CLIFFORD
CHANCE

Client briefing October 2016

Federal Banking Agencies Consider Tough Cybersecurity Regulations

On October 19, 2016, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency (collectively, the "**Agencies**") issued an advanced notice of proposed rulemaking that would establish enhanced cyber security standards (the "**Proposed Rules**" or the "**ANPR**"). The Proposed Rules would apply to large institutions subject to the Agencies' jurisdiction, including U.S. bank holding companies with total consolidated assets of $50 billion or more, banks with total consolidated assets of $50 billion or more; the U.S. operations of foreign banking organizations with total U.S. assets of $50 billion or more, and nonbank financial companies supervised by the Federal Reserve pursuant to section 165 of the Dodd-Frank Act (collectively, "**Covered Entities**").

Covered Entities may face a two-tiered set of cyber-security requirements. The base tier comprises five core categories of standards: 1) cyber risk governance, 2) cyber risk management, 3) internal dependency management, 4) external dependency management, and 5) incident response, cyber resilience, and situational awareness. Above this base tier, the Agencies provide additional standards for a higher tier of financial entities designated as critical to the sector ("sector-critical entities"). Of these additional standards, two are particularly novel. The ANPR would require firms to establish a recovery time objective ("RTO") within two hours after a cyber event; this would be validated by testing. Also, firms (and their boards) would be required to quantitatively measure their ability to reduce aggregate residual risk in their systems. In addition, the ANPR would impose unprecedented requirements on third-parties providing services to Covered Entities.

The Agencies are seeking comments and have asked a number of questions in the ANPR, and we urge Covered Entities and third-party service providers to actively participate in the rule-making process. Comments to the ANPR are due on January 17, 2017.

Background

The Agencies emphasize that the ANPR complements pre-existing requirements and guidance. The Proposed Rules would build on voluntary programs like the June 2015 Cybersecurity Assessment Tool and the NIST Cybersecurity Framework but would impose minimum standards tailored to the cyber risks facing "the largest, most interconnected U.S. financial entities."

The ANPR follows on the heels of the recent proposed regulations issued by the New York Department of Financial Services ("**DFS**") on September 13, 2016 (the "**DFS Cybersecurity Proposal**"). Our briefing regarding the DFS Cybersecurity Proposal is available here. Interestingly, the DFS apparently acted unilaterally when issuing its proposed cybersecurity rules, despite a DFS letter released in November 2015, which emphasized DFS support for coordination with the federal banking regulators in the establishment of a comprehensive cybersecurity framework. In what appears to be a split in opinion between the Agencies, the two sets of proposed regulations have a fairly different focus. The DFS Cybersecurity Proposal is focused on comprehensive cybersecurity plans and reporting requirements. Unlike the DFS Cybersecurity Proposal, the ANPR would not require Covered Entities to submit cybersecurity plans for approval or to notify the Agencies in the event of a data breach. While both the ANPR and the DFS Cybersecurity Proposal require enhanced monitoring of third parties, the ANPR appears to be more focused on interconnectedness and assessing risk. In an era of ever increasing regulatory burdens, it is unfortunate that Covered Entities regulated by the DFS would have to ensure compliance with cybersecurity rules that most likely will not be harmonized at the state and federal level.

Enhanced Cybersecurity Standards Under the ANPR

The ANPR proposes five categories of enhanced cyber risk standards as a base tier for all Covered Entities.

1. Cyber Risk Governance

The risk governance standard would be generally consistent with existing governance standards expected for large financial institutions. The enhanced cyber-security governance standards focus on four key areas. First, the Agencies would require Covered Entities to develop a "board-approved, enterprise-wide cyber risk management strategy" that is fully integrated with the firm's operations. Such a strategy would address inherent cyber risk, maintain low residual risk, and ensure constant resilience. Second, the ANPR proposes that the board review and approve an entity's cyber risk appetite. Third, the ANPR breaks new ground in placing specific cybersecurity risk-related duties upon the board of directors. In what will likely cause a stir within the industry, the Agencies may require the board to "have adequate expertise in cybersecurity" or maintain strong connections to such resources. The ANPR notes that, consistent with existing Agency expectations, the board of directors should maintain the ability to provide credible challenge to management in matters related to cybersecurity. Finally, the Proposed Rules would require senior cyber risk management to have direct and independent access to the board on an ongoing basis.

In addition to a cyber risk management strategy, the board would be required to establish a framework of policies to implement the strategy. It identifies five areas to be included in this framework: 1) reporting structures for independent risk management and audit personnel; 2) means to evaluate sufficiency of resources for cyber threats; 3) policies to address resource shortfalls and knowledge gaps; 4) cyber threat response policies and plans; and 5) plans to identify cyber risks and improve response plans.

2. Cyber Risk Management

The ANPR would codify a *three lines of defense risk-management model* for cyber risk management. The three lines of defense would comprise: (i) business decision-makers; (ii) independent risk managers (compliance and legal); and (iii) the independent audit functions. Business units would be required to assess cyber risk in all day-to-day decision-making. The independent risk management function would include an individual who would report directly to the board as indicated in the cyber risk governance category above. The audit function would independently assess the existing cyber risk management strategy and the efficacy of the framework and management in carrying out this strategy.

3. Internal Dependency Management

"Internal dependency management" refers to the management of cyber risk associated with a firm's business assets (workforce, data, technology, and facilities). Cyber risks associated with the firm's assets may arise from a wide range of sources, such as

data transmission errors or the use of acquired legacy systems. Standards in this category include internal dependency management strategy, continuous inventory and asset awareness, and back-up testing of alternates to business assets. The strategy to mitigate risk from business assets would: 1) have clearly defined roles and responsibilities for personnel, 2) create policies and update them regularly, 3) appoint appropriate monitoring and oversight, and 4) ensure compliance mechanisms.

4. External Dependency Management

"External dependencies" refer to external relationships between a Covered Entity and outside parties, including vendors, suppliers, utilities, service providers, and even customers. Like internal dependency, external dependency refers to the interconnections and information flow between these outside units. This category would require an external dependency management strategy and framework to continually monitor and improve upon third-party risk. It would require the strategy to include appropriate management of due diligence, contracting, on-boarding, ongoing monitoring, and off boarding. Additionally, the ANPR would require policies and plans to "identify and manage real-time cyber risks." It would require Covered Entities to have the ability to monitor, in real time, all outside relationships that support a cyber risk management strategy. These relationships could include outside counsel and cybersecurity firms. Covered entities would be required to map all such relationships in priority for monitoring and incident response. Furthermore, Covered Entities would be required to identify and test alternative solutions to external partners.

The Agencies' third-party requirements indicate concern about the increased risks posed by third parties, which often provide vulnerable points of entry to hackers. These risks are illustrated by the Target breach, where the access point was an outside vendor, and the 2016 SWIFT hack, which resulted in $81 million stolen from Bangladesh's central bank.

5. Incident Response, Cyber Resilience, and Situational Awareness

This category would provide standards for the cyber incident response cycle, from the planning to the responses and recovery phases. The Agencies provide eight broad standards that they might impose on Covered Entities.

1. Identify and mitigate any cyber risks that might be passed on to sector partners and external stakeholders through interconnectedness;
2. Maintain enterprise-wide cyber resilience and incident response programs;
3. Establish recovery objectives in the response to a cyber event; such objectives would be in timeline form and would include recovery points for any lost critical data;
4. Establish a means to perform core business functions during a wide variety of cyber disruptions. In particular, this includes disruptions in other interconnected critical infrastructure sectors such as energy and telecommunications;
5. Preserve critical records by developing "protocols for secure, immutable, off-line storage of critical records." These records must be formatted in a manner to allow for restoration by other financial institutions or even the federal government;
6. Establish transition plans if a Covered Entity cannot meet obligations to clients. Business would be transferred to another entity within set time frames;
7. Conduct testing to address cyber events and response, including impact to clients and external interdependencies. One potential requirement is joint cooperation with other entities where critical interdependency occurs; and
8. Collect threat intelligence and maintain a threat response plan.

Sector-Critical Systems

The ANPR provides guidance on how the Agencies would define sector-critical systems. Sector-critical systems would include Covered Entities "that support the clearing or settlement of at least five percent of the value transactions" consistently in critical financial markets. In addition, other factors such as substitutability and interconnectedness may be used to define sector-critical

systems. For example, Covered Entities that act as "key nodes to the financial sector" and are highly interconnected would significantly disrupt the U.S. financial system in the event of a major cyber event.

The Agencies highlight three potential additional standards for sector-critical systems. First, these systems would be required to implement "the most effective, commercially available controls" to minimize residual cyber risk. A second, unique requirement would be to quantitatively measure the ability to reduce aggregate residual risk to include risk from internal and external dependencies. Finally, the Agencies propose a two-hour RTO after a major cyber event. This RTO requires validation by testing under a wide range of scenarios, including disruption in other large financial systems.

Conclusion

The Proposed Rules would establish significant new regulatory compliance obligations for Covered Entities. These new requirements are still far from being finalized, however, and Covered Entities should review carefully the ANPR and consider providing comments. The Agencies pose 39 questions for comment, and significant changes to the Proposed Rules are possible. The Agencies note two major areas of potential revision. First, they have not yet determined an appropriate means to quantify cyber risk as required in the additional standards for sector-critical systems. Second, they have not yet determined which of three approaches to regulation a final rule might take. The Agencies may require Covered Entities to maintain a risk management framework in conjunction with guidance describing minimum expectations. Conversely, they may impose specific cyber risk management standards. Finally, the Agencies may consider a more detailed regulatory framework with specific objectives and practices a firm would be required to achieve in each of the five categories of cyber risk management. We urge Covered Entities to consider and provide comments on these critical matters.

Authors

Megan Gordon
Partner
T: +1 202 912 5021
E: megan.gordon
@cliffordchance.com

Daniel Silver
Partner
T: +1 212 878 4919
E: daniel.silver
@cliffordchance.com

Philip Angeloff
Counsel
T: +1 202 912 5111
E: philip.angeloff
@cliffordchance.com

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

© Clifford Chance 2016

Clifford Chance US LLP

www.cliffordchance.com

Abu Dhabi ■ Amsterdam ■ Bangkok ■ Barcelona ■ Beijing ■ Brussels ■ Bucharest ■ Casablanca ■ Doha ■ Dubai ■ Düsseldorf ■ Frankfurt ■ Hong Kong ■ Istanbul ■ Jakarta* ■ London ■ Luxembourg ■ Madrid ■ Milan ■ Moscow ■ Munich ■ New York ■ Paris ■ Perth ■ Prague ■ Riyadh ■ Rome ■ São Paulo ■ Seoul ■ Shanghai ■ Singapore ■ Sydney ■ Tokyo ■ Warsaw ■ Washington, D.C.

*Linda Widyati & Partners in association with Clifford Chance.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.