New York Law Journal

NEW YORK LAW JOURNAL SPECIAL REPORT

Cybersecurity

An ALM Publication

WWW.NYLJ.COM

VOLUME 257—NO. 106

MONDAY, JUNE 5, 2017

New **DFS Cybersecurity Regulations** Are Here: Will Your **Insurance** Protect You?

BY ANDREW M. REIDY AND JOSEPH M. SAKA

New York always is at the vanguard of innovation when it comes to making people's lives better with such inventions as air conditioning, credit cards and, not to be forgotten, the Cronut. This year, New York again is at the forefront of change. On March 1, 2017, the New York Department of Financial Services (DFS) issued "first-in-the-nation" cybersecurity regulations. 23 NYCRR 500. Governor Andrew Cuomo stated that the regulations will help assure that the financial services industry "has the necessary safeguards in place in order to protect themselves and the New Yorkers they serve from the serious economic harm caused by these devastating cyber-crimes."

SHUTTERSTOCK

The regulations impose stringent requirements on all businesses regulated by DFS, including banks, insurers, and other financial services companies. Subject entities, for example, will be required to appoint a chief information security officer, conduct regular cyber testing, provide cybersecurity awareness training, and implement multi-factor authentication. By August 28 of this year, covered businesses are required to meet certain of the regulations. By Feb. 15, 2018, companies are required to file a certification confirming

ANDREW M. REIDY *is a partner and* JOSEPH M. SAKA *is counsel in Lowenstein Sandler's insurance recovery group.*

compliance with the regulations. By March 2019, companies will be required to look beyond their own practices to ensure that vendors and third-party contractors also are meeting certain standards.

The requirements are not optional. Compliance with regulations, however, does not immunize businesses from potential liability. Industry experts are expecting that the new regulations may spawn even more claims relating to compliance.

Sophisticated businesses recognize that their insurance policies can help them manage this risk. But planning ahead is critical. As companies consider their readiness to meet the DFS cybersecurity regulations, they also should be considering the sufficiency of their insurance policies. From an insurance perspective, there are at least four steps every New York business should be taking right now to stay ahead of the curve:

Understand Your Potential Liability

Step one in assessing the adequacy of your organization's insurance is understanding your key risks. One size does not fit all. For some, there will be exposure to liability from storage of payment card information. For organizations with many employees, confidential information regarding employees will be a concern. Whatever the case, make sure you identify likely risks or exposures. By doing this on the front end, you can both make sure your insurance policies are properly structured and save money by avoiding premiums for coverage you do not need.

With the new DFS cybersecurity regulations, it is likely that companies will be exposed to altogether new claims. For example, with the certification requirement, businesses and their directors and officers may be exposed to lawsuits (including securities lawsuits) based on false or incomplete certifications to the DFS. As another example, state regulators may bring regulatory actions against companies for failure to comply with the regulations. In the event of a data breach, businesses also should expect that consumers and affected parties will cite any failure to comply with the DFS regulations when bringing claims. Companies should have protection from these potential liabilities in their policies.

After obtaining an understanding of key exposures, one needs to review insurance policies to assess the scope of coverage.

Understand Which Policies May Respond

After obtaining an understanding of key exposures, one needs to review insurance policies to assess the scope of coverage. Where should you look? Everywhere. Some coverage may be available under "traditional" insurance policies, such as directors and officers (D&O) liability insurance policies, errors and omissions insurance policies, general liability insurance policies, and fidelity insurance policies. For instance, one prevalent risk recently has been ransomware attacks, and coverage for the "ransom" payment or consequent business interruption losses may be covered under fidelity bonds or crime policies. D&O insurance may cover securities lawsuits based on alleged misrepresentations regarding cyber preparedness.

If your company has not purchased a stand-alone cyber insurance policy yet, now is a good time to start looking to do so. Although the market is still developing, in recent years, the insurance industry has done a much better job responding to consumer demand. The underwriting process remains tedious, but it is less burdensome than it once was. With a more extensive loss history, insurers also are able to better price cyber insurance policies and anticipate likely claims.

Ensure Policies Are Properly Structured

You make a telephone call and find out that you have a cybersecurity policy in place. You can rest easy, right? Unfortunately, cyber insurance

policy forms are largely untested in the courts. Many companies are using sophisticated policyholder counsel to review policy forms on a flat fee basis to look for gaps in coverage. Armed with information regarding your main risks, your insurance broker and counsel can help you avoid problematic language that might create gaps in coverage.

All insurance policies have exclusions, but all policies are not identical. In many instances, insurance companies may be willing to modify or eliminate exclusions. For example, one should avoid exclusions with prefatory language like "based upon, arising out of, or in any way relating to." Insurers commonly assert exclusions with this language broader than what was intended. Further, some cyber insurance policies contain an encryption exclusion barring coverage for loss resulting from unencrypted devices. Unless you know your employees do not use unencrypted devices (at home or in the workplace), such exclusions could be a significant coverage restriction. Finally, some policies contain exclusions for loss caused by "any governmental or public authority." With attacks by governmental entities becoming more prevalent, these exclusions should be avoided.

Other terms and conditions also need to be considered. For example, there may be limitations hidden in the "Definitions" section of the policy. Moreover, one should beware of sub-limits. Although insurers sometimes market these sub-limits as benefits, in many instances these limits actually reduce the amount of coverage that may otherwise be available.

The differences in policy forms often are subtle. But these subtle differences can have huge ramifications on coverage. Therefore, it is all the more important to work with experienced professionals who can identify gaps or limitations in coverage.

Have a Plan in Place

Prepared companies understand they need to have a plan *before* a loss takes place. Already, many companies have retained a SWAT team—consisting of a cyber coach, attorneys, forensic accountants, and engineers—to take action in the event of a breach. Insurance needs to be part of the plan.

In the aftermath of a breach or a loss, you should have coverage counsel in place that will assess which insurance policies may respond, provide notice to applicable insurers as required under the policies, and document corporate losses in a manner that is likely to be paid. With a small investment on the front end, experienced coverage counsel can help you avoid likely traps that can result in litigation or a total loss of coverage. The worst case scenario is both to have a cyber loss and fail to properly access and maximize your insurance.

Conclusion

The DFS cybersecurity regulations give every business the opportunity to assess its cybersecurity. Regardless of preparedness, however, no company is immune from an attack. In the words of former FBI Director Robert Mueller: "There are only two types of companies: those that have been hacked, and those that will be." As covered businesses work to meet the deadlines of the new cybersecurity regulations, they also should consider whether they have taken steps to secure insurance that will protect them.

Reprinted with permission from the June 5, 2017 edition of the NEW YORK LAW JOURNAL © 2017 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382 or reprints@alm.com. # : 070-06-17-08