Client Update
NAIC Cybersecurity Model Law Moves One Step Closer to Approval

On August 7, 2017, the National Association of Insurance Commissioners Cybersecurity (EX) Working Group adopted a new and presumptively final draft of the group's Insurance Data Security Model Law.

WHAT WOULD THE MODEL LAW REQUIRE?

The Model Law would apply to essentially all entities licensed in states that adopt it. A covered company would be required to adopt a flexible, risk-based cybersecurity program. Key provisions include:

- Implement an Information Security Program that reflects the size, complexity, and nature of the company's business;
- Conduct regular risk assessments;
- Manage risks by implementing appropriate safeguards;
- Involve the board through annual briefings on cybersecurity; and
- Maintain and test an Incident Response Plan.

Companies would be required to certify compliance annually to the insurance commissioner. They also would have to notify the commissioner of any confirmed cybersecurity incidents meeting certain criteria. The commissioner would be authorized to examine or investigate.

DOES THE MODEL LAW HAVE THE FORCE OF LAW YET?

No. The working group's adoption of the Model Law is an interim first step. The Model Law must be adopted by two other committees within the NAIC.

States will be free to adopt the Model Law, or not. Legislatures could enact the law, or insurance commissioners could adopt regulations that track the Model Law. States could adopt the Model Law wholesale; adopt it in modified form; or ignore it. It remains unclear which states will do which.

If strength of support within the NAIC is any indication, then the Model Law seems likely to be adopted in some form by some states. Prior to adoption by the Working Group, four drafts of the Model Law were released for comment. The Model Law was then adopted with broad consensus by the Working Group, where only three states did not vote for adoption.

HOW SHOULD INSURERS RESPOND TO THE MODEL LAW RIGHT NOW?

We encourage our clients and friends to study the Model Law carefully, and to consider planning for compliance with the substance of the Model Law whether or not it is eventually adopted by the states:

- The practices mandated by the Model Law track what are widely regarded as best practices in the information security community. It couldn't hurt to think about following them, as many companies already do.
- Similar requirements are taking hold in the law more broadly, often framed by courts and regulators in terms of a duty to maintain "reasonable" or "appropriate" cybersecurity measures. Even if your company does not become directly subject to the Model Law, the terms of the law may still be a useful guidepost for compliance more generally.
- Many insurers are already subject to the New York Department of Financial Services cybersecurity regulation, which is a close cousin of the Model Law. The DFS regulation took effect in March. Both it and the Model Law require companies to have an information security program, to know their cybersecurity risks via a risk assessment process, and to use appropriate controls to reduce these risks. By the terms of the Model Law, companies in compliance with the DFS regulation are deemed to also be in compliance with the Model Law.

* * *

For questions or assistance, please do not hesitate to call on any member of the Debevoise Cybersecurity & Data Privacy global practice team.

NEW YORK

Eric R. Dinallo
edinallo@debevoise.com

Jeremy Feigelson
jfeigelson@debevoise.com

Jim Pastore
jjpastore@debevoise.com

Julia Shu
lshu@debevoise.com

WASHINGTON, D.C.

Luke Dembosky
ldembosky@debevoise.com

Naeha Prakash
nprakash@debevoise.com