Cyber: New approach from New York regulator

On December 28, the New York State Department of Financial Services (DFS) issued a revised proposal containing a broad set of cybersecurity regulations for banks, insurers, and other financial institutions.¹ The revised proposal takes a less prescriptive and more risk-based approach than the original proposal issued by DFS last September.²

The revised proposal is the result of DFS’s focus on cybersecurity over the past several years, in which DFS conducted three industry surveys, held cybersecurity discussions with various financial institutions, and issued a letter to US regulators asking for feedback on potential cyber-specific requirements.³

The revised proposal adjusts many of the prescriptive requirements of the original proposal to be more risk-based. For example, the original proposal required that organizations use multi-factor authentication and encryption (most significantly, encryption of data “at-rest”) to protect nonpublic information, but the revised proposal allows organizations to use alternative controls (e.g., access controls, network security controls) to protect such information based on the results of their risk assessment. Additionally, the revised proposal relaxes the original proposal’s requirement that organizations include provisions around encryption, multi-factor authentication, and incident reporting in their contracts with third party service providers. Importantly, the revised proposal also narrows the definition of “nonpublic information” – the existence of which triggers many of the proposal’s requirements – to be more focused on information that is already subject to regulation or material to business operations.

Although the proposal is largely consistent with existing cybersecurity guidance (e.g., under the NIST Cybersecurity Framework or the FFIEC IT Handbook), it goes further in some ways. Notably, DFS will require that the chairperson of the board or a senior officer submit an annual certification that the entity is complying with the regulation’s requirements. Those submitting the certification could potentially be exposed to individual liability if the organization’s cybersecurity program is found to be noncompliant.⁵

The proposal will go into effect on March 1, 2017 and many of its requirements have compliance deadlines as early as September 1, 2017. We recommend that organizations begin reviewing their cybersecurity programs for conformance. Those entities with less mature programs – including many smaller banks and insurers – should be enhancing their cybersecurity programs to align with other leading industry practices such as the NIST Cybersecurity Framework, FFIEC guidance, or NAIC Data Security Model Law as appropriate.

It is clear that regulators across the financial services industry are focused on raising the bar for cybersecurity programs.⁶ As a result, we recommend that organizations holistically focus on developing a robust risk-based cybersecurity program rather than reactively responding to siloed regulatory guidance. Such an approach will make organizations well-equipped to comply with regulatory requirements while effectuating broader strategic objectives.⁷

This financial crimes observer analyzes the changes in the revised proposal, summarizes key challenges in the proposal, and provides our view on what organizations should be doing now.
Key changes from the original proposal

The revised proposal takes a less prescriptive and more risk-based approach than the original proposal, permitting organizations to adjust their controls based on their cyber risk assessment. The most important changes include the following.

Encryption of nonpublic information

While the original proposal called for organizations to encrypt nonpublic information both “in-transit” and “at-rest,” the revised proposal allows them to use alternative controls (e.g., access controls, network security controls) if their risk assessment determines that using encryption is unnecessary and that alternative controls would be as effective. These alternative controls must be reviewed and approved annually by the Chief Information Security Officer (CISO). It will be important that organizations formalize this risk acceptance process to appropriately document the rationale for using alternative controls and approval of such controls by the CISO.

Additionally, the revised proposal requires that organizations include encryption guidelines in their policies for third party service providers. This provides significant relief from the original proposal, which called for organizations to include encryption standards in their contracts with third parties.

Organizations will be required to comply with the revised proposal’s encryption requirements by September 2018.

Multi-factor authentication

The revised proposal relaxes the multi-factor authentication (MFA) requirements of the original proposal, which called for organizations to use MFA for any users accessing internal systems from an external network and for privileged internal access to nonpublic information.

Under the revised proposal, organizations are given the option to either use MFA for access to internal systems from an external network or use “reasonably equivalent” access controls that are approved by the CISO. Additionally, the revised proposal eliminates the original proposal’s prescriptive requirement to use MFA for privileged internal access to nonpublic information, instead calling for “effective controls” (which may include MFA or risk-based authentication) based on the organization’s risk assessment. Documenting the risk rationale will be an important evidentiary artifact in demonstrating compliance to DFS.

Organizations will be required to comply with these requirements by March 2018.

Third party risk management

The revised proposal provides a more narrow definition of what constitutes a third party service provider, excluding affiliates (e.g., parent companies and subsidiaries) and vendors that do not have access to nonpublic information from the proposal’s third party risk management requirements. Additionally, the revised proposal does not contain the original proposal’s requirement that organizations must include provisions around encryption, MFA, and incident reporting in their contracts with third party service providers.

However, organizations are still required in the revised proposal to have written policies regarding third party risk management, which include policies on conducting due diligence and periodic assessment of third party service providers. Conducting such due diligence and periodic assessments will be challenging for those organizations with a large number of third party service providers that do not already have a robust third party risk management program.

Organizations will be required to comply with the third party risk management requirements by March 2019.

Incident reporting

The original proposal required organizations to notify DFS within 72 hours of the discovery of cyber incidents that potentially compromise nonpublic information, including any unauthorized access of such information. Industry comments expressed concern that this requirement would result in an unnecessarily large number of reports of immaterial cyber events. The revised proposal reflects these concerns, requiring that organizations notify DFS only for those cyber incidents that have a reasonable likelihood of materially harming the organization’s normal operations or are reported to other supervisory, regulatory, or oversight bodies. These proposed reporting requirements align with what is currently required in other regulations (e.g., New York State’s data notification requirements).

To comply, entities should adjust their logging, monitoring, and detection operations and cyber incident response plans to include provisions for identifying and reporting incidents that fall under this requirement.

Organizations will be required to comply with these requirements by September 2017.
Penetration testing and vulnerability assessments

While the original proposal required that organizations conduct annual penetration testing and quarterly vulnerability testing, the revised proposal allows organizations that conduct continuous monitoring of their systems to forego the testing requirements. Such a continuous monitoring program should be able to detect changes in systems that indicate or create vulnerabilities, and assess the effectiveness of existing controls.

Organizations will be required to comply with the updated monitoring and testing requirements by March 2018.

Other requirements

DFS’s proposal codifies foundational cybersecurity requirements, which are consistent with existing guidance and leading industry practices, including the following.

Cybersecurity program

Organizations will be required to implement a cybersecurity program designed to perform the following core cybersecurity functions (consistent with the NIST Cybersecurity Framework):

- Identify internal and external threats
- Use defense infrastructure to protect the organization
- Detect cybersecurity events
- Respond to cybersecurity events
- Recover from cybersecurity events
- Fulfill all regulatory reporting requirements

Alternatively, an organization may adopt a cybersecurity program maintained by an affiliate if it meets the requirements outlined by the proposal.

Cybersecurity policy

The proposal also calls for entities to implement and maintain a written cybersecurity policy approved by the board or equivalent body, which must address the following areas (consistent with ISO 27001 standards and leading industry practices):

1. Information security
2. Data governance and classification
3. Access controls and identity management
4. Business continuity and disaster recovery planning and resources
5. Capacity and performance planning
6. Systems operations and availability concerns
7. Systems and network security
8. Systems and network monitoring
9. Systems and application development and quality assurance
10. Physical security and environmental controls
11. Customer data privacy
12. Vendor and third party service provider management
13. Risk assessment
14. Incident response

Annual certification

The proposed rule requires organizations certify annually that their cybersecurity program meets the proposal’s requirements. This certification is similar to the certification required by Sarbanes Oxley (SOX) for controls related to financial reporting. The Volcker Rule and last year’s instructions from the Federal Reserve regarding stress testing data include similar SOX-like certifications.9

Although not explicitly mentioned in the proposal, those submitting the certification could be held individually liable if the organization’s cybersecurity program is found to be deficient. The proposal notes that its requirements will be enforced “under any applicable laws,” which include laws (e.g., New York Banking Law, New York Insurance Law) that contain individual civil and criminal penalties for intentionally making false statements to DFS.

Because DFS has a similar certification requirement for anti-money laundering programs, some organizations will be able to develop a common capability for maintaining both certification programs.10

Organizations will be required to submit their first certification starting February 15, 2018.

Chief Information Security Officer

Organizations will be required to appoint a CISO to implement and oversee its cybersecurity program. The CISO will be required to present an annual report to the board or equivalent senior officer identifying cyber risks, evaluating the current effectiveness of the program, and summarizing material cybersecurity events.
Alternatively, organizations may use an affiliate or third party service provider to fill the CISO role, but must designate a senior officer to oversee the affiliate or third party.

Many organizations already have a CISO or similar role, but producing an annual report will be new for most entities. The first annual report must be presented to the board by March 2018.

**Risk assessments**
Organizations will be required to conduct periodic cybersecurity risk assessments of their information systems. The risk assessment takes on heightened importance in the revised proposal because organizations will be allowed to use alternative controls as determined by the assessment.

These assessments should identify cyber risks, evaluate existing controls, and have processes and provide mitigation procedures for such risks. Most organizations currently have policies in place to conduct regular risk assessments and should be well-equipped to meet this requirement. Firms will be well served to perform the risk assessment early on in its DFS compliance efforts as it may direct which alternative controls the firm chooses to implement.

**Access privileges**
Based on an organization’s risk assessment, access to systems containing nonpublic information will need to be restricted to only those with a business need for such access. In addition, firms must perform periodic reviews to confirm whether access is still appropriate. Many entities already address this requirement in their existing access controls, but may require additional investigation to identify all nonpublic information to successfully address the requirement.

**Audit trail**
Organizations will be required to maintain audit trails of sensitive data, including access to critical systems. The audit trail must be maintained for at least five years, which is longer than many organizations currently maintain audit records.

**Application security**
The proposal requires that internally built applications follow secure development practices and that organizations test the security of externally developed applications used within their own environments. Most large organizations have policies for secure development of internal applications, but testing external application security is less common.

---

**What should organizations be doing now?**

The revised proposal represents a significant shift in cybersecurity regulations. The rule goes into effect on March 1, 2017, and organizations must comply with many of its requirements by September 1, 2017, which does not leave much time to prepare.

As a result, organizations should begin reviewing the proposed regulations against their current programs to identify and remediate deficiencies. We recommend the following activities:

- **Current state capability assessment and gap identification** – Organizations should perform an assessment of their current state against the proposed requirements to identify any gaps with regards to the requirements of the rules.
- **Conduct a risk assessment** – The revised proposal allows organizations to develop alternative controls for several requirements (e.g., encryption, MFA) as determined by the risk assessment, which makes the assessment a critical part of complying with the rule.
- **Develop a remediation roadmap** – Use the gaps identified during the assessment to create a roadmap that will focus on complying with the proposal’s requirements.
- **Educate board of directors and senior officers** – Communicate the proposal’s requirements and expectations to the board and senior management. This sets the groundwork for conducting the annual certification by the board or senior officers by February 15, 2018.

In addition to those activities that organizations should be doing to meet the proposed requirements, there are a number of implicit requirements that are not stated in the proposed rule. These unstated requirements presuppose that organizations have in place policies, processes, and technology that support the requirements of the proposed regulation. The current state assessment and gap analysis recommended above should identify where these unstated requirements might not be sufficient. Unstated requirements include:

- **Data classification and mapping** – Organizations need to understand what data their systems contain and how that data is classified to comply with many of the proposal’s requirements. Therefore, organizations must have a data classification and mapping program to determine where nonpublic information exists, which will allow for properly implementing the encryption controls, MFA, and
other requirements intended to protect nonpublic information.

- **Identity management** – The proposal’s requirement that organizations limit access of nonpublic information (and maintain audit trails of such access) will require that organizations have an identity management program to identify, approve, periodically review and control which employees should have access to sensitive data.

- **Event monitoring and security operations** – Organizations need the ability to detect and respond to cybersecurity events in order to meet the proposal’s requirements, including the incident reporting and notification requirements. Security operations will necessitate a Security Information and Event Management (SIEM) system that is capable of capturing activity logs from systems and applications to monitor the environment and alert on potential cybersecurity incidents.

  Additionally, organizations should consider implementing User Behavior Analytics (UBA) to identify and alert when authorized users are exceeding their authority. Such a UBA program will help organizations comply with the proposal’s requirement that organizations monitor the activities of authorized users.
Endnotes

1. DFS’s proposal applies to banks that are chartered or licensed by New York State, insurers that are active in the state, and certain other financial institutions. The proposal exempts smaller institutions, including those with fewer than 1,000 customers over the last three calendar years, those with less than $5 million in gross annual revenue over the last three fiscal years, and those with less than $10 million in year-end total assets.

2. For additional information regarding the original proposal, see PwC’s Financial crimes observer, Cyber: New York regulator moves the goalposts (September 2016).

3. For additional information on DFS’s letter to US regulators, see PwC’s Financial crimes observer, Cyber: Is New York’s regulator upping the stakes? (November 2015).

4. The Federal Financial Institution Examination Council (FFIEC) is a regulatory council composed of the Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Consumer Financial Protection Bureau, and the National Credit Union Administration.

5. DFS’s anti-money laundering rule issued in June contains a nearly identical certification requirement. For additional information, see PwC’s Financial crimes observer, AML monitoring: New York regulator gets prescriptive (July 2016).

6. The Fed, OCC, and FDIC recently issued a joint ANPR containing heightened cybersecurity standards for large institutions. For further information, see PwC’s Financial crimes observer, Cyber: Banking regulators weigh in (November 2016).

7. For our guidance on developing a robust cyber risk management program, see PwC’s A closer look, Cyber: Think risk, not IT (April 2015).

8. Data “in-transit” refers to data moving from one location to another, such as over the internet or through an internal network. Data “at-rest” refers to data that is not actively moving, such as data stored on a hard drive.


10. For additional information on DFS’s anti-money laundering certification requirement, see the publication cited in Note 5.
Additional information

For additional information about this financial crimes observer or PwC’s Financial Crimes Unit, please contact:

**Dan Ryan**  
Financial Services Advisory Leader  
646 471 8488  
daniel.ryan@pwc.com  
@DanRyanWallSt

**Joseph Nocera**  
Cybersecurity Leader  
312 298 2745  
joseph.nocera@pwc.com  
@JoeNocera_PwC

**Chris O’Hara**  
Cybersecurity Principal  
646 471 5395  
christopher.ohara@pwc.com

**Sean Joyce**  
Financial Crimes Unit Leader  
703 918 3528  
sean.joyce@pwc.com  
@RealSeanJoyce

**Shawn Connors**  
Cybersecurity Principal  
646 471 7278  
shawn.joseph.connors@pwc.com

**Armen Meyer**  
Financial Services Managing Director  
646 531 4519  
armen.meyer@pwc.com

**Christopher Morris**  
Cybersecurity Principal  
617 530 7938  
christopher.morris@pwc.com

**Stephen Russell**  
Cybersecurity Managing Director  
203 539 3079  
stephen.j.russell@pwc.com

**Contributing authors:** Clarke Cummings, Mark Andruszkiewicz, Doug Bloom, and Michael Horn.

Follow us on Twitter @PwC_US_FinSrvcs

©2017 PwC. All rights reserved. PwC refers to the US member firm or one of its subsidiaries or affiliates, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

PwC US helps organizations and individuals create the value they’re looking for. We’re a member of the PwC network of firms in 157 countries with more than 223,000 people. We’re committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com/us