KPMG

NYDFS

Cybersecurity requirements for the financial services industry

kpmg.bm

In late 2016, the New York State Department of Financial Services (NYDFS) released an updated version of its cybersecurity requirements for financial services companies (first released in September 2016). The regulation establishes a baseline for all NYDFS regulated entities to address cyber risk. Apart from that, it also raises the bar in encryption, monitoring, and authentication to require controls beyond what most companies have currently implemented.

Covered entities

The regulation covers a wide range of entities within the banking, insurance, and financial services industries[i], and may also affect third-party service providers.

The examples of institutions supervised by NYDFS are:

- Bank and trust companies
- Credit unions
- Life and health insurance companies
- Mortgage bankers and brokers
- Money transmitters
- Investment companies
- Sales finance companies

The wide applicability of this regulation necessitates that companies evaluate if they will need to adhere to the cybersecurity requirements prescribed.

Key requirements

- Establish a cybersecurity program and designate a chief information security officer (CISO) to maintain the cybersecurity program and compliance with the regulations
- Encrypt all nonpublic information[ii] in transit and at rest
- Implement multifactor or risk-based authentication to access nonpublic information
- Notify the superintendent within 72 hours of any cybersecurity event that has a "reasonable likelihood of materially harming any normal operation of the entity"
- Report compliance on an annual basis

Source: NYDFS website, February 2017

[i]Covered Entity means any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation, or similar authorization under the Banking Law, the Insurance Law, or the Financial Services Law.

[ii]Nonpublic Information shall mean all electronic information that is not Publicly Available Information and is:

1. *Business-related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations, or security of the Covered Entity;*
2. *Any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account; or (v) biometric records.*
3. *Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual.*

What are the key challenges?

Multifactor authentication

The regulation requires multifactor authentication for all individuals (customer and internal) accessing the covered entity's internal network from outside. Multifactor or risk-based authentication is also recommended for all information systems storing or using nonpublic information.

To date, regulations have only mandated multifactor authentication for a small set of high-risk applications. Balancing security, ease of use, and operational overhead will be a tremendous endeavor for most companies as they implement the new requirements.

Data encryption

All nonpublic data will need to be protected at rest and in transit. Implementing encryption at rest may be difficult for companies using legacy systems. Companies will need a detailed analysis of all systems where nonpublic data exists, and detailed use cases for encryption. Third-party security contracts will now also need to have procedures and guidelines in order to protect nonpublic data in transit and at rest.

Audit trail

Entities will be required to log all system access and business activities so that financial transactions can be reconstructed for potential audits. These audit trails will augment efforts to detect and respond to cybersecurity events. The minimum retention period for these logs is significantly longer that that required by most regulations.

Annual certification and reporting

Compliance with cybersecurity regulatory requirements must be confirmed annually by an entity's board of directors. Organizations will be required to submit their first certification by February 15th, 2018.

NYDFS must be notified within 72 hours of any incident that either has, or could lead to, unauthorized use of, access to, or tampering with nonpublic data. This requirement adds to other regulations that already require notification in case of data breach or unauthorized disclosure, but the timelines proposed are more aggressive.

Data retention

Covered entities must create and/or update their data retention policy to align with the requirements of the regulation. Nonpublic data that is no longer needed for business reasons, must be disposed in a timely and secure manner, unless required to be stored by law or other regulations.

What are the other regulation requirements?

Cybersecurity program

Organizations are required to develop and implement a holistic cybersecurity program based on a risk assessment to identify threats and protect against attacks. The program's remit will also include regulatory compliance and application security.

Cybersecurity policy

The regulation requires all covered entities to maintain a cybersecurity policy that is approved by the board of directors (or their designees) and covers a wide spectrum of cybersecurity topics.

Chief information security officer (CISO)

Organizations are required to designate a CISO to oversee and manage the Cybersecurity Program. The CISO will present a current-state risk report to the board of directors annually. Most mature organizations will already either have a CISO or be able to delegate a "senior officer" to be responsible for the cyber program. On the other hand, the smaller shops that are also regulated by DFS-NYDFS will have to find a senior resource (internal or external) to perform the CISO function.

Access privileges

Access to systems where nonpublic information is stored must be limited to individuals requiring access to do their job, and this access must be periodically reviewed. Organizations may have an Access Management Program that has developed and implemented controls to prevent unauthorized access as well as periodic recertifications. However, they will have to verify that all systems where nonpublic data is stored or handled are in scope for the Access Management Program.

Risk assessments

Covered Entities are required to conduct a periodic risk assessment that includes criteria used to evaluate and categorize cyber risks, and evaluate the adequacy of existing controls in the environment. This needs to be followed up with risk treatment decisions, including justification and timelines.

Application security and pen testing

The Cybersecurity program must include guidelines for securing SDLC processes for applications developed in-house. This control is in line with NIST and ISO standards. Companies must also test the security of applications developed by external parties or vendor applications. This may have far-reaching impact on the financial industry, where many third-party or vendor applications are used in day-to-day operations, and companies rely on vendors to make changes to the code. Annual penetration tests and bi-annual vulnerability scans are also mandated.

Incident response plan

Companies must maintain an incident response plan detailing the internal processes for responding to an event, clear roles and responsibilities, and communication and remediation requirements. This is a standard control, and most organizations will just need to update required communications to include the NYDFS superintendent.

Training and monitoring

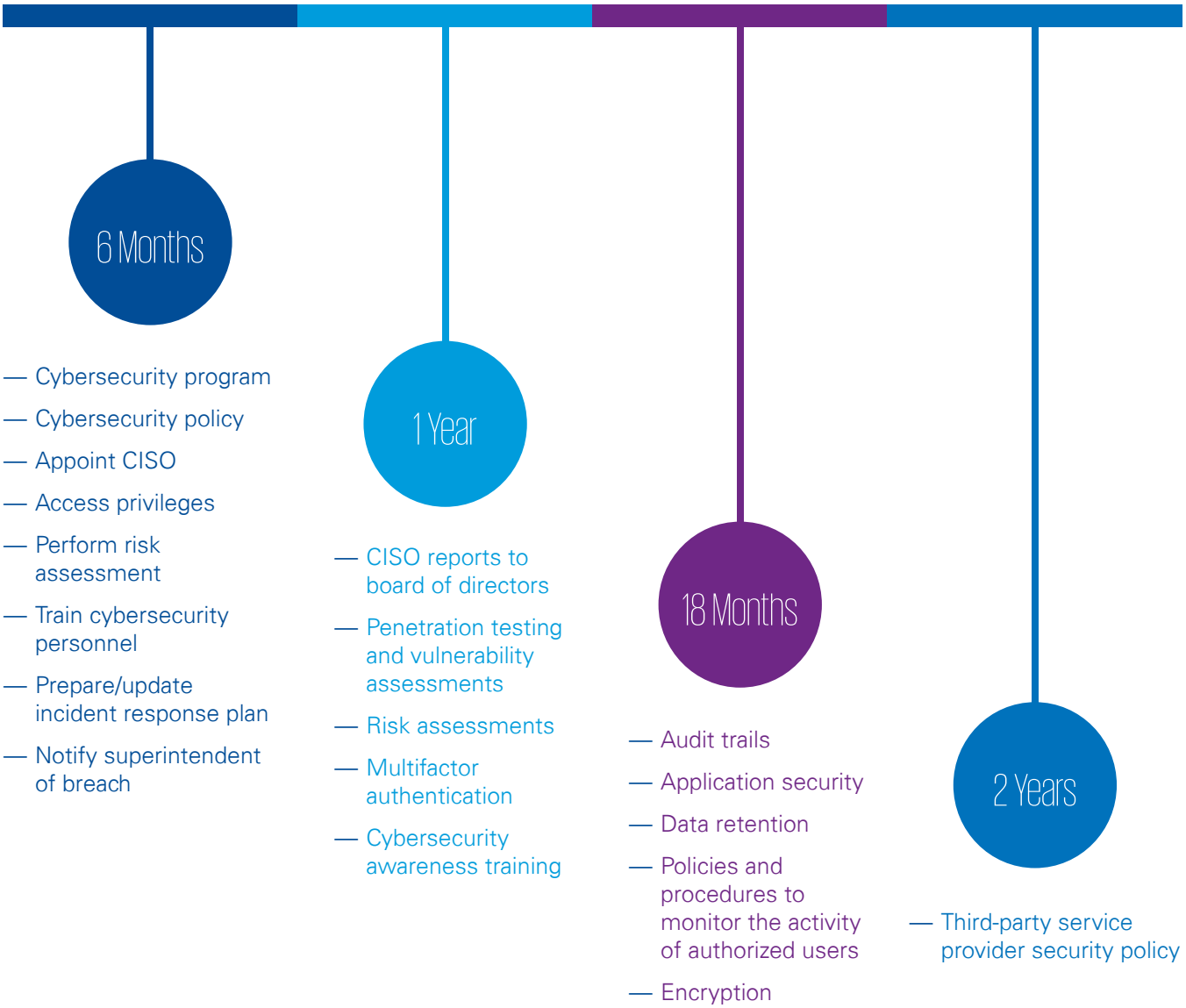
Organizations are required to provide periodic cybersecurity awareness training to all personnel. This training must be updated annually to reflect the risk assessment. Monitoring policies, procedures, and controls will need to be designed to identify anomalies in user behavior. User and entity behavior analytics (UEBA) solutions will start to play a bigger part as organizations enhance their monitoring capabilities.

Third-party risk management

Companies must have a robust third-party service provider risk management strategy. The numerous third-party/vendor relationships that most financial industry organizations have make it imperative to critically evaluate third-party risk and implement policy, procedures, and guidelines to address this risk.

Timelines

The revised regulation went into effect on March 1st, 2017, with the first certification due by February 15th, 2018. Covered Entities must maintain all relevant documentation supporting the yearly certification for a period of five years for examination by NYDFS. The timeline associated with implementing the requirements is as follows:



Contact:

Tom Kelly
Managing Director
T +1 441 294 2659
E thomaskelly@kpmg.bm

Chris Eaton
Senior Manager,
ITA, IT Advisory
C +1 441 294 2641
E chriseaton@kpmg.bm

kpmg.bm

INVESTORS IN PEOPLE | Gold