NY CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES: THE CLOCK IS TICKING

For even the most casual of observers, 2017 has been a watershed year in our government declaring battle against the growing, pervasive Cybersecurity threat. The new Administration issued an Executive Order on May 11th that aims to 1) drive the government to follow its own IT security standards 2) improve the cybersecurity of critical infrastructure, and 3) increase the overall cybersecurity preparedness of the nation. On August 18, the Administration went even further, elevating Cyber Command as its own distinct military command.

The federal government is not alone in the fight – this March, **the New York Department of Financial Services implemented arguably the most stringent Cybersecurity standards for financial services companies in the country.** As the financial capital of the world, New York wants to ensure that financial services companies are preparing themselves appropriately to safeguard trust, protect financial assets and defend consumer's nonpublic personal information from unauthorized access, disclosure or use.

In August of 2017, the clock started ticking loudly and the bar has started to get progressively higher.

August 28 marks the first of four due dates for companies that need to meet the NY Cyber Law 23 NYCRR 500. Yet, the compliance curve is steep, and affected companies' confidence in achieving compliance is inversely low. According to a Ponemon Institute Research Report published in May 2017, 53 percent of the respondents answered the question "Will your company be in compliance with the regulations on or before February 15, 2018" negatively – either as 'No, not likely', or 'No chance'

(The February 15, 2018 deadline is the second milestone of four, and one that requires a certification by the Board or a Senior Officer as to the organization's compliance with the statute). The key question is why do most companies think they will miss the deadline and what should they do about it?

Some of the critical hurdles financial service companies face is the appointment of and reporting from a CISO on the company's cybersecurity program and material risks (section 500.04b), completion of a comprehensive risk assessment (section 500.09) and adoption of multi-factor authentication (section 500.12) under specific circumstances. Given that there are two more "transitional periods" identified in the forthcoming six and twelve months respectively, it is fair to say that the deadlines are rapidly approaching and the slope to compliance is steep. The two main barriers to achieving compliance, according to the respondents in the Ponemon Report are:

- Not having the necessary in-house expertise (70 percent of respondents) and
- Not knowing where high value data assets are located (68 percent of respondents)

Given this, where can financial service companies look for such expertise outside their organizations – and gain the assurance they will meet the NY regulation and protect themselves from the growing cybersecurity threat?

First, I would recommend finding a firm with experience in helping financial institutions achieve compliance with regulations like GLBA and other FFIEC IT-related guidance. Such firms will have the expertise, process and content that has been well-tested and proven since 2001.

Next, look for a firm that has the depth of bench to cover IT environments that are outsourced or in-house, and has both technical and IT compliance professionals who specialize in this highly specialized arena.

Finally, seek a firm that can show you examples of what some of their completed deliverables will look like so that you can clearly compare service providers and distinguish to be trusted advisers from generalist "wanna be's."

Accume Partners is proud to work with financial services companies to comply with current and complex regulations. Accume prides itself on delivering services that are designed to get financial services companies out of trouble and keep them out of trouble.

This opinion paper was written by Michael Barrack, an IT Security and Compliance Executive with more than 25 years of serving financial service companies ranging in size from $1-5 billion. Over the years, he has developed and executed systems evaluations and implementation methodologies, IT Governance programs, and risk management programs. Mr. Barrack is the Managing Director of the Risk Director and Cyber Practice at Accume Partners.

For more information contact us at

888.696.1515

or

information@accumepartners.com

Follow us

About us

Accume Partners has a long history of providing internal audit, regulatory compliance and risk management services to banks and financial institutions. As the level of regulatory and business complexity has surged, so has the need for specialized knowledge and focus. We have organized our firm to achieve that goal providing our clients with deep knowledge, expertise and approaches in the following areas:

- Internal Audit
- Regulatory Compliance
- Enterprise Risk Management
- Technology Risk Management & Cybersecurity Solutions
- IT Audit
- Operations and Process Improvement

Through these key areas of focus, we are able to stay in front of change, bring balanced perspectives and the specialized knowledge demanded by today's banks and financial institutions.