



Financial crimes observer

A publication of PwC's Financial Crimes Unit

Cyber: New York regulator moves the goalposts

Last week, the New York State Department of Financial Services (DFS) proposed a broad set of cybersecurity regulations for banks, insurers, and other financial institutions.¹ The proposal is largely consistent with existing guidance (e.g., under the NIST Cybersecurity Framework or the FFIEC² IT Handbook), but it goes further in some ways.

The proposed rule 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 proposal contains several requirements that will be new or more expansive than most organizations currently practice. For example, the proposal's call for encryption of all nonpublic information (including data both "in-transit" and "at-rest") will be challenging for many organizations. While most entities encrypt data in-transit, they only encrypt data at-rest in more selective circumstances.⁴ The proposal also expands the requirements for using multi-factor authentication in a variety of ways that will be new for most organizations.

Additionally, 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.

The proposal is now in a 45-day comment period, ending on October 28th, and many of its requirements have compliance deadlines as early as June 30, 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 industry best practices such as the NIST Cybersecurity Framework, FFIEC guidance, or NAIC Model Data Security Law as appropriate.

It is clear that regulators across the financial services industry are focused on raising the bar for cybersecurity programs. 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.⁵

This **Financial crimes observer** analyzes DFS's proposal, identifying key challenges.

What does the proposal require?

To start, DFS's proposal codifies foundational cybersecurity requirements, which are consistent with existing guidance and leading industry practices:

Cybersecurity program

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

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

Cybersecurity policy

The proposal also calls for entities to implement and maintain a written cybersecurity policy, 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

New challenges

However, the DFS's proposal also introduces several requirements that extend beyond current regulatory guidance and industry practices. The most significant are:

Data encryption

The proposal calls for organizations to encrypt sensitive data both in-transit and at-rest. The suggestion for encryption of data at-rest is the most impactful because it is not a common industry practice and will be challenging for many organizations to implement.

Under the proposal, organizations will be required to include these enhanced data encryption standards in their contracts with third party service providers. This will be burdensome for organizations with large numbers of service providers, as they must take steps to confirm each service provider's adherence to the encryption requirements.

Encryption requirements for in-transit data must be met by January 2018, while compliance for at-rest data must be met by January 2022. However, DFS expects that, prior to those dates, organizations secure nonpublic information using alternative controls that have been reviewed and approved by the Chief Information Security Officer (CISO).

Enhanced multi-factor authentication

The proposed multi-factor authentication requirements go beyond existing regulatory guidance, which only requires multi-factor authentication for internet banking channels. Under the proposal, multi-factor authentication would be required for any users accessing internal systems from an external network and for privileged access to database servers. Furthermore, the proposal requires risk-based and multi-factor authentication for web applications that contain nonpublic information.⁶

The proposed requirements are not standard industry practice as most organizations use multi-factor authentication for a more limited subset of external applications, but do not do so for internal access. Likewise, privileged access management solutions are still in their infancy of deployment in all but the largest firms.

Enhancing authentication programs will be an especially heavy lift for insurers, as some have not implemented multi-factor authentication due to the lack of specific insurance regulatory requirements within this space. Many banks have implemented some aspect of multi-factor authentication in order to comply with current FFIEC internet banking guidance.

Organizations will be required to comply with these requirements by June 30, 2017.

Annual certification

The proposed rule requires that either the chairperson of the board or a senior officer⁷ 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.⁸

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.⁹

Organizations will be required to submit their first certification by January 15, 2018.

Incident reporting

Under the proposal, entities would be required to notify DFS within 72 hours of the discovery of cyber incidents that either compromise nonpublic information (including unauthorized access of such information) or are likely to materially affect the business.

Although some existing regulations include requirements for reporting cybersecurity events, the proposed reporting requirements exceed the scope of what is currently required in other regulations. For example, New York State's existing data notification requirements only mandate that organizations notify authorities when there is a loss of customer personally identifiable information. Additionally, the Securities and Exchange Commission's cybersecurity reporting requirements under Regulation Systems Compliance and Integrity (Reg SCI) only apply to securities market infrastructure.¹⁰

To comply, entities should adjust their detection operations and 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 June 30, 2017.

Additional provisions

In addition to the most significant areas highlighted above, other requirements of the proposal include:

- *Third party risk management* – DFS's proposal requires entities to conduct due diligence on third parties and perform annual assessments of third parties' cybersecurity practices. Additionally, the proposal calls for organizations to include provisions around encryption, multi-factor authentication, and breach notification in their contracts with third parties. Conducting annual assessments on third parties and ensuring that third parties are following the required contractual provisions will be challenging for organizations that use a large number of service providers.¹¹
- *Chief Information Security Officer (CISO)* – Organizations will be required to appoint a CISO to implement and oversee its cybersecurity program. The CISO will be required to present a report to the board twice per year identifying cyber risks, evaluating the current effectiveness of the program, and summarizing material cybersecurity events. Many organizations already have a CISO or similar role, but producing a biannual report will be new for most entities.
- *Audit trail* – Entities will be required to maintain audit trails of sensitive data, including logs of access to critical systems. The audit trail must be maintained for least six years, which is longer than many organizations currently maintain audit records.
- *Access privileges* – Access to systems containing nonpublic information will need to be restricted to only those with a business need for such access. 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.
- *Application security* – The proposal requires that internally built applications follow secure development practices, and that organizations test the security of externally developed applications. Most organizations have policies for secure development of internal applications, but testing external application security is less common.
- *Testing requirements* – The proposal calls for annual penetration testing and quarterly vulnerability testing, which are already common practices for most organizations.¹²
- *Risk assessments* – Organizations will be required to conduct annual cybersecurity risk assessments. 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.

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. 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.
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. 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.
5. For our guidance on developing a robust cyber risk management program, see PwC's *A closer look, Cyber: Think risk, not IT* (April 2015).
6. For additional information regarding multi-factor authentication, see PwC's *Financial crimes observer, Fraud: Email compromise on the rise* (February 2016).
7. According to the proposed rule, a "senior officer" is someone responsible for the management, operations, security, information systems, or risk management of the institution.
8. See PwC's *Regulatory brief, Matching SOX? CFO attestation for stress tests* (October 2015) and PwC's *A closer look, Volcker rule clarity: Waiting for Godot* (May 2014).
9. 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).
10. Reg SCI requires notice within 24 hours for certain cybersecurity incidents. For additional information regarding Reg SCI's cybersecurity reporting requirements, see PwC's *First take, Ten key points from the SEC's final Reg SCI* (December 2014).
11. See PwC's *A closer look, Outsourcing: How cyber resilient are you?* (June 2015) for more information on third party cyber risk management, including an analysis of FFIEC guidance on the issue.
12. The CFTC recently issued similar requirements for market infrastructure. For more information on the CFTC's requirements or cybersecurity testing generally, see PwC's *Financial crimes observer, Cyber: Regulators putting market infrastructure to the test* (September 2016).

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

Didier Lavion

Anti-bribery/corruption Leader
917 770 2196
didier.lavion@pwc.com
@DidierLavion

Sean Joyce

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

Jeff Lavine

AML and Sanctions Leader
703 918 1379
jeff.lavine@us.pwc.com

Armen Meyer

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

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

Follow us on Twitter @PwC_US_FinSrvcs