PROTIVITI FLASH REPORT

New York State Proposes New Cybersecurity Regulations

September 20, 2016

New York Governor Andrew Cuomo has proposed a long-anticipated cybersecurity regulation for entities regulated by the Department of Financial Services, including banks and insurers in New York State.[1] As stated by the governor, "This regulation helps guarantee the financial services industry upholds its obligation to protect consumers and ensure that its systems are sufficiently constructed to prevent cyber-attacks to the fullest extent possible."[2]

Subject to a 45-day notice and public comment period, these new rules require regulated financial institutions to:

- Establish a cybersecurity program;
- Adopt written cybersecurity policies;
- Designate a chief information security officer (CISO) responsible for implementing, overseeing and enforcing the new program and policy; and
- Have policies and procedures designed to ensure the security of information systems and nonpublic information (NPI) accessible to, or held by, third parties, along with a variety of other requirements to protect the confidentiality, integrity and availability of information systems.

The rules also include minimum standards for the cybersecurity program and notifications to New York State's superintendent of financial services, such as disclosure of cybersecurity events within 72 hours and an annual statement of compliance against the requirements.

New York State's proposed legislation is without precedent, but more may follow given the current threat environment. There is a maturing black market for consumer information. Hackers are collecting private consumer records and distributing them to other malicious actors, who collate the information for financial theft, identity theft, ransom or other coercive purposes, in addition to sharing that information with foreign state or terrorist-driven sources.

New York State's proposed cybersecurity requirements also detail how the CISO shall report to the board of directors every six months, and that these reports must be made available to the state superintendent of financial services. These reports include assessments of the confidentiality, integrity and availability of information systems, as well as the effectiveness of the cybersecurity program, including any remedial actions required. In addition, they must include any material cybersecurity events that affected the organization over the period. Thus, along with establishing a cybersecurity program or aligning an existing

[1] New York Codes, Rules and Regulations (NYCRR) Title 23 Financial Services, Regulations of the Superintendent of Financial Services, Part 500, "Cybersecurity Requirements for Financial Services Companies."

[2] "Governor Cuomo Announces Proposal of First-in-the-Nation Cybersecurity Regulations to Protect Customers and Financial Institutions," New York State Department of Financial Services, Sept. 13, 2016: www.dfs.ny.gov/about/press/pr1609131.htm.

cybersecurity program with these requirements, financial services organizations essentially have six months to “clean house” or document cybersecurity issues in a discoverable report.

This regulation likely will have a greater impact on foreign banks and insurers that have branches and operations in New York but lack a significant technology presence or a designated CISO. Foreign banks, in fact, may have the greatest burden. In many cases, these institutions rely largely – or entirely – on their head offices to administer their cybersecurity programs. Within New York, they lack the necessary security infrastructure, policies and procedures, and personnel to comply with the new DFS regulation, meaning they may have a much greater task before them and thus may have little time to achieve compliance within the required deadline.

Impact on Financial Institutions in New York

While the rules are new, the cybersecurity practices on which they are based are not. The “establish cybersecurity program” requirements follow the Identify, Protect, Detect, Respond and Recover steps of the NIST Cybersecurity Framework, established per Executive Order 13636, Improving Critical Infrastructure Security, and the rules for adopting written cybersecurity policies have the familiar look of ISO 27001 – Information security management practices. While these frameworks are risk-based, New York State’s new rules set out minimum requirements for cybersecurity, including the encryption of all “at-rest” NPI, noting a five-year implementation timeline for the at-rest requirement. The rules on third-party service providers may also be familiar to organizations with mature vendor risk management programs, and these are aligned with existing risk management guidance such as the federal Office of the Comptroller of the Currency (OCC) bulletin on third-party relationships (OCC BULLETIN 2013-29).

There are some exemptions to compliance with the requirements based on the size of the entity – specifically, financial services institutions with fewer than 1,000 customers and/or less than $5 million in revenue over a three-year period, or less than $10 million in assets. When any of these thresholds are reached, an entity will have 180 days to comply with the rules.

It is also worth noting that the rules do not preclude the use of third parties to support an entity in meeting the cybersecurity personnel and intelligence requirements, so specialized firms can maintain the cybersecurity program and ongoing threat assessment.

Finally, the proposed regulation represents yet another certification requirement from the DFS. Could there be more certification requirements on the way? DFS-regulated financial institutions should be alert for other potential new certification requirements and be prepared to respond and react accordingly.

Organizations should analyze these new cybersecurity rules carefully and ensure their existing programs cover the minimum requirements of New York State’s Cybersecurity Requirements for Financial Services Companies. They should prepare to invest time and technology if there are gaps against these rules – for example, discovery and documentation of all customer NPI to ensure that it is encrypted at rest, and implementation of multi-factor authentication (MFA) for privileged access to internal systems. Companies also should consider whether they have the right individuals with appropriate delegated authority to take on the CISO role.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. Protiviti and our independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Named one of the 2015 *Fortune* 100 Best Companies to Work For®, Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

How We Can Help

Protiviti helps our financial services sector clients manage cybersecurity risks through benchmarking programs against leading practices, such as NIST CSF, ISO 27001 and regulatory guidance from the FFIEC. Our team of cybersecurity subject-matter experts assists organizations with:

- Cybersecurity program assessment
- Vendor risk management
- Security architecture and design
- Penetration testing
- Incident response plan development and testing
- Identity and access management
- Security training and awareness
- Security policy development and implementation

By partnering with Protiviti, management can demonstrate a commitment to addressing these emerging compliance requirements head on through establishing a cybersecurity program that is aligned with both the organization's risk appetite and the minimum standards set forth by the governor's office. We help companies develop and implement cybersecurity road maps that deliver the people, process, technology and governance needed to meet future challenges.

protiviti®
Risk & Business Consulting.
Internal Audit.