Guidepost

CYBERSECURITY GOVERNANCE CONVERGING AROUND COMMON PRINCIPLES

This February marks an important milestone in the evolution of cybersecurity regulation: entities regulated by the New York State Department of Financial Services (DFS) were required to submit their first annual certification of compliance with New York's, first in the nation, cybersecurity regulation by February 15, 2018. This occasion provides a good opportunity to reflect upon the emerging trends in the world of cybersecurity governance.

Since companies often answer to multiple authorities, the possibility exists for overlapping and even conflicting obligations. Fortunately, there is good news: cybersecurity regulations and cybersecurity best practices are all converging around a common set of fundamental principles. By following generally accepted best practices for securing your company's data, such as risk-based penetration testing and multi-factor authentication, you are also likely to be in compliance with both existing and proposed regulations.

Cybersecurity governance comes in a range of approaches, from voluntary best practices such as the NIST Cybersecurity Framework, to required, albeit broadly written guidelines such as those contained within the Federal Financial Institutions Examination Council's Cybersecurity Assessment Tool, to somewhat more prescriptive requirements such as the DFS regulations. The Model Cybersecurity Law adopted last year by the National Association of Insurance Commissioners closely parallels the DFS regulations.

While different sets of rules and best practices may differ depending on the applicable industry and jurisdiction, taking the following fundamental steps will help position your company to meet any standard:

1. ***Perform a Cybersecurity Risk Assessment.*** Regulators and cybersecurity experts agree that a company's own personnel are in the best position to know their company's cybersecurity risk, which can vary greatly depending on the company's business type, size, customer base, type of data held, and many other factors. Assessing your company's risk is challenging, but it must be performed thoughtfully and thoroughly because virtually your entire cybersecurity program will be tailored to your risk assessment.

2. ***Establish a Cybersecurity Policy.*** A cybersecurity program does not exist unless it is written down. Regulators and cybersecurity experts agree that it is critical to establish and maintain a written and regularly updated cybersecurity policy that is appropriate to your company's risk assessment. This policy will be a primary source for you to demonstrate to the Board of Directors, regulators, insurance carriers, and customers or clients that your company is diligent in creating, executing, and adhering to a robust cybersecurity program.

3. ***Designate a Chief Information Security Officer (CISO).*** Charging a single

qualified individual with responsibility for cybersecurity ensures clarity and accountability. For smaller companies, the CISO function can be outsourced.

4. ***Conduct Penetration Testing and Vulnerability Assessments.*** While different sets of best practices and regulations vary somewhat on how frequently and in what manner companies should conduct penetration testing and vulnerability assessments, they all agree these measures are an important part of a robust cybersecurity program.

5. ***Deploy Multi-Factor Authentication.*** All authorized users should use multi-factor authentication, such as entering both a password and a code texted to a cell phone, particularly when logging in from outside the network. Under what circumstances multi-factor authentication may be required will frequently depend on your company's risk assessment.

6. ***Encrypt Your Data.*** All non-public data that is critical to your business or to your customers or clients should be encrypted while in transit or at rest. Establish policies and procedures governing encryption based upon your company's risk assessment.

7. ***Prepare an Incident Response Plan.*** All companies have had or will have a cybersecurity incident of some kind. Many companies have one or more incidents they are not even aware of. How the company responds to such an incident may later be subject to intense scrutiny by regulators, investigators, and potential plaintiffs. Maintaining and following a written incident response plan that covers subjects such as detection, recovery, and notification procedures will help your company recover more quickly and fare much better in the ensuing scrutiny. Note that no incident response plan is complete until it has been tested in a tabletop exercise or similar drill.

Establishing cybersecurity programs and getting them right is a challenging, but necessary exercise. It is always a good idea to consult experts in the fields of cybersecurity and regulation when formulating and updating these programs. But understanding and thinking through these common principles will help ensure that you are complying with both cybersecurity best practices and the law.

KENNETH CITARELLA JD, MBA, CFE, CIPP/US

Senior Managing Director, Investigations and Cyber Forensics

Ken Citarella guides the international compliance efforts of the firm in its investigative, security consulting, due diligence and compliance consulting practices, including advising clients on how to create and maintain a privacy compliance program. An attorney and Certified Information Privacy Professional by the International Association of Privacy Professionals, Mr. Citarella was one of the earliest prosecutors in the nation involved in the investigation and prosecution of computer-based crime. The High Technology Crime Investigation Association bestowed its Lifetime Achievement Award on Mr. Citarella in 2011.