Perspective//

//// New York Cybersecurity Regulation: Finding Balance Between Cybersecurity and Regulatory Compliance

by Christopher Kelly

October 16, 2018

U.S. financial organizations have been the victims of some of the largest cyber security breaches. From the customer data breach of JP Morgan in March 2014 to the more recent Equifax and Uber breaches last year, cybercrime is undoubtedly the biggest threat facing firms today.

According to the 2018 Verizon Data Breach Investigations Report (DBIR), there were over 53,000 security incidents last year with 2,216 confirmed data breaches, up from nearly 2,000 confirmed breaches and 42,000 security incidents in 2016. According to the findings, 58 percent of data breaches attacked small businesses – the most commonly attacked segment.

In an effort to protect customer data and bolster the integrity of the information technology systems that support that data, the New York Department of Financial Services ("DFS") implemented a new set of cybersecurity regulations – 23 NYCRR Part 500 – in March 2017, requiring all DFS-regulated financial institutions, or "covered entities," to develop and maintain a robust and compliant cybersecurity program.

Described as being the "first in nation" cybersecurity regulation for banks, insurance companies, and other financial institutions regulated by DFS, 23 NYCRR 500 (or DFS 500) is generally viewed as a net positive for the financial services industry and a major improvement over several other established cybersecurity frameworks such as ISO 27002, the NIST Cybersecurity Framework, or NIST 800-53. "The (DFS 500) framework is based on risk, which is an improvement. Many of the controls should be implemented based on the annual risk assessment each financial company should perform," said a cybersecurity executive at a large foreign bank organization.

The new regulation establishes a series of four major compliance deadlines over a two-year period:

Phase 1 (180 days)	• Establish cybersecurity program • Hire Chief Security Officer & security personnel • Review user access privileges • Develop written incident response plan
Phase 2 (1 year)	• Perform penetration testing & vulnerability assessments • Conduct risk assessments • Conduct cyber awareness training • Produce annual report on cyber program
Phase 3 (18 months)	• Maintain records & audit trails • Establish guidelines for application security • Limit data retention and establish safe data disposal procedures • Monitor unauthorized access of sensitive information & encrypt nonpublic data
Phase 4 (2 years)	• Comply with 23 NYCRR 500 • Obligate third-party service providers to comply

SECONDLINE// ADVISORS//

Some DFS-regulated institutions, however, will be able to qualify for an exemption from some of the cybersecurity requirements under the Regulation if the number of employees, revenues and assets do not exceed certain thresholds.

Much like the European Union's General Data Protection Regulation (GDPR), DFS 500 will have far-reaching geographic impact. "The biggest challenge for large, global enterprises is ensuring the support of remediation activities beyond the borders of NY State or the Americas generally," the cyber executive said.

The requirements around third-party risk management will likely pose the biggest challenge for many organizations. While many already have third-party risk management programs in place, DFS 500 will make it more stringent on banks to ensure their supply chains are equally compliant.

"Larger, global vendors that provide critical services to financial companies have actively implemented the controls proactively, but for the thousands of vendors a typical financial company has, many will not have implemented them and the resultant risk must be carefully considered," the cybersecurity executive said.

What remains unclear, however, are the potential penalties for firms not in compliance with the regulation. Some believe NYDFS will calculate fines based on the existing New York Banking Law, which uses the following benchmarks:

- $2,500 per day during which a violation continues
- $15,000 per day in the event of any reckless or unsound practice or pattern of misconduct
- $75,000 per day in the event of a knowing and willful violation

As a result, the risk management function has gone through an evolution of sorts across numerous financial institutions, many of whom have begun to add or enhance their second-line compliance/risk management coverage by embedding them into the IT organization. Some have taken the approach of adding a Risk Technology Officer or an IT Compliance Officer to work closely with the Chief Information Security Officer (CISO) and ensure the firm is compliant with applicable laws, regulations and best practices.

But with the ever-increasing regulatory scrutiny, some worry that cybersecurity programs may "devolve" into a check-the-box compliance exercise, and while DFS 500 provides a good public service for the broader industry, it does not measure the effectiveness of the controls in thwarting actual cyberattacks.

"The regulations are good when not over-burdensome. When you see how much pressure the regulators tend to put on the banks, it devolves into a state of compliance," said Phil Agcaoili, Chief Information Security Officer at Elavon.

Even with these concerns, the Regulation seems to have spurred financial regulators in other states to consider imposing cybersecurity requirements on financial services firms. State financial regulators in both Colorado and Vermont recently adopted cybersecurity rules to broker-dealers and investment advisers regulated by those states.

With roughly six months to go before the final regulation comes into full effect, all DFS-regulated institutions should carefully be reviewing their cybersecurity programs, governance and supply chain relationships to address any remaining inefficiencies in order to meet regulatory expectations. This will require sponsorship from the executive committee as well as strong collaboration between Information Technology and Legal and Compliance teams to identify the risks, implement infrastructure, and enhance policies and procedures, so if and when there is a cybersecurity issue, the organization can better detect it, respond to it, and notify and report it accordingly.

About the Author:

Christopher Kelly is a Director at Second Line Advisors. Previously, he served as a Senior Associate with Sheffield Haworth, assisting in the identification and placement of executives within the risk, compliance, legal, technology and finance functions. Prior to his executive search career, Chris was a journalist with Thomson Reuters for 12 years, where he covered the daily commodity futures trading, with a particular focus on the precious and industrial metals markets. His career in finance began in 1998, working in the middle office clearing function of Liberty Brokerage.

Chris can be contacted at: (646) 798-0790 or ckelly@secondlineadvisors.com