Cybersecurity: Banking regulators weigh in

Last month, the Federal Reserve Board (FRB), the Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC) (collectively, “Agencies”), jointly issued an Advance Notice of Proposed Rulemaking (ANPR) regarding cyber risk management standards. The ANPR aims to enhance the abilities of large, interconnected financial services entities to prevent and recover from cyber attacks, and goes beyond existing requirements in several ways.

The Agencies issued the ANPR as a response to their concern that, due to the interconnectedness of the financial system, a cyber attack at one large, systemically important entity could impact the entire industry. To address this concern, the Agencies’ proposal requires that entities with total assets of $50 billion or more and their third party service providers take steps to strengthen their incident response programs, enhance their cyber risk governance and management practices across the three lines of defense, and better understand and manage risks associated with their dependencies on technology and service providers.

The ANPR is based on existing regulatory guidance (e.g., the FFIEC IT Handbook, NIST Cybersecurity Framework, and CPMI-IOSCO guidance on cyber resilience), but contains several requirements that will be new or more expansive for most entities. For example, the proposal applies directly to third party service providers, whose cyber practices are not as sophisticated as large financial services entities and will need to significantly enhance their cyber programs. The proposal also requires that critical systems are able to recover from a cyber attack within a two hour timeframe, which will be very challenging – if not untenable – to meet.

The Agencies are considering whether the final rule will be issued as a broader set of policy statements, or as a more prescriptive and detailed approach that contains specific requirements with which entities would need to comply. The proposal is now in a 90-day comment period ending on January 17, 2017. Given the skepticism of new regulation under the upcoming Trump administration, the future of the ANPR is uncertain.

Overall, the ANPR is another example of industry best cybersecurity practices turning into prescriptive regulatory obligations, as regulators continue to focus on raising the bar for cybersecurity programs. With this trend in mind, 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.

This Financial crimes observer analyzes the ANPR’s requirements, identifying key challenges.
The ANPR’s requirements and challenges

The proposal calls for entities to enhance their standards in five areas: incident response and cyber resilience; cyber risk governance; cyber risk management; and internal and external dependency management. Each of these areas contain requirements that will be new for most entities, and enhancing incident response programs to comply with the requirements will be especially challenging.

The Agencies also call for a higher tier of standards for critical systems, including a two-hour recovery time objective and a requirement that such systems implement “the most effective commercially available controls.”

The proposal’s requirements are as follows:

Incident response, cyber resilience, and situational awareness

The ANPR contains a broad set of requirements for cyber resilience and incident response programs. Notably, entities will be expected to have a two-hour objective for recovery from an outage for critical systems. Under current industry practice, most critical systems have a recovery time objective of four hours. Industry comments suggest that the two-hour timeframe will be very challenging to meet, and could be untenable as forensic gathering to determine whether systems are safe to start up will take longer than two hours in many cases.

Additionally, entities would be required to preserve critical data (e.g., financial records, account information) using secure offline storage, and format such data to allow other entities to restore the data in case of a prolonged disruption. Most entities currently do not have systems in place for secure offline storage of data, but the industry has made significant progress in developing standards for such secure offline storage.

The ANPR also calls for entities to develop plans to transfer business to other entities in case of a prolonged disruption. Most entities do not have such plans in the context of a cyber attack, but have plans to transfer business to other entities in the case of resolution.

Finally, entities will be required to develop a plan to mitigate “cyber contagion” – i.e., the risk that a cyber attack would also impact other financial entities. While similar concepts are addressed in existing guidance, the ANPR would present the first prescriptive obligation to develop such a plan.6

Cyber risk management

The ANPR calls for entities to incorporate cyber risk management practices into the three lines of defense – business units, independent risk management, and audit functions.7 The proposal is consistent with banking regulators’ recent focus on establishing an independent, objective, second line of defense to oversee and monitor risk.

In the first line, business units would be required to own and manage the organization’s cyber risks. Specifically, the proposal requires that they take steps to reduce cyber risk to the appropriate level according to the organization’s risk tolerance. Business units would also be required to conduct ongoing assessments of their cyber risks and vulnerabilities, and share the results with senior management (including the CEO).

Additionally, second line independent risk management functions would be required to oversee and monitor cyber risks. Specifically, the proposal requires that they assess enterprise-wide risk and notify senior management (including the CEO) when their assessment differs from the assessment of the business unit. The ANPR also calls for risk management functions to monitor whether adequate controls are in place and to quantitatively measure whether the entity has reduced their aggregate cyber risk to the Board-approved risk appetite level.

Finally, the proposal calls for the third line audit function to provide assurance. Specifically, they would be required to include a cyber risk management assessment in their overall audit plan, and assess whether the cyber risk management framework complies with applicable laws and regulations.

Cyber risk governance

Entities will be required to develop a written cyber risk governance strategy, which must include plans for how the entity will assess its cyber risk, determine its cyber risk tolerance, and reduce its cyber risk to the appropriate level. The proposal calls for entities to establish an enterprise-wide cyber risk management framework with policies and procedures to implement and maintain the strategy.

Furthermore, the strategy must be approved by the Board of Directors, which would be required to have adequate expertise in cybersecurity (or have access to resources or staff with such expertise). The Board would also be required to hold senior management accountable for establishing and implementing the cyber risk management framework.
While the requirement to maintain a written cyber governance strategy is consistent with existing regulatory requirements and current industry practice, the ANPR’s call for the Board to have cybersecurity expertise will be challenging for some entities that would need to change the composition of their Boards to meet the requirement.

While many entities already conduct cyber risk management practices that are largely consistent with these requirements, the ANPR goes further in some ways. The proposal’s call for independent risk management functions to quantitatively measure cyber risk will be new for most organizations, and the industry currently lacks standards for quantifying cyber risk.

Additionally, the requirement for each business unit to conduct its own cyber risk assessment – as well as the need for cyber expertise in audit functions – will require some entities to hire new cybersecurity personnel. This will impose additional costs on many entities, and will be challenging as qualified cybersecurity talent has been increasingly difficult as demand continues to grow.

**Dependency management (internal and external)**

The ANPR requires that entities assess and mitigate cyber risks associated with both internal dependencies (e.g., the entity’s workforce, data, technology, and facilities) and external dependencies (e.g., third party service providers, customers, utilities). To do so, entities would be required to develop a dependency management strategy that includes defined roles and responsibilities, policies and procedures to manage cyber risk, and plans to monitor the effectiveness of the strategy.

Additionally, the ANPR requires that entities monitor all external relationships in real time. While current guidance (e.g., FFIEC, NIST) recommends that entities monitor their service providers, the requirement to monitor them in real time goes beyond current guidance and practice. As a result, entities will need to hire new personnel to conduct such real-time monitoring, and will need to renegotiate agreements with many third party service providers to allow for such monitoring.

The ANPR also calls for entities to maintain an inventory of internal and external dependencies. In developing this inventory, the ANPR requires that entities prioritize business assets and external relationships according to criticality of the functions they support and their importance to the financial sector, and mapped to information flows and other connections. Based on this prioritization, entities would be required to adjust their incident response and recovery programs to focus on the most critical assets in the event of a disruption.
Endnotes

1. The ANPR covers those entities regulated by the Agencies, which include bank holding companies, US operations of foreign banking organizations, financial market infrastructure, savings and loan holding companies, national banks, federal savings associations, and others.

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. The Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions

4. The Agencies are considering defining “critical systems” to include systems that support the clearing or settlement of at least five percent of the value of transactions in various markets, systems that provide key functionality to the financial sector for which alternatives are limited, and systems that are critical to the financial sector due to their interconnectedness to other financial entities.

5. For example, the New York Department of Financial Services recently proposed a broad set of cybersecurity regulations for banks, insurers, and other financial institutions. See PwC’s Financial crimes observer, Cyber: New York regulator moves the goalposts (September 2016). Additionally, the CFTC in September issued cybersecurity testing requirements for financial market infrastructure. See PwC’s Financial crimes observer, Cyber: Regulators putting market infrastructure to the test (September 2016).

6. For example, CPMI-IOSCO guidance on cyber resilience recommends that financial market infrastructure develop plans to address cyber contagion. Additionally, FFIEC guidance provides general recommendations that mitigate the risk of cyber contagion.

7. For example, ISO 27001 and the New York Department of Financial Services’ recent cybersecurity proposal require that firms establish a written cybersecurity policy that covers governance and risk assessments. See PwC’s Financial crimes observer, Cyber: New York regulator moves the goalposts (September 2016).

8. The “three lines of defense” are a well-known risk governance concept. The first line of defense is part of the business unit and is responsible for managing the risks of its activity. The second line consists of independent risk management functions, separate from the first line, that have responsibility for identifying, measuring, monitoring, or controlling aggregate risk. Finally, the third line of defense – internal audit – provides independent assessment and assurance on the entire risk framework.
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

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

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

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

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

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

Contributing authors: Shantanu Chandra, Matthew Hagerty, Mark Andruszkiewicz, and Michael Horn.

Follow us on Twitter @PwC_US_FinSrvcs