Client Update
Federal Financial Regulators to Propose Enhanced Cyber Risk Management Standards

WASHINGON, D.C.
Luke Dembosky
ldembosky@debevoise.com

NEW YORK
Jim Pastore
jjpastore@debevoise.com

David L. Portilla
dlportilla@debevoise.com

Jeremy Feigelson
jfeigelson@debevoise.com

Eric R. Dinallo
edinallo@debevoise.com

Gregory J. Lyons
gjlyons@debevoise.com

Johanna N. Skrzypczyk
jnskrzypczyk@debevoise.com

Joshua J. Smith
jjsmith@debevoise.com

On October 19, 2016, the Board of Governors of the Federal Reserve Systems, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation (collectively, the "Agencies") issued an advance notice of proposed rulemaking ("ANPR") regarding enhanced cyber risk management standards for certain entities under their supervision (the "Enhanced Standards").[1] The ANPR contemplates that the Enhanced Standards would cover five topic areas:

- Cyber risk governance;
- Cyber risk management;
- Internal dependency management;
- External dependency management; and
- Incident response, cyber resilience, and situational awareness.

The ANPR also contemplates that even higher standards would apply to those systems identified as "critical to the functioning of the financial sector."

In addition to this two-tiered approach to standards, the ANPR seeks input on the development of a repeatable and consistent scoring system to quantify cyber risk across a range of entities. And, while recognizing that the FFIEC Cybersecurity Assessment Tool and NIST Cybersecurity Framework already provide cybersecurity guidance to financial institutions, the ANPR suggests that its enhanced standards could go beyond this guidance by providing binding requirements for covered entities to meet. The ANPR leaves open the precise form of the Enhanced Standards, instead laying out three possibilities ranging from policy guidance (similar to the approach taken in other areas), to more

[1] The ANPR comment period concludes on January 17, 2017, after which the Agencies will promulgate a more detailed proposal followed by an additional comment period.

specific standards, to granular regulations with which entities would need to comply.

WHO WOULD BE COVERED?

The ANPR contemplates the application of the Enhanced Standards to regulated entities with consolidated assets of $50 billion or more, including subsidiaries of those entities and foreign banks with U.S. operations.[2] The ANPR specifically notes that subsidiaries of covered entities would be subject to the Enhanced Standards "in view of the subsidiaries' potential to act as points of cyber vulnerability to the covered entities." In addition, the Enhanced Standards may be extended to nonbank financial entities under the supervision of the Federal Reserve pursuant to the Dodd-Frank Act.

Perhaps most notably, the ANPR seeks comment on whether the Enhanced Standards ought to apply to "third-party service providers" of covered entities. This proposal–which is a natural outgrowth of regulators' increasing focus on third-party risk–likely, will generate substantial discussion during the comments period.

THE FIVE CATEGORIES

[2] Specifically, the proposed covered entities include the following institutions:

- Regulated by the FRB: U.S. bank holding companies 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; U.S. savings and loan holding companies with total consolidated assets of $50 billion or more; nonbank financial companies designated for FRB supervision by the Financial Stability Oversight Council ("FSOC"); financial market utilities designated by the FSOC for which the FRB is the supervisory agency per the Dodd-Frank Act; other financial market infrastructures for which the FRB is the primary supervisory or are operated by Federal Reserve Banks; any state member bank (and any subsidiaries thereof) that is a subsidiary of a bank holding company with total consolidated assets of $50 billion or more; and, any state member bank that has total consolidated assets of $50 billion or more that is not a subsidiary of a bank holding company. The FRB's standards would apply to subsidiaries of depository institution holding companies (other than depository institutions supervised by the OCC or FDIC, which are covered separately).

- Regulated by the OCC: Any national bank, federal savings association (and any subsidiaries thereof) or federal branch of a foreign bank that is a subsidiary of a bank holding company or savings and loan holding company with total assets of $50 billion or more; and, any national bank, federal savings association, or federal branch of a foreign bank that has total consolidated assets of $50 billion or more that does not have a parent holding company.

- Regulated by the FDIC: any state nonmember bank or state savings association (and any subsidiaries thereof) that is a subsidiary of a bank holding company or savings and loan holding company with total consolidated assets of $50 billion or more; and, any state nonmember bank or state savings association that has total consolidated assets of $50 billion or more that does not have a parent holding company.

Although still at the ANPR stage, the Enhanced Standards' categories are worth further examination, particularly because some of them contain granular suggestions for comment. We identify a few particularly noteworthy aspects below.

Governance

Sounding a common theme with earlier guidance, the ANPR suggests cybersecurity must be an exercise in enterprise-wide risk management involving the very highest levels of the organization. (This theme will be familiar from, among other guidance, the Interagency Guidelines Establishing Information Security Standards.) The ANPR proposes significantly more granular steps, however, including:

- That a board-reviewed and approved plan be established that not only speaks to inherent cybersecurity risks (that is, cyber risk before mitigating controls or other factors are considered) but also residual cyber risk.
- The establishment of a formal risk tolerance with respect to cyber, with a requirement that the board review and approve the proposed risk appetite.
- A requirement that the board of directors have adequate expertise in cybersecurity or maintain access to appropriate resources to discharge their duties in this regard.
- Demanding that those responsible for cyber risk be independent of business units, and have independent access to the board of directors.

The level of board involvement contemplated, and in particular, the requirement regarding board expertise, merits particular consideration, as it suggests the Agencies may examine board composition to ensure adequate experts exist within the board or, barring that, suggests that boards will need to retain their own cyber experts to manage cyber risks.

Cyber Risk Management

The ANPR conceives cyber risk management cutting across three independent functions:

- Business units, which would be required to assess cyber risks and adhere to policies and procedures designed to manage those risks;
- Independent risk management, which would assess cyber risks across the enterprise and have its own line of reporting to an appropriate officer and/or the board of directors; and

- Audit, which would be required to develop a full audit plan to measure the effectiveness of the cyber risk controls, including through penetration testing and other vulnerability assessments consistent with an entity's size, complexity, scope of operations, and interconnectedness.

Particularly noteworthy is the ANPR's suggestion that the independent risk management function may be tasked with measuring cyber risks quantitatively. As noted above, the ANPR seeks comments regarding methods for creating such a quantitative measure that could be consistent and repeatable across entities.

Internal Dependency Management

Under this heading, the ANPR proposes a series of steps to manage cyber risks arising out of not only technology, but also workforce and facilities issues. The proposal places particular emphasis on maintaining an updated inventory of "all internal assets and business functions" supporting a firm's cyber risk management strategy. If such a principle ultimately is adopted, it would transform the current best practice of knowing your assets and architecture into a legal requirement.

External Dependency Management

Not surprisingly, the ANPR devotes substantial time to third-party vendor management, focusing on procedures used through the vendor lifecycle including due diligence, contracting and sub-contracting, onboarding, monitoring, change management, and offboarding. The ANPR, however, goes deeper and suggests that covered entities would need to "monitor in real time" all external dependencies and trusted connections supporting cyber risk management. Given the time and expense associated with such real-time monitoring, this portion of the proposal may generate substantial discussion.

Incident Response, Cyber Resilience, and Situational Awareness

This fifth and last category reflects the reality that, even if entities enhance their cybersecurity, breaches and attacks will happen nonetheless. The ANPR contemplates requiring covered entities to develop plans to mitigate and contain damage, giving particular emphasis to the storage and maintenance of back-ups of critical files. The more granular aspects of the proposal include:

- Requirements that covered entities consider "secure, immutable, off-line storage of critical records";
- Identification and designation of alternative service providers for critical functions;

- Consideration of a multi-sector cyberattack across industries, "such as energy and telecommunications"; and
- The creation and maintenance of threat profiles and threat modeling consistent with identified risks.

KEY OBSERVATIONS

Although still at the ANPR stage, a few themes clearly emerge:

- Cyber risk is enterprise risk. The word "enterprise" litters the ANPR, and many of the proposals clearly set forth a view that cyber risk must begin at the top and pervade the business. The message is plainly that businesses no longer can treat cybersecurity as simply an IT problem, and that even the board will be expected to have sufficient resources internally (or, if lacking, externally) to understand and manage it. Notably, this paradigm informs the ANPR's effort to develop–and to seek comments on–a quantitative measure of cyber risk that can be applied across industries.
- Third-party risk must be managed. The ANPR both suggests that the rules might be applied directly to third-party providers, and sets forth a series of considerations for how covered entities must approach their third-party vendors. There is a particular awareness of the interconnectedness of the banking sector and, as a result, covered entities would be expected to maintain–in real time–an understanding of both internal and external dependencies, as well as a complete inventory of their information and technology assets, whether held internally or managed through a third party.
- Breaches will happen, so resilience is key. The ANPR spends considerable time focusing on the steps that covered entities would need to take to plan for, and respond to, cyber attacks. Indeed, the ANPR proposes a two-hour recovery time objective for the so-called "sector critical systems" of covered entities, which could be challenging in practice.
- Technological best practices continue to harden into regulatory requirements. Finally, the ANPR is yet another example of technological best practices hardening into regulatory requirements. Much remains, of course, to be worked out. There is, however, little doubt that some measures previously considered "best practices" will now become legally enforceable obligations on covered entities.

WHAT'S NEXT?

The Agencies are seeking comment from stakeholders on the ANPR, and plan to use the information gathered to develop a more detailed proposal, which will

also be open to public comment. The deadline for submitting comments on the ANPR is January 17, 2017.

* * *

Please do not hesitate to contact us with any questions.