Decode cyber risk.

Spotlight on Revised NY Financial Regulations

By Kenneth K. Dort and Reeya Thakrar

The New York State Department of Financial Service ("DFS") published a new set of cybersecurity regulations on March 1, 2017. The new regulations, entitled "Cybersecurity Requirements for Financial Services Companies" (the "Regulations"),* set forth new requirements for financial services companies to address cybersecurity threats and require such organizations to establish more robust cybersecurity programs.

Although the Regulations are now effective, financial services companies subject to the new Regulations do not need to implement all of the regulations at once. In fact, affected companies have a "transitional period" to phase the more complex requirements into their current cybersecurity programs. For example, while some Regulations must be implemented as of September 1, 2017, the checkpoints for phasing in the remaining Regulations will occur at intervals of one year (March 1, 2018), one and a half years (September 1, 2018) and two years (March 1, 2019). Section 500.22 covers the detailed timeline.

Covered entities

Financial services companies that are subject to the new Regulations are called "Covered Entities" and include non-governmental banks, insurance companies, investment firms, and other financial institutions subject to New York's Banking Law, Insurance Law and Financial Services Law (Section 500.01). As a result, the Regulations cover a wide range of financial institutions that may extend further than the types of companies regulated by the Gramm-Leach-Bliley Act.

The Regulations also exempt certain financial organizations from some of the Regulations if they have (1) fewer than 10 employees, (2) less than $5,000,000 in gross annual revenue in each of the last three fiscal years, or (3) less than $10,000,000 in year-end total assets (Section 500.19). Although these exempt companies are not required to designate a Chief Information Security Officer or perform penetration testing, they still must maintain a written cybersecurity program and related policies, perform risk assessments, monitor third party access, and limit their data retention. Imposing such requirements to maintain a written cybersecurity program and related policies on these exempt companies is a significant change from the proposed version of the Regulations.

In Section 500.09(c), the Regulations also exempt financial services companies that "do not directly or *indirectly,* operate, maintain, or utilize any Information System and that do not, and are not required to, directly or indirectly control, own, access, generate, receive or possess Nonpublic Information [as defined below]." However, for the purposes of this article, any reference to "exempt entities" refers to the former requirements of the exemption and assumes that any such company does operate information systems and does own nonpublic information.

*The Regulations are available at: https://www.pbwt.com/content/uploads/2016/12/Hosted-Link-Updated-Regulation.pdf.

Risk assessments

At the heart of the Regulations lies the requirement for financial services organizations to perform periodic risk assessments of the company's information systems (Section 500.09). These risk assessments must also be updated as reasonably necessary due to changes in the information systems, data, or business operations.

The Regulations require that risk assessments be contained within a written company policy which includes (i) criteria for evaluating and categorizing risks, assessing the confidentiality, integrity, security and availability of the information systems and adequacy of existing controls, and (ii) requirements describing how risks will be addressed, mitigated or accepted. The risk assessment will be the foundation of the Covered Entity's cybersecurity program and future testing. Covered entities, including exempt companies, have until March 1, 2018 to conduct a risk assessment according to this section.

Comprehensive cybersecurity policy

All Covered Entities are required to maintain updated written policies (approved by a Senior Officer, the entire Board of Directors, or equivalent committee), setting forth the procedures and policies for protecting "Nonpublic Information" stored on the company's information systems. "Nonpublic Information" is defined as "all information that is not Publicly Available [or reasonably believed to be lawfully available to the public]" and is related to the business (such that an unauthorized disclosure would materially and adversely impact the entity), personal information, or information derived from a healthcare provider (Section 500.01). The definitions also provide a test to determine whether "Publicly Available" information may be "reasonably believed" to be lawfully available to the public (Section 500.01, "Publicly Available").

The comprehensive cybersecurity policy should be based on the risk assessment and should address (Section 500.03).

(1) information security;
(2) data governance and classification;
(3) asset inventory and device management;
(4) access controls and identity management;
(5) business continuity and disaster recovery planning and resources;
(6) systems operations and availability concerns;
(7) systems and network security;
(8) systems and network monitoring;
(9) systems and application development and quality assurance;
(10) physical security and environmental controls;
(11) customer data privacy;
(12) vendor and third party service provider management;
(13) risk assessment; and
(14) incident response.

As noted above, all Covered Entities, including exempt entities, must implement a comprehensive cybersecurity policy by September 1, 2017.

Penetration testing and vulnerability management

In addition to the list provided above, a Covered Entity's cybersecurity policy must also contain policies for continuous monitoring, periodic penetration testing, and periodic vulnerability assessments (Section 500.05). These ongoing measures should be designed to continuously assess the effectiveness of the cybersecurity program. "Periodic" in this section is further defined to mean at least "annual" penetration testing and "bi-annual" vulnerability assessments, including systematic scans or reviews of a Covered Entity's information systems focusing on publicly known cybersecurity vulnerabilities. The requirement for "bi-annual" vulnerability assessments confirms the DFS' concern about the risk resulting from recent cybersecurity attacks and how quickly companies should expect such malware to advance.

Covered entities, not including exempt entities, have until March 1, 2018 to implement a risk assessment according to this section.

Encryption

As part of a Covered Entity's cybersecurity program controls, financial services companies should also implement encryption technology to protect Nonpublic Information held at rest or transmitted over networks (Section 500.15). If a Covered Entity determines that such encryption is not feasible, this decision should be documented and "effective alternative compensating controls" must be reviewed and approved by the company's Chief Information Security Officer instead.

Covered entities, and not exempt entities, are required to implement appropriate encryption tools within the next 18 months.

Third party service providers

The new Regulations not only apply to a Covered Entity's internal information systems, but also require Covered Entities to implement written policies for their third party service providers to ensure the security of the Covered Entity's information systems and the protection of Nonpublic Information (Section 500.11). Thus, a Covered Entity must first perform a risk assessment of its third party service providers and conduct due diligence to evaluate the adequacy and the practices of such third parties. Covered Entities must also continue to periodically assess the third parties as part of their ongoing assessment and include all contractual provisions, such as multi-factor authentication, encryption, notification of cybersecurity events, and representations and warranties related to cybersecurity policies in their agreements.

The DFS acknowledges that this section presents a substantial burden to Covered Entities and will require Covered Entities to update internal form agreements. As a result, the DFS is allowing Covered Entities, including exempt entities, two years to implement this Regulation (to March 1, 2019).

Authorized user training

Another requirement of a Covered Entity's cybersecurity program is the implementation of training for all "Authorized Users," which includes any employee, contractor, or agent that participates in the business operations of a Covered Entity and is authorized to access and use any information systems and data of the Covered Entity. Since training will be conducted as a result of both the risk assessment and comprehensive cybersecurity policy, the DFS is allowing Covered Entities to implement controls and monitoring mechanisms within the first year (by March 1, 2018) and implement training programs for all personnel within 18 months of the effective date of the Regulations (by September 1, 2018).

Conclusions

The Regulations represent a significant step in requiring financial services companies to proactively assess and continuously monitor their cybersecurity programs. Financial services companies that fall under the Regulations' scope should already be reviewing their cybersecurity strategies and policies, and preparing to assess their cybersecurity risks.

Within this context, financial companies must recognize that the model imposed by the Regulations is one of high dynamics. Simply complying with the technical components of the Regulations – such as by implementing encryption tools, performing a penetration test and/or conducting user training – as of a specific point in time is not enough. While the Regulations certainly require these efforts, they specifically reject such a static approach – instead imposing a continuing duty and obligation on financial companies to continually review their security efforts and the risk landscape in which they operate so as to maintain a solid readiness against the constantly evolving threats and dangers posed by cyber criminals. Signaling this approach more than anything else is the requirement that companies hire a chief information security officer to oversee these efforts and their appropriate implementation.

The Regulations' overriding message – that companies must be vigilant at all times and remain flexible to changing situations – is one that applies to all business sectors. If this message is not received and acted upon, those companies failing to do so will be irreparably harmed at some point in time. *The time to act is now.*

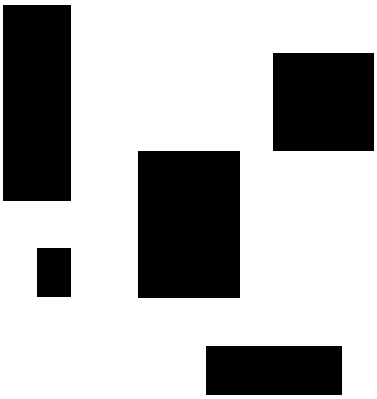
Kenneth Dort is a partner in the Intellectual Property Group of Drinker Biddle & Reath LLP, practicing in its Chicago office. He is also the chairman of the firm's Technology Committee and Data Security Committee.

Reeya Thakrar is an associate in the firm's Intellectual Property Group, also practicing in its Chicago office.

Contact

Kenneth Dort
312.569.1458
Kenneth.Dort@dbr.com

Reeya Thakrar
312.569.1467
Reeya.Thakrar@dbr.com



About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 40,000 employees serving more than 140 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

WTW-GL-17-PUB-8053a1d

willistowerswatson.com

Willis Towers Watson