Cyber: Is New York’s regulator upping the stakes?

Overview

Last week, the New York State Department of Financial Services (DFS) issued a letter to other US regulators proposing cyber-specific regulations for banks and insurers. The proposal is largely consistent with existing regulatory guidance and statutes (e.g., under the FFIEC or Gramm Leach Bliley Act), but it goes further in some ways. The most impactful new suggestions are the proposal's call for enhanced encryption of data from third party service providers and improved multi-factor authentication.

Guidance from DFS and other regulators thus far has come in the form of examination guidelines and self-assessment tools rather than regulations. This first potential cyber-specific US regulation could raise the stakes for financial institutions, but only if it mandates that examination staff who discover noncompliance take pre-defined enforcement actions. Since DFS's letter is silent on this issue, current guidance will remain just as consequential (as it is based on safe and sound practice).

Since the largest organizations have mature cybersecurity programs, most of their practices are already consistent with the proposal's suggestions. Furthermore, the proposal contains many suggestions that are similar to guidance issued by the FFIEC and the SEC's Office of Compliance Inspections and Examinations (OCIE).

However, insurers who have only been regulated at the state level, and banks that are not among the largest players will have significant enhancements to make, especially for those proposed requirements that go beyond current guidance. Insurers will especially be challenged because they are not covered by federal requirements under the Gramm Leach Bliley Act and the FFIEC's multi-factor authentication requirements.

Given the increasing importance and rapidly evolving threat of cyber attacks, we recommend that organizations focus on proactively developing a robust cybersecurity program rather than simply reacting to regulatory guidance. A holistic approach to cyber risk management will provide regulatory compliance while effectuating broader strategic objectives.

This Financial crimes observer analyzes (a) the suggestions of DFS's proposal and (b) key considerations for the industry.
DFS’s proposed requirements

DFS’s proposal introduces several new compliance requirements that extend beyond current regulatory guidance. Many of these requirements have already been met by the largest banks, but they will impact insurers and smaller banks.

The five most significant new suggestions are:

- **Enhanced multi-factor authentication requirements** – Existing FFIEC guidance requires multi-factor authentication for internet banking channels. The DFS proposal extends the scope of multi-factor authentication to also include employee and service providers’ access of critical internal systems.

- **Third party service provider data encryption** – The proposal would require organizations to mandate that their third party service providers encrypt sensitive data “in transit” and “at rest.” The suggestion for encryption of data at rest is the most impactful because it is not a common practice among many service providers, and ensuring service provider adherence to this requirement will be burdensome to organizations with a large number of service providers.

- **Annual cybersecurity reporting to the Board and DFS** – The proposal requires that the Chief Information Security Officer (CISO) send a Board-reviewed cybersecurity report to DFS that contains an assessment of the organization’s cybersecurity practices. This will require those organizations that have not already done so to hire or designate a CISO while imposing new obligations on the Board.

- **Enhanced applications security** – While prior requirements have focused on the protection of critical systems and applications, the proposal requires organizations to maintain security procedures and guidelines for all applications utilized by the organization. Additionally, the proposal requires that the CISO review and update application security procedures on an annual basis.

- **Additional notification requirements** – The proposal requires that organizations report to DFS any material cybersecurity event, including any event shared with the Board. Under New York State’s existing data notification requirements, organizations are only required to notify authorities when there is a loss of customer personal information.

The proposal does not address several cybersecurity topics that are currently being addressed by the industry, including threat intelligence collection and analysis, insider threat management, cybersecurity insurance, and cloud and mobile security. Additionally, the proposal does not address emerging cybersecurity risks associated with Internet of Things and social media, technologies that are becoming more common in the financial services industry.

The following figure summarizes the proposal’s eight areas of focus:
Key considerations for financial institutions

Organizations with less developed cybersecurity programs should focus on strengthening their overall cybersecurity programs, rather than solely focusing on regulatory requirements. With more sophisticated tools increasingly available to cyber criminals, cybersecurity is a rapidly evolving field, and mere compliance with regulatory requirements will not translate to adequate cybersecurity. We recommend that organizations perform a comprehensive cyber risk assessment to identify the risks inherent in their environment, and then assess the efficacy of technical and procedural controls in mitigating the identified risks.

Below are further considerations for insurers, banks, third party service providers, and investment companies that are regulated by DFS:

- **Insurers** – Large insurers that have gone through the first round of DFS cybersecurity examinations should be able to comply with most of the proposed requirements. However, medium and small insurers are still building their cybersecurity practices, so we expect that they will face challenges in meeting DFS’s proposal. Most importantly, many insurers have not implemented multi-factor authentication, as they are not regulated by the FFIEC. Therefore, insurers will need to hire adequate personnel and engage their senior management and Boards in order to implement sufficient multi-factor authentication.
• **Banks** – Given that cybersecurity programs at banking institutions have been examined for years now, we expect that banks will be well positioned to comply with the proposal. For example, the Gramm Leach Bliley Act already requires that CISOs present a cybersecurity report to the Board on an annual basis, so banks will simply need to send the report to DFS.

• **Service providers** – Though largely not regulated by DFS, third party service providers will be significantly impacted by the proposal. In a report published earlier this year, DFS identified that organizations need to perform onsite assessments of their service providers and also should require service providers to provide notification in the event of a cybersecurity incident. The proposal requires that organizations also include contractual terms around indemnification and information security warranties, which will require service providers to implement rigorous cybersecurity practices, including encryption of data in transit and at rest.

• **Investment companies** – Investment companies have been enhancing their cybersecurity programs since the publication of OCIE’s and DFS’s cybersecurity examination guidelines in 2014. However, these firms will have to focus on some of the proposed requirements such as multi-factor authentication and annual reporting that go beyond the existing examination guidelines. Additionally, the proposal will require that investment companies enhance their application security procedures to include all applications in their environment (which will build on the risk-based approach they have been taking).

These institutions should remain focused on DFS’s next steps and, perhaps most importantly, pay attention to other states who may take similar action towards formal regulations in the future.

**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.
2. The Commodity Futures Trading Commission (CFTC) is expected to formally propose a cybersecurity regulation in the coming weeks.
3. 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.
4. For an analysis of US regulators’ cybersecurity guidance to date, see PwC’s *A closer look, Cyber: Think risk, not IT* (April 2015). In the case of DFS, last year the agency announced that cybersecurity assessments will be integrated into exams and issued related guidance. Earlier this year, DFS released a report highlighting key cybersecurity risks associated with third party service providers.
6. The National Association of Insurance Commissioners recently issued cybersecurity guidance for insurance companies. See PwC’s *A closer look, Cybersecurity: Enter insurance regulators* (September 2015).
7. For our guidance on developing a robust cyber risk management program, see PwC’s *Viewpoint, Threat smart: Building a cyber resilient financial institution* (October 2014).
8. 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 the FFIEC’s regulatory guidance.
www.pwc.com/us/financialcrimes

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

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

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

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

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

Armen Meyer  
Director of Regulatory Strategy  
646 531 4519  
armen.meyer@pwc.com

Contributors: Harish Siripurapu and Joseph Dubbs.

Follow us on Twitter @PwC_US_FinSrvcs

© 2015 PricewaterhouseCoopers LLP, a Delaware limited liability partnership. All rights reserved. PwC refers to the US member firm, 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 158 countries with more than 180,000 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