Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# Insurers Given Path To Avoid Data Security Liability

By **Allison Grande**

*Law360, New York (April 21, 2015, 10:24 PM ET)* -- The National Association of Insurance Commissioners last week rolled out guidance outlining the data security safeguards that regulators expect insurers to implement, a useful tool that will help codify existing best practices and provide insurers with clarity on regulators' increased — and often inconsistent — scrutiny.

In new regulatory guidance adopted Thursday, NAIC's cybersecurity task force laid out 12 principles meant to serve as a foundation for the protection of sensitive consumer information held by insurers and insurance producers and to guide regulators that oversee the insurance industry.

"Hopefully, given that insurers tend to be a repository for large amounts of valuable protected data, they already are taking cybersecurity and data privacy seriously," K&L Gates LLP partner Roberta Anderson said. "But NAIC's recent guidance may prove to be another useful tool for moving toward an elevated state of cybersecurity."

While the principles reflect best practices that insurance companies should be undertaking already, especially in light of recent high-profile data breaches at health insurers such as Anthem Inc. and Premera Blue Cross, the guidance from the state regulators for the first time provides insurers with clear rules of the road for cybersecurity, attorneys say.

"The principles don't introduce any brand-new concepts, but not everyone in the insurance industry is necessarily focused on those concepts, so the guidance is a good way to get regulators and regulated entities all focused on the same core principles for addressing the cyber challenges that threaten the industry," Locke Lord LLPpartner Ted Augustinos said.

According to the principles, industry members need to take steps to safeguard confidential, personally identifiable consumer information, put in place incident response plans and employee training programs, ensure third parties and service providers have controls to protect sensitive data, and incorporate cybersecurity risks into their enterprise risk management process.

Although such safeguards are becoming increasingly commonplace in a wide range of industries, the guidance delivers a warning shot to insurers that ignorance of these best practices is no longer acceptable, according to attorneys.

"It's likely that very soon we're going to see data security rules codified in statues either at the federal or state level, given the publicity and momentum and negativity against those who don't fall in line with best

practices, and the insurance industry appears to be trying to get ahead of that," Kaufman Dolowich & Voluck LLP technology practices group vice chair Mark Mao said.

The NAIC guidance made a push for state regulators to provide "appropriate regulatory oversight," such as conducting "risk-based financial examinations and/or market conduct examinations regarding cybersecurity."

"Practical application of the principles remains to be seen, but there is a strong indication that insurance regulators intend to increase oversight of insurers' cybersecurity practices," Pillsbury Winthrop Shaw Pittman LLP partner James Bobotek said.

While state regulators have had the power to police insurers' data security and privacy practices since the passage of the Gramm-Leach-Bliley Act in 1999, enforcement has been spotty and inconsistent, attorneys say.

"Although insurers have been bound by GLB, it's fair to state that state regulators have not been focused on the statute's security rule, and we haven't really seen enforcement around that," BakerHostetler privacy and data protection team co-leader Gerald Ferguson said.

But with the release of the regulatory guidance, the NAIC has brought renewed attention to the issue and updated expectations for how insurers should be protecting sensitive data from increasingly sophisticated cyberthreats.

"While the principles may not result in a completely uniform approach by regulators, which is a very high goal, they will at least result in coherence, since all the regulators will be starting from the same place in developing a regulatory scheme that fits those 12 specific principles," Augustinos said.

Heeding the principles put forth by the NAIC is likely to help insurers avoid the imminent increase in state regulatory scrutiny and dodge claims advanced by other regulators such as the Federal Trade Commission or by consumers suing after a significant data breach, attorneys say.

"The best-prepared companies will be able to state that they have used reasonable efforts to prevent a cyberattack and have taken reasonable efforts to protect personally identifiable information, which accordingly will lead to the measure of damages, if any, being significantly less," said James Woods, the co-leader of Mayer Brown LLP's global insurance industry group.

However, implementation of the principles won't necessarily be a cakewalk for companies. The principle that data security plans be "flexible, scalable, practical and consistent with nationally recognized efforts" such as those embodied in the voluntary framework the National Institute of Standards and Technology issued last year could be problematic, attorneys point out.

While this principle gives insurers flexibility and increases the likelihood that the data security plans they build will be appropriately tailored to their specific vulnerabilities, it strips away the "check-the-box" approach favored in other regulatory schemes, where companies need only to ensure that they are meeting certain safeguards to achieve compliance.

"It's going to be a challenge to the chief information security officer and chief technology officer to not take comfort in the check-the-box approach and really conduct a risk assessment that truly helps them understand the risk, and be creative and innovative in finding solutions to the challenge they face," Ferguson said.

Attorneys also singled out as potential stumbling blocks the requirements that insurers guarantee the data security of the third parties they do business with and that they use an information-sharing and analysis organization to stay informed regarding emerging threats or vulnerabilities.

“Perhaps the most significant part of the guidance is the requirement that insurers use an information sharing organization,” Shook Hardy & Bacon LLP data security and privacy practice co-chair Al Saikali said. “It is unusual that such a practice, although recommended and often times beneficial, be mandated.”

--Editing by Kat Laskowski and Kelly Duncan.

---