Tuesday, October 11, 2016

Cybersecurity - A Model Approach

Jonathan Foxx
Managing Director
Lenders Compliance Group

As some of you know, Lenders Compliance Group is the first risk management firm in the country to provide both a risk assessment and a disaster recovery plan for banks and nonbanks. The goal is to make the due diligence approach both affordable and consequential. Importantly, the resulting findings must meet regulatory scrutiny, since liability remains with the financial institution with respect to implementing Internet Technology, Information Security, and Cybersecurity requirements. The review process is conducted by Kevin Origoni, our Director/IT-IS-Cybersecurity, who is a Six Sigma awardee for his knowledge and experience. Our interest in this area has only grown more attentive as federal and state regulators have become very active in implementing disaster recovery and cybersecurity guidelines.

Our attentiveness has been borne out by the recently proposed regulation involving cybersecurity issued by the New York State Department of Financial Services (DFS). The regulation would impose significant cybersecurity standards on entities it supervises. The proposal is subject to a 45-day public comment period, which will end on November 14, 2016. Importantly, some of these standards exceed current state and federal requirements. It is valuable, therefore, to take a brief look at these prospective standards.

INSTITUTIONS
The proposed regulation would apply to entities operating or required to operate under a license, registration or other authorization under the New York Banking Law, Insurance Law or Financial Services Law. These covered entities include:

- New York state chartered banks,
- New York licensed branches and agencies of foreign banks,
- insurance companies,
- money transmitters,
- licensed lenders,
- mortgage brokers, and
- mortgage bankers, lenders and servicers.

Certain small entities would be exempt from some, but not all, of the requirements of the proposed regulation.

If adopted, the proposed regulation would require covered entities to adopt a written cybersecurity program and implement various safeguards to protect nonpublic information, as broadly defined in the proposal. Covered entities would have to annually certify to the DFS their compliance with the proposed regulation.

NATIONAL STANDARDS
We believe that the DFS proposal will set a nationwide standard for cybersecurity and should be carefully considered as a model for disaster recovery, IT, IS, and cybersecurity requirements.

As it is currently drafted, the proposed regulation is prescriptive, inasmuch as it goes beyond the requirements imposed by the federal banking regulators on the depository institutions they supervise. For instance, guidance provided by the Federal Financial Institutions Examination Council (FFIEC) in its September 2016 Examination Handbook suggests that financial institutions should implement the type and level of encryption that is commensurate with the sensitivity of information being protected. However, FFIEC does not mandate that all nonpublic information be encrypted while in transit and at rest, or resident, as the DFS has proposed. But the DFS proposal also appears to require multi-factor authentication in a much broader range of circumstances than the guidance provided by federal regulators to depository institutions, which is mostly focused on online banking.

Similarly, the federal banking regulators require financial institutions to provide notice of information security breaches involving unauthorized access to or use of sensitive customer information; however, the DFS would mandate such notification within 72 hours of any cybersecurity event, a timeframe which the federal banking regulators do not require.

SPECIFIC STANDARDS
The DFS sets forth standards for policies and procedures. Each covered entity's cybersecurity program would need to be designed to ensure the confidentiality, integrity and availability of the covered entity's information systems and to perform the following functions:

- Identify internal and external threats;
- Employ defensive infrastructure and implementation of policies and procedures to protect the covered entity's information systems and its confidential information from unauthorized access, use or other malicious acts;
- Detect cybersecurity events, which the proposal defines as any act or attempt (whether or not successful) to gain unauthorized access to, disrupt or misuse an information system or any information stored on such a system;
- Mitigate negative effects of cybersecurity events, recover from such events and restore normal operations; and
- Fulfill any regulatory reporting requirements.

POLICIES AND PROCEDURES
Covered entities would also need to implement and maintain a detailed, specific, written cybersecurity policy that sets forth procedures to protect information systems and nonpublic information. The policy would need to address certain minimum requirements described in the proposed regulation and would need to be approved by a senior officer and reviewed by the entity's board of directors at least annually.

CHIEF INFORMATION SECURITY OFFICER (CISO)
One of the essential features of the cybersecurity standards is the requirement that each covered entity must designate a qualified individual as the covered entity's Chief Information Security Officer (CISO). This terminology has been around for a while, but is now being directly addressed in regulatory standards.

The CISO would be responsible for implementing the cybersecurity program and ensuring compliance. A third-party service provider may be retained to fulfill the CISO's responsibilities, but the covered entity would ultimately remain responsible for compliance with the regulation and would need to designate a senior officer as being responsible for overseeing the third party. In other words, a financial institution cannot outsource the ultimate responsibility for seeing that the standards are implemented. In any event, the covered entity would need to require the third party to maintain its own cybersecurity program that meets the requirements of the proposed regulation.

At least twice a year, the CISO would need to report to the board of directors on the covered entity's cybersecurity program. Among other matters, the report would need to (1) address the confidentiality, integrity and availability of the covered entity's information systems, (2) identify exceptions to cybersecurity policies and procedures, (3) identify cyber-risks, (4) assess the effectiveness of the cybersecurity program, (5) propose any necessary remedial measures, and (6) summarize any cybersecurity events during the period covered by the report.

OVERALL STANDARDS
In addition to the foregoing attribute of a plan, personnel, and cybersecurity standards, the proposed regulation would also require the implementation of certain additional measures, including:

- Limiting access privileges to information systems that provide access to nonpublic information solely to those individuals who require such access to perform their responsibilities;
- Creating and implementing an audit trail system to track and log all privileged authorized user access to critical systems;
- Performing penetration testing at least annually and vulnerability assessments at least quarterly;
- Implementing written procedures, guidelines and standards designed to ensure secure development practices for in-house developed applications as well as assessing and testing externally developed applications;
- Conducting a cybersecurity risk assessment at least annually;
- Employing personnel to manage the covered entity's cybersecurity risks and perform the functions required by the proposed regulation, and providing regular training sessions for such personnel;
- Requiring multi-factor authentication for any individual accessing the covered entity's internal systems or data from an external network or for any privileged access to database servers that allow access to nonpublic information;
- Requiring risk-based authentication to access web applications that capture, display or interface with nonpublic information;
- Destroying nonpublic information that is no longer necessary for the provision of the products or services for which such information was provided (except where such information is required to be retained by law or regulation);
- Requiring all personnel to attend regular cybersecurity awareness training;
- Establishing a cybersecurity incident response plan that meets certain minimum requirements; and,
- Notifying the DFS of any cybersecurity event that may affect the normal operation of the covered entity or that affects nonpublic information as promptly as possible but in no event later than 72 hours following the event.

ENCRYPTION
The proposed regulation would also require covered entities to encrypt all nonpublic information held or transmitted by the covered entity, both in transit and resident. However, if such encryption is not currently feasible, the proposal would allow covered entities up to one year to comply with the encryption requirement so long as they implement compensating controls in the meantime.

INFORMATION SECURITY

Covered entities would also be required to implement policies and procedures designed to ensure the security of information systems and nonpublic information accessible to or held by third parties doing business with the covered entity. By extension, this means that certain requirements of the proposed rule would apply to service providers to New York banks and other covered entities.

In particular, a covered entity's third-party information security policy would need to address, to the extent applicable, the use of multi-factor authentication to limit access to sensitive systems and nonpublic information, the use of encryption to protect nonpublic information in transit and resident, prompt notice of cybersecurity events affecting the service provider, the ability of the covered entity to conduct cybersecurity audits and other matters.

ACTION PLAN

The proposed regulation will impact bank and nonbank IT, IS, and cybersecurity standards quite significantly. Many federal regulators already are moving their standards in the direction that the DFS has promulgated. In using the DFS guidelines as a model, it is important now to undertake a due diligence review of current implementation guidelines.

If you want assistance in this regards, please contact us.

Labels: Chief Information Security Officer, CISO, Cybersecurity, Department of Financial Servies, DFS, Federal Financial Institutions Examination Council, FFIEC, Information Security

Home Older Post

Contact