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

Privacy 'Bill Of Rights' To Boost Demand For Breach Coverage

By **Allison Grande**

Law360, New York (October 23, 2015, 5:58 PM ET) -- The insurance industry's standard-setting body recently introduced a privacy bill of rights that would ramp up insurers' cybersecurity obligations to policyholders, a development that coincides with regulators' increased scrutiny of data security practices and is likely to expand the fledgling cyberinsurance market.

Looking past industry objections, a task force for the National Association of Insurance Commissioners on Oct. 14 adopted a cybersecurity “bill of rights” that would entitle policyholders to be notified within 60 days of a data breach and get one year of free credit monitoring paid for by the insurer or agent hit by the breach. Consumers would also have the right to be informed of their insurer's privacy policy and what kind of data their insurer holds, and to expect the insurer to take appropriate measures to protect the information.

The proposal, combined with increased scrutiny by federal and state lawmakers and regulators such as the U.S. Department of Justice and the Federal Trade Commission, will contribute to the growing demand for cyberinsurance, including among insurers themselves that will need to ensure that their own coverage addresses evolving regulatory demands, attorneys say.

"The cyberinsurance industry that now exists but didn't exist 15 years ago came into existence because of regulation," John Mullen, the chair of the data privacy and network security practice at Lewis Brisbois Bisgaard & Smith LLP, told Law360. "Companies are collecting the same data as they were in the 1980s and 1990s, but they now have increased exposure because of the new laws and regulations being rolled out."

The increased demand for cyberinsurance fueled by regulatory involvement is also likely to aid insurers and underwriters, which are scrambling to gather the data that they need to better set rates and devise coverage options, attorneys say.

"Cyberinsurance remains the Wild West of insurance," said Scott Godes, an insurance recovery partner and co-chair of the data security and privacy practice at Barnes & Thornburg LLP. "But with the changing regulatory environment, we're starting to see changing prices and the market opening up and tightening up."

The NAIC’s proposed bill of rights is the latest in a long line of legislative and regulatory developments that have brought increased attention to the issue of cyberinsurance and have had a profound impact on the growth and evolution of the industry, attorneys say.

“The cyber insurance market over the last decade has done a good job of expanding the scope of cyber and privacy coverage to meet and address the exposures presented by a remarkable proliferation of state and federal cybersecurity and data privacy-related laws, and increasingly heightened regulatory scrutiny — and it has done so at very competitive rates,” K&L Gates LLP partner Roberta Anderson said.

Agencies including the DOJ and the U.S. Securities and Exchange Commission in recent months have floated their own industry-specific guidance on what constitutes a strong cybersecurity preparation and response plan. Even insurance authorities have been active, with an NAIC task force revealing in April adopting a set of 12 guiding principles for effective cybersecurity that were meant to provide the insurance industry with insight into the types of safeguards regulators expect insurers to have in place to protect consumers' sensitive data from unauthorized disclosure.

Recent legal decisions, most notably the Seventh Circuit’s revival of a data breach class action against Neiman Marcus and the Third Circuit’s rejection of Wyndham Worldwide Corp.’s claims that the FTC doesn’t have the authority to regulate data security, have also operated to embolden federal and state authorities to become more involved, attorneys say.

“In fact, you may see FTC inquiries of some companies about their cyber practices even where no data breach has occurred [in light of the Third Circuit’s ruling],”Anderson Kill PC shareholder Joshua Gold said. “I expect this will lead some insurance companies to review their cyber insurance policy fine print and adjust it to expressly cover the risks and lead yet others to limit it.”

The privacy bill of rights for the insurance industry builds on the trend of heightened involvement by outside forces, while highlighting the growing divide among the cybersecurity standards currently in place at state and industry-wide levels that makes pricing and crafting cyberinsurance options tricky, attorneys say.

The industry’s main criticism with the proposed bill of rights hinges on the perception that it imposes notification and response obligations that go well beyond the requirements of the 47 state breach notification laws that currently exist, most of which do not have a reporting clock or the mandate to offer credit monitoring.

“The big impact on insurers is that the state regulators have determined that they want to make a nationwide standard for insurers that is higher than what is applicable in many states, which would increase their responsibilities and potential exposure,” Hunton & Williams LLP partner Lon Berk said.

The 60-day notice requirement in particular may present a difficult challenge for insurers, given that recent research has indicated that the average breach is not discovered until more than 200 days after it occurs, Mayer Brown LLP global insurance industry group leader James Woods noted.

“There’s a fair amount of industry concern related to the fear that the bill of rights would create some expectations that might not be able to be fulfilled,” Woods said.

While the proposal is only guidance and not legally binding, it comes from a highly-influential body that state regulators usually draw inspiration from, making it likely that insurers will work to comply with the bill of rights in order to avoid scrutiny from regulators as well as dissatisfied consumers in the event of a breach, attorneys say.

“The proposed bill of rights, if adopted, is likely to increase scrutiny of regulated entities’ privacy policies, … [which] in turn will potentially increase regulatory proceedings in the event of actual or alleged noncompliance, as well as consumer litigation,” Sedgwick LLP partner Laurie Kamaiko said. “The entities that this [bill of rights] would apply to often have cyberinsurance themselves, and with increase in exposure, there may be an increase in the cost of insurance that is impacted by that exposure.”

The lack of clarity and certainty posed by having a separate set of cybersecurity rules for the insurance industry could also affect pricing and offerings, attorneys say.

“When there are actions like the NAIC bill of rights, which in some cases have differences and gaps and consistencies with existing requirements, those kind of things can increase uncertainty and cost,” Locke Lord LLP partner Theodore Augustinos said. “While everyone is working hard with good intentions to collect more data and make the situation better and safe from a cyber standpoint, there’s a difficulty when different standards are being created that can make coverage increasingly expensive.”

Given that the insurance market relies on the spreading and pooling of risk, the growth of industry standards and regulatory involvement, despite the uncertainty the actions may cause, is likely to generate a wealth of data that will only help the market grow and gain a voice of its own, attorneys say.

"You always hear in the market that there is not enough data, but I think the market is maturing and the larger players are getting more data about their own books and clients that is allowing insurance coverage to be more developed, and I would expect that to continue in the future," Berk said.

--Editing by Kelly Duncan.
