The Changing Landscape of Cyber Insurance and the Response from Regulators

FG Cyber Law Blog

August 31, 2021

Krishna A. Jani

The State of Cyberattacks

Cyberattacks are on the rise, and have significantly increased since the pandemic began in March of 2020. Remote work, coupled with bring your own device policies, have only increased vulnerabilities of businesses and individuals during this time. In fact, ransomware attacks in particular increased 300% in 2020.

The Cybersecurity and Infrastructure Security Agency ("CISA") defines ransomware as:

an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid.

Ransomware can be exorbitantly expensive because it is one of the most disruptive forms of cybercrime. Cybercriminals keep demanding larger sums and ransomware demands have increased 171% from 2019 to 2020, and continue to grow.

While small businesses account for 43% of all cyberattacks, neither large businesses nor government institutions are immune. In March 2021, for example, CNA Financial Corporation, one of the largest insurance companies in the United States, paid $40 million to regain control of its network after a ransomware attack. In another recent example, the Kaseya ransomware attack in July 2021 paralyzed as many as 1,500 organizations by compromising the tech management software. Kaseya's software serves many managed services providers so the attacks multiplied before Kaseya could effectively warn its users thereby allowing the attackers to rapidly encrypt data and demand ransoms of as much as $5 million per victim. From the rise of this type of ransomware to the SolarWinds-based cyber-espionage campaign, it is abundantly clear that cybersecurity is now fundamental to almost every aspect of modern life—from consumer protection to national security.

The Insurance Industry's Response

The rise of cyberattacks has consequently impacted the cyber insurance market. Because of the increasing regularity of ransomware attacks, the loss ratios on cyber insurance increased from an average of 42% between 2015 and 2019 to 73% in 2020. Cyber-related business interruption claims are the most sought after cyber coverage. Increasing costs are affecting premiums and scope of coverage. Insurers are also becoming more rigorous in assessing the cybersecurity of their customers and providing insurance according to that risk.

Cyber insurance plays a key role in managing and reducing cyber risk. This is a relatively new area of insurance for most insurers though cyber insurance is becoming increasingly common. In 2019, the U.S. cyber insurance market was a $3.15 billion market. By 2025, it is estimated that the market will be worth about $20 billion. Is it important to note, too, that these numbers may understate the insurance coverage of cyber risk as many policyholders submit insurance claims arising from cyber incidents under non-cyber insurance policies.

Insurance companies themselves have also come under scrutiny for their cyber hygiene. As insurance companies collect, store, and maintain a plethora of sensitive personal and business data, this is somewhat predictable and only follows the trend of increasing regulation of the cybersecurity world. In the absence of federal comprehensive legislation, states are paving the regulatory pathway and setting baseline standards of care for cybersecurity.

State Cybersecurity Regulation

At least one state has taken a proactive role in issuing a cybersecurity regulation directed towards insurance companies, and other financial institutions. As many top companies are headquartered in New York or conduct substantial business in New York, this new regulation is significant, and may have implications for how other states decide to regulate the cyber insurance market. In 2017, New York's Department of Financial Services ("NYDFS") promulgated the first cybersecurity regulation for the financial services sector, and it created a specific Cybersecurity Division in 2019. *See* 23 N.Y.C.R.R. 500.

The regulation became effective on March 1, 2017 and instituted a two-year implementation period. By March 1, 2019, all insurance companies and other financial services institutions and licensees regulated by DFS were required to have a robust cybersecurity program in place that is designed to protect consumers' private data. In addition, they were required to have a written policy or policies approved by the Board of Directors or a Senior Officer, a Chief Information Security Officer to help protect data and systems, and controls and plans in place to help ensure the safety and soundness of New York's financial services industry including encryption and multifactor authentication. The regulation sets forth certain limited exceptions, many of which still require certain cybersecurity programs and practices.

According to a 2018 DFS Memorandum, the purpose of this regulation is to bolster the financial services industry's defenses against cybersecurity attacks in order to protect the markets and consumers' private information. The regulation also requires that all entities and persons regulated or licensed by the New York State Department of Financial Services are required to file various cybersecurity notices to the Superintendent, including notifications of cybersecurity events—whether they are successful or not.

The DFS has already brought several investigations into covered entities that were thought to be non-compliant with the new regulation, with the most recent resulting in a settlement with the First Unum Life Insurance Company of America ("First Unum") and Paul Revere Life Insurance Company ("Paul Revere") on May 13, 2021. The Superintendent of DFS announced that the insurance companies agreed to pay a $1.8 million penalty to New York State for violations of DFS's Cybersecurity Regulation that caused the exposure of a substantial amount of sensitive, non-public, personal data belonging to its customers, including thousands of consumers nationally and hundreds in New York. As part of the settlement, the companies also

agreed to implement further improvements to their existing cybersecurity program to ensure that their cybersecurity controls are fully compliant with the regulation.

DFS's Cybersecurity Regulation serves as a model for other regulators both at the national and state level, as well as for industry-specific organizations, such as the National Association of Insurance Commissioners.