Insurance Companies Take Note: Another Compliance Concern For Your Cybersecurity "To Do" List

Amundsen Davis Data Privacy & Security Alert
April 26, 2019

If you are an insurance provider, you are already awash in regulatory quagmires. Now, you can add one more. In fact, if you don't have a comprehensive data privacy and security plan in place, then you may not be in compliance with quickly-expanding cybersecurity regulations spreading across the country.

Last year, New York was the first state to enact regulations that required insurers to establish a comprehensive data privacy plan to protect their sensitive and confidential information from hackers and other unauthorized access. New York's cybersecurity regulations apply to any insurer licensed to sell insurance in the state of New York. That's (already) a broad group.

Other states are getting in line. Specifically, the state legislatures in South Carolina, Michigan and Ohio have all recently enacted cybersecurity legislation applicable to licensed insurance sellers in their states. Within the next two years, *all* insurance companies licensed in these states must be in compliance with state specific rules; they must file documentation certifying this compliance—unless they qualify for an exemption.

In contrast to the background to New York's cybersecurity laws, these three states adopted, in substantial part, the National Association of Insurance Commissioners (NAIC) Data Security Model Rule. The NAIC's model rules are an acknowledgement that insurance companies often store and maintain large amounts of personal information about clients, and as a result, should proactively take steps to protect that information. The Model Rule contains several provisions which insurers must comply with, including, for example: a comprehensive data security program; designation of a Chief Information Technology Officer; regular training for employees on cyber-risks; and, a data breach response plan.

It is expected that other states will soon follow. The NAIC drafted its model rule with the hope that, in the *next five years*, all 50 states will have enacted this model rule in some form. With looming compliance requirements—but, really, ones to which every company should adhere for best business practices—insurance companies should take steps, today, toward the following:

PROFESSIONALS

Molly A. Arranz
Partner

John Ochoa
Partner

RELATED SERVICES

Cybersecurity & Data Privacy

1. Review whether you do business in a state that has enacted cybersecurity regulations;
2. Analyze whether your company qualifies for any exemptions from requirements in those state regulations;
3. Partner with your cybersecurity advisors and attorneys to audit your current information systems to create a cybersecurity plan; and,
4. Consider—and calendar—compliance and reporting deadlines in each particular state.

Insurance Companies Take Note: Another Compliance Concern For Your Cybersecurity "To Do" List