2019 Cyber, Management and Professional Liability Conference
July 10-12, 2019
Boston, MA

THE CHALLENGE AHEAD: CYBER PRICING, U/W, MODELING AND RESERVING

I. Developments in Cybersecurity Regulations for Insurers

State Activity

On February 16, 2017, New York Department of Financial Services promulgated a final regulation on Cybersecurity Requirements for Financial Services Companies. The rule, which took effect March 1, 2017, applies to insurance companies, banks, and other financial services companies regulated by DFS, and requires these entities to adhere to new standards to protect consumers from cyber threats. The rule implements a host of new requirements, such as the Annual Risk Assessment, which is a set of written guidelines developed by covered entities identifying and evaluating risks. Covered entities must also develop written cybersecurity policies to protect against risks identified in the Risk Assessment. The regulation further sets forth specific requirements for third party service providers, and requires covered entities to development and implement Incident Response Plans, as well as several other requirements.

The National Association of Insurance Commissioners (NAIC) adopted the Insurance Data Security Model Law in October 2017. It was heavily influenced by the New York regulation and is similar in many ways, but differs in some significant aspects, such as treatment of third parties. Since each state will need to adopt its own version of the NAIC model, we can expect to see some significant variation between state requirements over the next several years, and companies will need to decide how best to approach compliance with potentially inconsistent requirements. To date, other than New York, only South Carolina and Michigan have adopted versions of the NAIC model. There are also periodic proposals for federal standards that would preempt state regulators' oversight of insurers' cybersecurity, but so far none have made significant headway.

Corporate Governance and Cybersecurity

For many years, boards often delegated creation of cybersecurity policies to management, but now cybersecurity has become an integral component of a board's role in risk oversight and overall corporate governance. Boards must ensure that appropriate mechanisms are in place to adequately protect their companies, customers, and employees from the increasing threat of cybersecurity attacks. Directors should designate and communicate regularly with the insurer's

Chief Information Security Officer ("CISO") to address any issues regarding the effectiveness of the cybersecurity program. Destructive attacks call for legal defensibility strategies and must be met with an effective business continuity plan to minimize operational downtime.

II. Underwriting Cyber Risk

Due to the great risks associated with data breaches, it is no surprise that many companies have turned to the cyber liability marketplace to help reduce their exposure. However, underwriting cyber risks is not simple or straight-forward. Because it is a relatively new risk it is not as well understood as more traditional risks, and overcoming the lack of underwriting data is a chief concern of underwriters. To try to better gauge a company's cyber preparedness, underwriters can look to National Institute of Standards and Technology (NIST) standards and the standards promulgated by other organizations. Underwriters can also analyze a company's risk by considering its financial strength, which can make a company more resilient but also more likely to be targeted.

Insurance coverages continue to evolve. Commercial general liability policies typically do not cover cyber risks, necessitating the purchase of stand-alone cyber products. These products cover various cyber risks, such as privacy liability, loss of intellectual property, business interruption, cyber extortion, and breach response/crisis management coverage. These coverages may be available as separate policies or as endorsements to existing policies.

III. Modeling Cyber Risk

Underwriters have developed new risk models to better understand cyber risks, and thus insure against them. Underwriters are able to leverage newly available data to create more accurate models to correctly price cyber risks. Modelers can better evaluate the effectiveness of technical safeguards, such as advanced firewalls, as well as the human element, which is a major source of data breaches.

Cyber risk models can also help companies evaluate risks that can be more difficult to quantify, such as business interruption. Companies are more aware of the risks involved in losing their customers' confidential personal information, but they are less cognizant of the impact of loss of use of their systems, such as cloud computing systems. Modeling can also help companies evaluate the potential damage of a breach at a major vendor and plan accordingly.