GreenPoint> Financial
www.greenpoint.financial

REGULATORY PERSPECTIVES
June 27th, 2017
Volume - 12
Series - 1

NAVIGATING NEW CYBERSECURITY RULES: IMPACT ON INSURANCE COMPANIES

By **William Anderson, Esq.**
Managing Director, GreenPoint Law & Compliance

The New York Department of Financial Services (DFS) has issued cybersecurity requirements for financial services companies (cyber rules) that recently went into effect March 1, 2017.

The cyber rules, codified at 23 NYCRR §500, require insurance and insurance-related companies as well as brokers, agents and adjusters licensed in New York to assess their specific cyber risk profiles and design cybersecurity programs that address such risk in a "robust fashion."

There is no doubt that cyber risk is real, and the DFS has taken steps to manage it by way of the regulation. Still, the cyber rules could prove to be problematic, particularly for licensed brokers, agents and adjusters. To these individuals – and the insurance and insurance-related companies that employ or utilize them – there are several things to keep in mind.

Entities Affected

The cyber rules apply to any "covered entity," which the regulation defines as "any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, Insurance Law or Financial Services Law."

This means that in addition to insurers, individual brokers, agents and adjusters have a new mandate. What this requires – and pursuant to §500.02(a) of the cyber rules – is that these individuals must "maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of [their] Information Systems."

Depending upon a covered entity's size and reach, the following broad requirements (among others) imposed by the cyber rules may be rather burdensome:

- Establishing a cybersecurity program;
- Adopting a cybersecurity policy;
- Designating a Chief Information Security Officer (CISO);
- Implementing privacy policies and procedures for third-party service providers;
- Conducting periodic risk assessments; and
- Notifying the Superintendent within 72 hours of determining the occurrence of a cybersecurity event that has a reasonable likelihood of materially harming any material part of the normal operations of the covered entity, or if notice would need to be provided to another regulatory body.

Achieving Compliance

There are a lot of new requirements for a broker, agent or adjuster to digest. First, a covered entity should appoint a CISO or use a third-party to fill the role. Thereafter, it is required that an initial risk assessment be conducted to identify breaches in security followed by the adoption of corresponding policies and procedures and implementation of necessary security overhauls to bridge any gaps. All of this would be bolstered by appropriate staff education or training. Third-party vendor security also needs to be addressed.

Ultimately, the key to complying with the cyber rules is the implementation of a "living, breathing" cybersecurity program that can adapt to ever-changing security concerns, including new technologies and threats. This program must be one that can be refined when new issues arise and risks are identified.

What will not withstand governmental audit is a set of written policies that sits on a shelf and gathers dust. Likewise, policies and procedures that merely serve as restatements of the law will be ineffectual. Indeed, the likelihood of an enforcement action decreases proportionally to level of diligence exercised in compliance. Licensed brokers, agents and adjusters must act accordingly.

Who is Exempt?

The cyber rules could create a burden on many individual brokers, agents and adjusters doing business in New York, particularly the "mom and pop shops" that lack the resources of the more substantial and sophisticated industry players. Nevertheless, those licensed by the DFS must comply with the regulation in its entirety unless they are exempt, which could be a possibility depending upon a covered entity's size or annual revenue, among other things. The cyber rules reduce, but do not entirely eliminate, the onus of compliance in certain situations as follows:

- A Covered Entity with (1) fewer than 10 employees (including independent contractors) located in New York; (2) less than $5 million in gross annual revenue stemming from New York in each of the past 3 years; or (3) less than $10 million in year-end total assets, including assets of all affiliates, must still have a cybersecurity program and policy, conduct risk assessments, implement privacy policies and procedures for third-party service providers and notify the Superintendent, but are exempt from most of the other requirements.
- An employee, agent, representative or designee of a covered entity, who is itself a covered entity, does not need to develop its own cybersecurity program to the extent it is covered by the cybersecurity program of the covered entity.

This could be a positive sign for some, but there is a catch. Those who qualify for an exemption must file a Notice of Exemption form, as set forth in the cyber rules, within 30 days of determining that an exemption applies. The takeaway: to be relieved of at least some of the requirements of the cyber rules, qualifying brokers, agents and adjusters must submit the requisite paperwork. The failure to do so will subject them to whatever penalties ultimately apply.

It would be good practice for insurance companies and agencies to alert their potentially exempt licensees of the filing requirement.

The Role of Legal Counsel

Qualified legal counsel can be of great help in managing the cyber rules. Not only can it provide the framework for initial and periodic risk assessments mandated by the DFS, but legal counsel can also facilitate continuing compliance and create the attestation trail necessary to demonstrate adherence to the regulation.

Likewise, legal counsel can help to evaluate and fulfill reporting requirements in the event of a cybersecurity breach, and assist in adopting associated reporting protocol. Additionally, an insurance regulatory lawyer can design a cybersecurity curriculum for staff education and training, which can curtail human error, assure proper device management and communicate disciplinary consequences for information or protocol breaches. Finally, legal counsel can advise insurance companies and their licensees on the exemption parameters and procedures built into the cyber rules.

Additional Questions: Stay Tuned … Stay Vigilant

How will the cyber rules be monitored? What will be the measure of non-compliance? What control protocols other than encryption will authorities accept to withstand enforcement action? What analysis will need to be conducted to determine the actual need for reporting? Is it realistic for smaller entities to comply?

These are all questions that have been raised, and ones without complete answers – yet. Covered entities must nevertheless take prompt action to conduct a risk assessment and establish policies and procedures.