Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

New Cybersecurity Regulations for New York Insurers and Banks

Law360, New York (October 13, 2016, 12:15 PM EDT) --


Alice T. Kane


Philip A. Goldstein

Over the last few years, the financial services industry has been recognized by the New York Department of Financial Services (NYDFS) as a significant target of cyberthreats. While the frequency and cost of data breaches in the insurance industry is less than that of banks, healthcare data can, in fact, be more valuable over time than credit card information. For instance, insurance companies store data on where the insureds live, spouses' names and serious (or embarrassing) medical conditions. Last year, the Anthem data breach resulted in the information of millions of individuals being compromised. On the same day, Premera Blue Cross hackers are estimated to have stolen up to 11 million customer records. While health insurers store credit card and Social Security numbers, what may be even more concerning is the possibility of hackers accessing the medical records of individuals. In both of the aforementioned instances, rather than penetration by isolated hackers, it is possible that a state actor was involved since both Anthem and Premera are huge providers to government workers.

Initially, 43 insurance companies were surveyed, comprising over $3.1 trillion in assets and millions of insureds, for the NYDFS to gain industry insight. In the report that followed,[1] the NYDFS indicated that although the insurance industry may not be targeted as frequently as banks or hospitals, there remains growing concern. Based on their findings, the NYDFS issued a first-ever cybersecurity regulation on Sept. 13, 2016. This new cybersecurity regulation[2] applies to all insurance companies and banks (the covered entity), including some of the largest foreign global institutions, regulated by the NYDFS. As the first regulator to issue cybersecurity guidelines, the NYDFS has set a standard for other state, federal and global regulators.

1. Cybersecurity Program

Each covered entity must establish a cybersecurity program and policies to ensure the confidentiality, integrity and availability of its information systems and nonpublic information. A chief information security officer (CISO) must be designated and he or she is responsible for implementing, overseeing and enforcing the program and policies. The cybersecurity policy must be in writing, must be approved by a senior officer and, at a minimum, must address specific enumerated areas, such as system and information security, customer data privacy, and vendor and third-party service provider management. The board of directors is required to review the policy at least yearly. The CISO must develop biannual reports for the board of directors and for the NYDFS superintendent, if requested.

2. Certification Requirement

An annual certification that must be submitted annually to the superintendent by January 15 is required, stating that the covered entity is in compliance. All records, schedules and data supporting the covered entity's certification must be maintained for five years and available for examination by the NYDFS.

3. Incidence Response Plan

The covered entity must establish an incidence response plan to respond to or recover from a cybersecurity breach or attempted breach. If there is such an incident affecting normal operations or involving nonpublic information, the superintendent must be notified within 72 hours. The superintendent must also be notified within 72 hours if the covered entity has identified any material risk of imminent harm relating to its cybersecurity program, and such material risks must be included in the annual certification report.

4. Cybersecurity Program Minimum Requirements

Minimum requirements for the cybersecurity program include encryption and timely destruction of nonpublic information, general personnel training and monitoring of authorized users, annual penetration testing, quarterly vulnerability assessments, audit trail systems and limited information access. Furthermore, the program must provide written procedures, guidelines and standards, which the CISO must review, assess and update annually, to ensure the security of both internally and externally developed applications. Risk assessments are required on an annual basis. Qualified personnel must be in place to manage the risks and core cybersecurity functions. These key cybersecurity personnel must attend regular cybersecurity updates and training sessions while also taking steps to stay abreast of ever-changing cybersecurity threats and countermeasures. Alternatively, a covered entity may utilize a qualified third party to meet this requirement.

5. Third-Party Information Security Policy

A written third-party information security policy is required to ensure the security of information systems and nonpublic information accessible or held by third parties doing business with a covered entity. A required due diligence process will evaluate the third party's cybersecurity practices, and ongoing assessments will determine the continued adequacy of such practices. At a minimum, third-party service provider contracts must include provisions for multifactor authentication, encryption of nonpublic information, prompt notice of a cybersecurity breach or attempted breach and the right to perform cybersecurity audits. The third party must provide representations and warranties that the services or products provided are free of viruses, trap doors, time bombs and any other mechanism that would impair the security of the covered entity's information systems or nonpublic information.

6. Multifactor Authentication

Multifactor authentication must be utilized by covered entities for any individual accessing its internal systems or data from an external network. Multifactor authentication is also required for certain access to nonpublic information. This requirement can be met by verification of at least two of the following: knowledge factors, such as a password; possession factors, such as a token or text message on a mobile phone; or inherence factors, such as a biometric characteristic.

7. Effective Date

The regulation is subject to a 45-day notice and public comment period before final adoption. If and when approved, covered entities have 180 days from the effective date to comply, unless otherwise specified. There are limited exceptions for smaller covered entities.

8. Recent National and International Insurance Regulatory Activity

As noted, the NYDFS, as a first mover, has set a standard for other key regulators focused on this key issue. This spring, the International Association of Insurance Supervisors (IAIS) issued an extensive white paper on cyber-risk in the insurance sector.[3] According to the paper, the IAIS Financial Crime Task Force is considering whether its insurance core principle on countering fraud in insurance, known as ICP 21, should be extended to specifically address elements of cybersecurity putting a global spotlight squarely on this growing risk.

Last year, the National Association of Insurance Commissioners (NAIC) adopted the 12 Principles for Effective Cybersecurity Insurance Regulatory Guidance.[4] Most recently, the development of the Insurance Data Security Model Law was much discussed at the 2016 NAIC summer meeting. The proposed NAIC Insurance Data Security Model Law will establish exclusive standards for data security and investigation and notification of a breach of data security applicable to insurance companies.

The initial draft of the NAIC model law was revised after receiving extensive comments from trade associations, market participants and regulators. The trade association speakers' main criticism was that the model law would not result in uniform breach response requirements. Different trade associations insist that there is no need for a model law if it does not provide for exclusive standards consistently applied that result in uniform consumer protection among states. The NAIC comment period just closed on September 16, making it apparent that cybersecurity remains an open topic of discussion for the NAIC.

Conclusion

Adoption of the required cybersecurity program should be a priority for any covered entity in New York state. The number of cyberevents and the estimates of their potential risk have been steadily increasing, and the NYDFS believes it is vital for all covered entities that have not yet done so to move swiftly adopt and implement a robust cybersecurity program. Since senior management, the CISO and the board of directors are now legally responsible for their covered entity's cybersecurity program and its annual certification confirming compliance, the onus is wholly on them to take prompt action on this key issue.

—By Alice T. Kane and Philip A. Goldstein, Duane Morris LLP

Alice Kane, a partner with Duane Morris LLP in New York, practices in the area of insurance law. Kane formerly served as the group general counsel at two Fortune 100 insurers, Zurich Insurance Group and New York Life Insurance Company.

Philip Goldstein, an associate with Duane Morris LLP in New York, practices in the area of real estate, including commercial and residential purchases and sales, leasing and finance, as well as corporate transactions.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] http://www.dfs.ny.gov/reportpub/dfs_cyber_insurance_report_022015.pdf.

[2] http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf.

[3] http://www.iaisweb.org/file/60062/issues-paper-on-cyber-risk-to-the-insurance-sector-public-consultation.

[4] http://www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf.