CARLTON FIELDS

State Insurance Regulators Target Insurers' Responses to Cyber-Attacks

CYBERSECURITY AND PRIVACY | FINANCIAL SERVICES REGULATORY | TECHNOLOGY | FEBRUARY 11, 2015

Robert B. Shapiro

Ann Young Black

Cyber-attacks are becoming increasingly common and destructive, with the recent incidents involving Sony and Anthem Blue Cross Blue Shield serving as cautionary tales. As a result, state insurance regulators are focusing on how regulated entities respond to this challenge. Consistent with this trend, the New York Department of Financial Services (DFS) announced that it will step up its oversight of regulated insurance companies within the state.

The DFS recently released its " Report on Cyber Security in the Insurance Sector ." The report summarized the findings of a DFS cybersecurity survey conducted from 2013 to 2014, and drew responses from a significant cross-section of regulated insurance companies. The survey questioned a total of 43 insurance providers (21 health insurers, 12 property and casualty insurers, and 10 life insurers) regarding their information security framework; the budget and costs associated with cybersecurity; corporate governance around cybersecurity; and their cybersecurity plans.

In addition to examining the cybersecurity programs of the insurers who participated in the survey, the DFS reviewed the enterprise risk management reports (ERM) that insurers are statutorily required to file with the DFS by April 30 of each year. These reports informed the DFS's understanding of how cybersecurity fits into an insurer's overall risk management strategy.

In the coming weeks and months, the DFS will proceed with initiatives to help regulated insurers strengthen their cybersecurity protections. These include implementing enhanced regulations that require institutions to meet heightened cybersecurity standards; researching possibly stronger third-party vendor warranties and representations to insurers; and including cybersecurity assessments as part of the DFS's examination process.

Potential DFS Actions

Given that ERM reports must be filed with the DFS by April 30 of each year, and that Own Risk and Solvency Assessment (ORSA) reports must be filed by December 1 of each year, it is extremely likely that any new requirements regarding either (i) insurers' cybersecurity programs or (ii) disclosures related to insurer-issued cyber-insurance policies will be accomplished through amendments to the New York regulations that govern ERM and ORSA reports (11 NYCRR Part 82). Enhanced requirements may include mandatory, regular briefings of each insurer's CEO on the subject of information security. The DFS survey found that only 14 percent of CEOs receive monthly information security briefings from their companies' employed or retained information security personnel.

DFS Superintendent Benjamin Lawsky also indicated that his office is considering new regulations that would address how financial institutions work with third-party vendors. Mr. Lawsky stated, "The regulations we're considering include getting warranties from third party vendors about their security protections." The Superintendent also stated that, "The fear we all have is for a catastrophic attack to occur that would cause us to look around and ask why we didn't have these regulations in place."

Compare these efforts to the Connecticut Insurance Department's new requirements in its examinations of insurers, mentioned in our recent blog post. Connecticut's Financial Analysis unit now routinely includes analysis of each insurer's cybersecurity protocols and procedures, including incident reporting and escalation procedures, backup and recovery procedures, and penetration testing. The Connecticut Insurance Department also monitors the increased solvency risk that issuing cyber insurance entails.

Impact of DFS Examination Procedures on Insurers

How will the new DFS examination procedures affect insurers? For one thing, they may affect consumer behavior. The DFS's consumer alert regarding the Anthem data security breach, for example, recommends that consumers (i) monitor their credit card and bank statements, monthly bills, and other financial statements for transactions they did not make; and (ii) check their credit score for sudden changes. Further, in its cybersecurity report the DFS, perhaps conceding the inevitability of data breaches, discusses testing of insurers' cybersecurity disclosures. Such consumer alerts and disclosures may make consumers lose confidence in the safety of their personal data. As a consequence, insurers would be wise to both increase their cybersecurity efforts as necessary, and to also consider implementing a proactive approach that informs their consumers of their cybersecurity efforts.

We anticipate new cybersecurity requirements from the DFS and other insurance departments, as well as pronouncements from the National Association of Insurance Commissioners Cybersecurity (EX) Task Force, and plan to report on them as they become available.