New York DFS Cybersecurity Regulation Just Turned 1

New York State's Department of Financial Services (DFS) passed a cybersecurity regulation directed at financial institutions doing business in the state. The regulation, 23 NYCRR Part 500, is in response to an ever-growing threat posed to information and financial systems by nation-states, terrorist organizations and independent criminal actors.

The cybersecurity requirements from the DFS are the first of their kind passed by a state, and violations can carry heavy fines and include Senior Executive and Board liability. What senior management of financial institutions need to internalize is that enforcement of these regulations is a stated priority for New York State--cyber events have been steadily increasing, the potential risks to the financial services industry are severe, and New York is pushing to get organizations to meet the threat seriously.

All financial institutions, including banks and insurance companies that do business in New York, must now implement a comprehensive cybersecurity program that includes managing the cyber risks associated with their third-party vendors. The regulation requires company board members to provide annual compliance certification—imposing the responsibility for the governance program directly on senior management and board members.

Many New York State financial institutions are mid-stride of getting their heads around the new DFS regulation that turned 1 year old on March 1, 2018. But as you can see from the key dates below, for conformance to the New York Cybersecurity regulation (23 NYCRR Part 500)—anyone late to the party has some catching up to do . . .

- **March 1, 2017:** 23 NYCRR Part 500 became effective.
- **August 28, 2017**: 180-day transitional period ended. Covered Entities are required to be in compliance with requirements of 23 NYCRR Part 500 unless otherwise specified.
- **February 15, 2018**: Covered Entities were required to submit the first certification under 23 NYCRR 500.17(b) on or prior to this date.
- **March 1, 2018**: One-year transitional period ends. Covered Entities are required to be in compliance with the requirements of sections 500.04(b), 500.05, 500.09, 500.12 and 500.14(b) of 23 NYCRR Part 500.

© 2018, ACG Info Systems, LLC, All Rights Reserved

- **September 3, 2018:** Eighteen-month transitional period ends. Covered Entities are required to be in compliance with the requirements of sections 500.06, 500.08, 500.13, 500.14(a) and 500.15 of 23 NYCRR Part 500.
- **March 1, 2019:** Two-year transitional period ends. Covered Entities are required to be in compliance with the requirements of 23 NYCRR 500.11.

At a high level, the regulation requires that all covered entities:

- ☐ Conduct and document a cybersecurity risk assessment
- ☐ Designate a qualified CISO role
- ☐ Establish a risk-based cybersecurity governance program
- ☐ Adopt a written cybersecurity policy
- ☐ Establish a written incident response plan
- ☐ Submit an annual certification of compliance (February 15th)

All covered entities must also be able to perform the following core cybersecurity functions:

1. Identify and assess internal and external cybersecurity risks that may threaten the security or integrity of Nonpublic Information stored on the Covered Entity's Information Systems;
2. Use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts;
3. Detect Cybersecurity Events;
4. Respond to identified or detected Cybersecurity Events to mitigate any negative effects;
5. Recover from Cybersecurity Events and restore normal operations and services, and fulfill applicable regulatory reporting obligations.

Is your Organization prepared to meet these requirements?

Were you prepared to submit your annual Certification of Compliance to the superintendent by February 15, 2018?

Are you prepared to demonstrate your organizations' compliance if the regulators follow up on your certification?

The ACG Info Systems cybersecurity team is ready to help companies, and their senior executives and boards, meet the DFS cyber requirements. Our cybersecurity governance and cyber resiliency application ensures your organization is focused on all aspects of the DFS cybersecurity regulation including:

- Data Governance and Classification
- Asset Inventory and Device Management
- Physical Security and Environmental Controls
- Third-Party Vendor Management
- Board Education

© 2018, ACG Info Systems, LLC, All Rights Reserved

How can you give your institution the best possible chance of compliance with Part 500? We have some ideas at www.ACGInfoSystems.com.

> "Compliance" is just a subset of "governance" and not the other way around."
> — Pearl Zhu, Digitizing Boardroom: The Multifaceted Aspects of Digital Ready Boards

About the Author(s)

Jay Marqua is CIO of ACG Info Systems Cybersecurity and Information Systems Consulting Practice and Board Advisory Services Consulting Practice. Jay is based in ACGIS Info Systems' Durango, Colorado office. In his professional role supporting and serving Boards and Executive Leadership, Jay has led transformation efforts in the Healthcare, Energy, Financial, Communications, Technology, Software, Logistics, Hospitality and Travel Sectors. The pace and advantage to organizations of technology aligned with high performing teams has steered Jay to his concept, strategy and execution roles in the development of organizations globally. Jay can be reached at jay.marqua@acginfosystems.com

About ACG Info Systems, LLC

ACG Info Systems has developed an Active Cyber Governance Information System (ACGIS) to help organizations actively manage their cybersecurity and resiliency postures. The Active Cyber Governance Information System solution leverages the NIST CSF and US CERT CRR and provides the framework and functional capabilities to actively govern, manage and reduce complexity and risk. The ACGIS provides the functional governance capabilities to apply the principles and best practices of risk management to improving the cybersecurity and cyber resilience of organizations. The application guides enterprises in matching IT resources to business mission and activities, and enforcing the principals of governance, awareness, security, resiliency, maturity, and accountability on the entire organization—including business unit leads and third-party vendors.

© 2018, ACG Info Systems, LLC, All Rights Reserved