Financial Services ALERT

Follow us on

September 2016

New York Proposes Cybersecurity Regulations for Financial Services Companies

By Peter Schablik, CISA, CPA, MBA | Partner
Charles Abraham, CPA |Partner
Barry Goodman, CPA |Partner

New York Department of Financial Services (DFS) has significantly raised the bar for cybersecurity programs, releasing regulations on September 13, 2016 slated to go into effect on January 1, 2017. The regulation will affect all entities with a DFS "license, registration, charter, certificate, permit, accreditation or similar authorization under the banking law, the insurance law or the financial services law." The regulation requires each entity's Board of Directors to file an annual certification of compliance with the superintendent of DFS. We recommend that covered entities begin evaluating the requirements and preparing plans, as remediation initiatives may require several months to complete.

Although the topics included in the new regulation are not new, the specific requirements are more stringent than previous regulations. An entity with fewer than 1,000 customers, less than $5,000,000 in gross annual revenue, and less than $10,000,000 in assets at the end of the year is exempt from some of the requirements. However, the grace period is only 180 days (e.g., June 2017), and the new regulations will be included in DFS examinations beginning January 1, 2018.

Based upon our research, New York is the lead state requiring cybersecurity controls to protect the financial industry. We understand that other states have similar initiatives and that the requirements in this pending regulation are being considered at a national level. The critical focus areas for this legislation include the following:

500.1 (g) – Non-Public Information – The definition has been expanded to include (1) business information that would cause a material adverse impact to the business, operations or security, (2) "Any information that an individual provides…in connection with ….any financial product or service…", (3) any information obtained from a health care provider for an individual, and (4) any information that can be used to distinguish or trace an individual's identify. This broadened definition of non-public information could include information in customer relationship management (CRM) and other sales systems, internal files, applications such as share transfer agents, and third parties. This expanded definition must be considered when evaluating other sections of the regulation.

"The regulatory focus seems to question the traditional practice of department managers reviewing and approving access privileges."

500.04 (a) – Chief Information Security Officer (CISO) – All covered entities are now required to assign the CISO role to an individual. This individual shall assume responsibility for oversight and prepare a board report detailing the effectiveness of the entity's cybersecurity program.

500.05 – Penetration Testing and Vulnerability Assessments – The best practice for conducting external penetration testing and internal vulnerability assessments on an annual (or more frequent) basis is not new. However, performing a vulnerability assessment at least quarterly is a new requirement. Based upon our experience, complying with this requirement will include both implementing a network appliance and hiring an external party to perform the assessment. A network appliance would provide for continuous monitoring, and an external party would be independent of management.

500.06 – Audit Trail – The requirements for the audit trail include (1) data logging of all privileged Authorized User access to critical systems; (2) protecting the integrity of data stored and maintained; and (3) maintaining records for no more than 6 years. These detailed requirements pose several dilemmas to be resolved. For example, what are the critical systems (e.g., financial application, network, database management system, third-party vendors), and what are critical transactions (new user accounts, security setting changes, master file edits). Data protection may not be a simple task, and may include significant changes to the network architecture and software tools. Finally, the requirement to maintain logs may require a substantial amount of data, and even more so for financial organizations with thousands of daily transactions. Industry tools such as Logrythms and Summo may be necessary to provide log filtering, storage, and cross-organizational view.

500.08 – Application Security – The regulatory focus seems to question the traditional practice of department managers reviewing and approving access privileges. Many organizations have been encouraged to implement solutions that combine access privileged from various applications and provide an organization-wide view of application security the intention of the review is to identify any possible segregation of duties concerns by reviewing the transaction capabilities. . The guidance further emphasizes that the review of the users entitlements should be completed by the Chief Information Security Officer (CISO) as this would provide the necessary independence.

500.10 – Cybersecurity Personnel and Intelligence – In addition to a CISO role, the expectation is that specific cybersecurity personnel will attend trainings and conferences and obtain certifications. Our experience has been that examiners will look for professionals certified in security disciplines (CISSP, CISA) and technical platforms (e.g., CISCO, Microsoft). In addition,

examiners will expect to see membership in organizations such as Infoguard for ongoing threat intelligence monitoring.

500.12 – Multi-Factor Authentication – Multi-factor has been the standard for customer transactions for more than a decade. The significant difference under the new regulations is that multi-factor authentication now will be required for both internal users and information technology support personnel. This requirement adds an additional layer of security to existing access management practices.

500.13 – Limitations on Data Retention – Although the language in this section appears to be straightforward, the previous definition of non-public information significantly increases the complexity of "…timely destruction of any Nonpublic Information..." Non- or partially integrated solutions, including web applications such as Mortgagebot, loan origination applications, CRM solutions, and others, makes it difficult to comply with this regulation. Data backup and rotation controls must be considered within this requirement's context.

500.14 – Training and Monitoring – Annual training in cybersecurity is no longer sufficient. A program is required that raises awareness, is supported by periodic reinforcement, and results in changed behavior and effectiveness in order to mitigate risk. In our experience, internal training solutions require significant management effort are exposed to major gaps, and have been criticized during regulatory reviews. We suggest clients consider solutions such as those offered by ThreatReady Resouces.

What Steps Should You Take?

We recommend you immediately assess how your organization's practices align with the pending regulation. Identifying potential gaps and developing a plan early in the process allows for an orderly assessment of requirements and remediation. We anticipate a significant industry effort and tightening of resources will occur in early 2017.

Click here to download 23 NYCRR Part 500 (Financial Services Law

For more information contact:

Peter Schablik, CISA, CPA, MBA | Partner
617.501.4195
Peter.Schablik@WeiserMazars.com

Charles Abraham, CPA | Partner, Financial Services Practice Leader
516.620.8526
Charles.Abraham@WeiserMazars.com

Barry Goodman, CPA | Partner
646.315.6163
Barry.Goodman@WeiserMazars.com

Visit us on **www.weisermazars.com**