MAYER·BROWN

Legal Update
October 9, 2018

5 Considerations for General Counsels Regarding the New York Cybersecurity Regulations

The cybersecurity regulation ("CyberRegs") adopted by the New York State Department of Financial Services ("NYDFS") is almost two years old and will be fully in effect by March 2019.[1] The CyberRegs has already had a broad impact on financial institutions that are authorized to engage in business in New York ("Covered Entities"). Furthermore, even for those financial services companies not directly covered, the CyberRegs has generally raised the expectations of other regulators and defined what are considered best practices for cybersecurity programs in the industry. We briefly discuss below five things that general counsel ("GCs") should understand about the CyberRegs and their organizations' compliance with the requirements.

Annual Board Report and Certification

At least annually, the chief information security officer ("CISO") is required to provide a report to the Covered Entity's board or other governing body on the cybersecurity program and material cybersecurity risks, considering, as applicable, material cybersecurity events and the overall effectiveness of the program. Additionally, the board of directors (or one or more of the senior officers of the Covered Entity) are required to certify the Covered Entity's compliance with the CyberRegs to the NYDFS on an annual basis by February 15 of each year.

GCs of Covered Entities should understand the annual reporting and certification obligations. This may include determining whether the annual report is being made to the board of directors and whether the board is actually engaging the CISO or management on the report's content. GCs also should understand who within their organization is certifying compliance with the CyberRegs and what procedures are in place to ensure that those individuals providing the certification have the information needed to support the compliance certification. For some Covered Entities, these procedures may include obtaining sub-certifications or other similar assurances from employees with direct knowledge and responsibility for the key elements of the cybersecurity program.

Breach Notification

A Covered Entity is required to put in place a written incident response plan designed to enable the organization to promptly respond to and recover from a cybersecurity event materially affecting the confidentiality, integrity or availability of its systems. As part of this plan, Covered Entities are required to notify the NYDFS within 72 hours after becoming aware of any cybersecurity event with a "reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity" or for which notice must be provided to any government body, self-regulatory agency or other supervisory body.

GCs of Covered Entities should understand how their CyberRegs notification procedures are integrated into pre-existing 50-state breach notification procedures set out in the incident response plan. They also should ensure that the incident response plan identifies the person or group of individuals responsible for deciding whether an incident is subject to the CyberRegs notification requirement and making sure that this decision-making process involves the GC or another lawyer.

Third-party Service Provider Compliance

Beginning in March 2019, the CyberRegs will cause Covered Entities to pass on certain cybersecurity obligations to third-party service providers ("TSPs") by requiring Covered Entities to develop written policies and procedures designed to ensure the security of systems and data accessible to, or held by, TSPs. Additionally, each Covered Entity will be required to address with their TSPs through due diligence or contractual protections (i) the use of access controls and multi-factor authentication, (ii) encryption of nonpublic information in transit and at rest, (iii) prompt notification to the Covered Entity of certain cybersecurity events and (iv) representations and warranties from the TSPs concerning their cybersecurity policies and procedures.

GCs of Covered Entities should consider whether their company has updated its contractual terms for TSPs to include the required contractual protections contemplated by the CyberRegs. For example, do the Covered Entity's contracts require notice of the types of "cybersecurity events" covered by the CyberRegs and in a time and manner that would enable the Covered Entity to satisfy its notification obligations to the NYDFS (as described above)? GCs also should understand how procurement personnel (including lawyers and stakeholders) and others within the organization evaluate new TSPs and monitor the activities of existing TSP relationships and activities for compliance with the CyberRegs.

Data Governance and Classification

The CyberRegs states that a Covered Entity's cybersecurity policy must address data governance and classification but does not define those two terms. We think this provision refers to the need for a Covered Entity to be aware of the types of information it possesses and to implement a framework that is designed to ensure that nonpublic information is identified and protected by the cybersecurity program.

GCs of Covered Entities should understand where their nonpublic information is stored and how data is classified within the organization (e.g., public, confidential, highly confidential). A Covered Entity cannot effectively protect its nonpublic information until it understands where the information is stored, who has access and how is it transmitted. Proper data classification is another important element of data security as providers, senders and recipients of such information will need an immediate understanding of the sensitivity of the data. GCs also should help ensure that the flows of nonpublic information within the Covered Entity are protected in a manner consistent with applicable law (including the CyberRegs).

Training

A Covered Entity's cybersecurity personnel are subject to ongoing subject-matter training requirements, and all of a Covered Entity's personnel must undergo regular cybersecurity awareness training that is updated to reflect risks identified in its periodic risk assessment. Employee and vendor training is an important aspect of any cybersecurity program as employees, along with vendors, are frequently responsible for breaches and other cybersecurity incidents. Many of the breaches resulting from

phishing, spearing phishing and other third-party attacks could be avoided by targeted training, and the resulting harm from successful attacks could be mitigated by conducting tabletop and similar training exercises to test the incident response plan.

GCs of Covered Entities should ask their learning/training and information security departments about the type of employee and vendor training that the organization is providing and assess whether this training meets the requirements of the CyberRegs. They also should ensure that the Covered Entity is able to demonstrate that the training being provided is related to its particular cybersecurity risks and goes beyond generalized "how to use technology" training that is often provided as part of an employee's on-boarding.

Be Aware of New State Cybersecurity Requirements

After the NYDFS adopted the CyberRegs, the National Association of Insurance Commissioners adopted an Insurance Data Security Model Law that is intended to be enacted by the legislature of each state and has already been enacted in South Carolina.[2] While the model law's requirements have strong similarities to the CyberRegs, there also are some differences, particularly with respect to insurance industry-specific structures and practices. Therefore, compliance with the CyberRegs will not necessarily ensure compliance with other states' statutes that are based on the model law. However, in our experience, insurance licensees can leverage the steps they have taken to comply with the CyberRegs to achieve compliance with the model law's requirements. We'll cover new and emerging state cyber and privacy requirements in more detail later this month as part of this series.

For more information section about the topics raised in this Legal Update, please contact any of the following lawyers.

Lawrence R. Hamilton
+1 312 701 7055
lhamilton@mayerbrown.com

Jeffrey P. Taft
+1 202 263 3293
jtaft@mayerbrown.com

Matthew Bisanz
+1 202 263 3434
mbisanz@mayerbrown.com

Endnotes

[1] NYDFS, *Cybersecurity Requirements for Financial Services Companies*, XXXIX (No. 9) N.Y. Reg. 3 (Mar. 1, 2017) (*codified at* N.Y. Comp. Codes R. & Regs. tit. 23, pt. 500).

[2] NAIC, *NAIC Passes Insurance Data Security Model Law* (Oct. 24, 2017). The text of the Model Law, which has been designated by the NAIC as Model 668, is available at http://www.naic.org/store/free/MDL-668.pdf.