at the congressional hearing was the need for a sound actuarial database to assist in underwriting cyber policies. Currently, there is a lack of data on cyberrisk, which leads to various problems in pricing cyberinsurance policies. As Adam Hamm, commissioner of the North Dakota Department of Insurance stated at the hearing, the problem with quantifying risk without actuarial data may mean that a product is priced too low and the insurer may not have the financial means to pay claims to the policyholder. Or, the policy may be priced too high, and few businesses will be able purchase it, limiting the ability of cyberinsurance to encourage companies to implement effective security safeguards.

Another result of the lack of actuarial data is that underwriting is made on a qualitative basis (i.e., how well does the prospective policyholder appear to manage its cyberrisk, rather than what is the actuarial experience of similar risks). Specifically, Thomas Finan, who served as senior cybersecurity strategist and counsel with the U.S. Department of Homeland Security and led DHS' Cybersecurity Insurance Initiative, testified that brokers and underwriters consider two major risk management factors when assessing a company's eligibility for coverage: (1) the company's compliance with available cybersecurity standards and (2) its risk culture. Consequently, cybersecurity risk policies are not one-size-fits-all, but must be customized to the specific characteristics of each company. Not only are these policies more expensive, but from a regulatory point-of-view, they lack the desired accuracy of actuarial risk assessment based upon data from actual cybersecurity incidents.

A robust database can also be useful in assisting catastrophe risk modelers to prepare models upon which investors could rely in funding cyber bonds. The Cambridge School of Risk Management and Lloyd's of London have estimated the economic damage caused by a shutdown of the Northeast power grid as a result of a cyber attack at as much as $1 trillion. There simply is not sufficient cyberinsurance capacity to cover such risks.

Given these concerns surrounding the lack of actuarial data and the advantages of having such data, the hearing also addressed the creation of an actuarial database. Such a data repository would encourage

the voluntary sharing of information about data breaches, business interruption events and cybersecurity controls to aid in risk mitigation. Data from leading actuarial firms, such as Milliman Inc., and forensic technology firms, like FireEye Inc., together with individual insurer cyber claims experience, can be the basis for such a database. To foster data gathering, DHS organized the Cyber Incident Data and Analysis Working Group (CIDAWG), which includes brokers, underwriters, chief information security officers and other cybersecurity professionals. The group has discussed the data points that the actuarial data repository should collect, such as type and severity of incident, incident timeline, contributing causes, mitigation, costs and vendor incident reports. CIDAWG has also identified obstacles to repository sharing and potential solutions, such as assuring anonymization to prevent data from being traced to a particular contributor. Filtering out personally identifiable information will also address personal privacy concerns.

Storage of the data was also discussed at the congressional hearing. Should the data be stored with the government? While DHS is actively investigating the creation of a database, it will not own or operate the repository and has put the onus on the private sector to lead the efforts in the creation of the data repository. A possible nongovernmental location for such a database is the Insurance Services Office Inc. (ISO), which has managed insurer actuarial databases for more than four decades and provides actuarial and claims information and analytics. Wherever the data is stored, the key is to pool as much actuarial data as possible and allow equal insurer access to the data — equal access will mitigate against antitrust issues.

Other efforts to gather data include the National Association of Insurance Commissioners' (NAIC) Cybersecurity and Identity Theft Coverage Supplement. This mandatory data supplement is included in an insurer's annual financial report submitted to the NAIC. It requires that all insurance carriers writing either identity theft insurance or cybersecurity insurance report to the NAIC on their claims, premiums, losses, expenses and in-force policies. Regulators hope that with this data, they will be able to better understand the size of the cyberinsurance market and identify market trends. The first set of company filings were due April 1, 2016. Some observers are skeptical about this data call, arguing that although a data call from insurance regulators will be useful in assessing an insurer's exposure to risk of loss (and ultimately the insurer's solvency), the regulatory data collected is generally not useful for indemnity purposes.

Another effort to gather data is the Hitrust Cyberthreat XChange, which is a tool that automates the process of collecting and analyzing cyberthreats and cyberthreat indicators, and provides information that organizations can use to improve their cyber defenses.

The subcommittee hearing also addressed the potential legislative implications of cyberinsurance. Are new laws needed? Are existing laws interfering with the development of cybersecurity coverage? The hearing disclosed no immediate call for new or remedial legislation. Nevertheless, in the future, more uniformity in data breach notification laws would be beneficial so that insurers and other businesses operating in multiple states could follow the same protocols for consumer notification in the event of a data breach. The NAIC has proposed a Draft Insurance Data Security Model Law, which attempts, in part, to harmonize state laws regarding data breach notifications for insurance companies. The Draft Model Law also creates onerous insurer responsibilities in the event an insurer is hacked and personal information is accessed. The Model Law covers: Information Security Programs; Risk Management; Oversight by Board of Directors; Oversight of Third-party Service Providers; Consumer Rights Before a Breach of Data Security; Investigation of a Breach of Data Security; Notification of a Breach of Data Security; Providing Notice to Consumer Reporting Agencies; Providing Notice to Consumers; Providing Notice to Third-Party Service Providers; Establishing Consumer Protections Following a Breach of Data

Security; Powers of Commissioner; and Penalties, Hearings and Appeals. The implementation of the requirements dictated by this Model Law could potentially serve as a basis upon which a company's cybersecurity risk is assessed.

Currently — like the cyberinsurance market — the Draft Insurance Data Security Model Law remains in its infancy. Its eventual form will emerge from a long process of input, negotiations and revisions. Other initiatives, such as those to build actuarial databases for underwriters, also may require extended periods of development. As Chairman Ratcliffe suggested, many years may pass before we "see a matured cyberinsurance ecosystem that incentivizes companies of all sizes to adopt stronger cybersecurity best practices and more effective management of cyberrisks against bad actors in cyberspace." Until that time comes, more and more organizations will want to obtain cyberinsurance coverage. And they will need to meet the qualitative tests of complying with available cybersecurity standards and demonstrating that their cultures effectively manage cybersecurity risk.

—By James R. Woods, Marcus A. Christian and Jeyshree Ramachandran, Mayer Brown LLP

*James Woods is a partner in Mayer Brown's New York and Palo Alto offices and co-leader of the firm's global insurance industry group.*

*Marcus Christian is a partner in Mayer Brown's Washington, D.C., office. Jeyshree Ramachandran is an associate in Mayer Brown's Palo Alto office.*