Harvard Law School Forum on
Corporate Governance and Financial Regulation

SUPPORTED BY:
pwc

Banking Agencies' Proposed Cybersecurity Regulations

Posted by Joseph P. Vitale, Schulte Roth & Zabel LLP, on Friday, November 11, 2016

Editor's note: Joseph P. Vitale is a partner at Schulte Roth & Zabel LLP. This post is based on a Schulte Roth publication by Mr. Vitale, Michael L. Yaeger, and Noah N. Gillespie.

On Oct. 19, 2016, the Board of Governors of the Federal Reserve System ("Federal Reserve"), the Office of the Comptroller of the Currency ("OCC") and the Federal Deposit Insurance Corporation ("FDIC," collectively the "Agencies") issued a joint advance notice of proposed rulemaking ("Notice") inviting public comment on cybersecurity regulations and guidance designed to improve the safety and soundness of the U.S. financial system. The Notice includes 39 questions on which the Agencies seek input, including whether the Agencies ultimately issue a formal regulation, guidance or some combination of those tools. That choice will be particularly important as it may determine whether the regulatory regime remains flexible enough for covered entities to adapt to new technologies and evolving threats. The Agencies will receive public comments until Jan. 17, 2017. The Agencies are "considering establishing enhanced standards for the largest and most interconnected entities under their supervision, as well as for services that that these entities receive from third parties."

The Notice proposes a two-tiered framework in which all covered institutions would have to meet a minimum standard, and "those entities that are critical to the functioning of the financial sector," which the Notice refers to as "sector-critical systems," would have to meet with "more stringent standards." The Agencies ambitiously call for entities that provide sector-critical systems to ensure they can recover those systems within two hours of a cyber event and validate their efforts with regular, quantitative testing.

If the Agencies do in fact issue binding standards, they will go beyond the existing, largely nonbinding frameworks that apply to covered institutions, such as the Gramm-Leach-Bliley Act (and the rules promulgated thereunder, including the Interagency Guidelines Establishing Information Security Standards), the Federal Financial Institution Examination Council's IT Handbook and the National Institute of Standards and Technology Cybersecurity Framework. Further, the Agencies are also considering going beyond the Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, written by the Federal Reserve, the OCC, and the Securities and Exchange Commission, which concerned clearing and settlement activities, to address the cyber risks that could impact the largest, most interconnected U.S. financial entities in all their operations.

Who Is Covered

The Agencies propose to apply the new enhanced standards to institutions under their supervision (including non-bank financial institutions) with total consolidated assets of $50 billion or more. In addition, the Federal Reserve proposes to apply the standards to financial market utilities for which it acts as "Supervisory Agent" and other financial market infrastructures over which it has primary supervisory authority or which are operated by the Federal Reserve Banks. Further, the Notice also contemplates defining who is covered based on the overall "number of connections an entity (including its services providers) has to other entities in the financial sector." However, as the notice acknowledges, metrics such as "connections" may be difficult to quantify.

The Notice's enhanced standards apply with equal force to the service providers of any of the above entities. The Agencies also foresee that in some instances, entities that are not covered institutions and thus not themselves subject to the enhanced standards will nonetheless be subject to the highest tier of standards (sector-critical standards) if they "provide services considered sector-critical [either] directly to the financial sector or through covered entities."

Standards Applicable to All Covered Institutions

The Notice outlines five categories of standards that will apply to all covered institutions on an enterprise-wide basis (i.e., across all subsidiaries and affiliates).

Cyber Risk Governance

Many covered entities already have strategic plans and risk governance structures that anticipate and build resilience against shocks that threaten their businesses and operations. The Notice anticipates making it a legal requirement that covered entities approach cyber risk in that same way, and that they continually monitor the residual risk that remains after their efforts at mitigation. To aid the board of director's ability to receive timely and accurate information about cyber risks, the Notice considers "requiring the senior leaders with responsibility for cyber risk to be independent of business line management."

Cyber Risk Management

The Notice encourages covered entities to assess and protect against cyber risk in three overlapping ways. First, covered entities should consider each business unit separately, considering the internal and external assets it depends on in order to understand the risks specific to that business unit. Second, covered entities should integrate cyber risk into their existing independent risk management functions to understand the risks they face on the enterprise level. Finally, regular assessment of cyber risk and the covered entity's cybersecurity program should be a significant component of the covered entity's audit plan. For example, the Agencies are considering requiring covered entities to assess and quantitatively measure the "completeness, effectiveness, and timeliness" with which they reduce the residual and aggregate risk they face so they can demonstrate that they are meeting their board-approved risk levels. Depending on the size, complexity, scope of operations and interconnectedness of the covered entity, such an audit should include penetration testing and other appropriate vulnerability

assessment activities. The Agencies are likewise seeking comment on possible consistent, repeatable methods to measure the cyber risk within covered entities.

Internal Dependency Management

The Notice calls for covered entities to inventory the assets that their operations depend upon, looking both at assets under their control and under the control of third parties. The "internal dependencies" of a covered entity are the "business assets (i.e., workforce, data, technology, and facilities) … upon which such entity depends to deliver services, as well as the information flows and interconnections among those assets." The Agencies would like covered entities to generate and maintain a current, accurate and complete listing of all their internal assets and business functions, including the information flows and interconnections between them, on which the covered entity can map associated risks. Each covered entity should assess the risk of a new asset prior to deployment as well as throughout its lifecycle, attend to all known violations of or deviations from its cybersecurity policy, and regularly test its backup systems.

External Dependency Management

Likewise, the Notice calls for covered entities to inventory and assess their "external dependencies," which are their "relationships with outside vendors, suppliers, customers, utilities (such as power and telecommunications), and other external organizations and service providers that the covered entity depends on to deliver services, as well as the information flows and interconnections between the entity and those external parties." As with internal dependencies, the Notice anticipates that covered entities will inventory and rank the systems outside their direct control to prioritize their cyber risk management efforts.

Incident Response, Cyber Resilience and Situational Awareness

The Notice calls for covered entities to create and implement plans that will allow them to "anticipate, withstand, contain, and rapidly recover from a disruption caused by a significant cyber event." Those plans should consider the impact of "multiple concurrent or widespread interruptions and cyber-attacks" on critical infrastructure, including the U.S. energy and telecommunications grids. Covered entities should also make themselves aware of their connections to sector partners and external stakeholders so that they limit "cyber contagion." The Agencies envision that covered entities will establish recovery time objectives appropriate for each of their systems. Such plans should recognize that malware and corrupted data can propagate through connected systems and should ensure recovery point objectives appropriate to the nature of specific kinds of data so that the covered entity is resilient against attacks that corrupt or destroy important data. Interestingly, the Agencies propose that covered entities store data using a shared defined data standard so that other covered entities or even the FDIC can rapidly take over and carry on the operations of covered entities incapacitated by an attack.

In all of these areas, covered entities must timely identify and assess potential cyber risks to the organization by tracking and analyzing relevant data and learning about current threats and solutions. At various points, the Notice highlights that boards and business lines need to have sufficient personnel with the cybersecurity expertise to properly assess, mitigate and adapt to technology and cyber risks as they evolve. The Notice encourages reporting up pertinent

cybersecurity information to senior management and the board so that the leadership of the covered entity is fully informed of the organization's risks and strategies.

Sector-Critical Standards for Specific Systems

What Makes a System Sector-Critical

The sector-critical standards apply not to institutions or entities but rather to specific systems that would profoundly affect the financial sector if disrupted. Therefore, as noted above, entities not otherwise subject to the enhanced standards may still be required to implement the sector-critical standards for certain of their systems, particularly the third parties that covered entities rely upon to conduct their operations. The Notice proposes several possible metrics for determining which systems are "sector-critical":

- "systems that support the clearing or settlement of at least five percent of the value of transactions (on a consistent basis) in one or more of the markets for federal funds, foreign exchange, commercial paper, U.S. Government and agency securities, and corporate debt and equity securities";
- "systems that support the clearing or settlement of at least five percent of the value of transactions (on a consistent basis) in other markets (for example, exchange-traded and over-the-counter derivatives)";
- systems "that support the maintenance of a significant share (for example, five percent) of the total U.S. deposits or balances due from other depository institutions in the United States";
- "systems that provide key functionality to the financial sector for which alternatives are limited or nonexistent, or would take excessive time to implement (for example, due to incompatibility)"; and
- "systems that act as key nodes to the financial sector due to their extensive interconnectedness to other financial entities."

The Substance of Sector-Critical Standards

The entity that provides a sector-critical system must "substantially mitigate the risk of a disruption due to a cyber event." For example, entities must "establish protocols for secure, immutable, transferable storage of critical records" "including financial records of the institution, loan data, asset management account information, and daily deposit account records, including balances and ownership details" and prioritize maintaining an up-to-date inventory and assessment of the internal and external dependencies of their sector-critical systems.

Perhaps the most striking part of the Notice is the proposal that entities be required to secure, and validate by testing, a recovery time objective of only two hours for sector-critical systems. Thus, covered entities and third parties would have to ensure that their sector-critical systems could return to full operation within two hours of a cyber event "with the overall goal of completing material pending transactions on the scheduled settlement date."

Some sector-critical systems may be outside of U.S. control or at smaller institutions that may have more difficulty reaching the level of resilience the Notice aspires to achieve. For example,

the hackers who robbed more $100 million from the central bank of Bangladesh succeeded by placing malware on the central bank's computers that keylogged the bank's credentials and then placed apparently authenticated SWIFT transfers with the New York Bank of the Federal Reserve over the weekend. While the Federal Reserve and other banks' suspicions prevented a further $869 million in transactions from being completed, the Bangladesh hack illustrates how interconnected the global financial sector is, and how hard it may be to secure a sector-critical system.

Conclusion

The Notice invites public comment on what the Agencies intend to be a robust and wide-reaching policy to enhance the cybersecurity of the U.S. financial sector. The formal regulations, guidance, or other policy the Agencies ultimately issue will likely reach far more entities than the $50 billion-or-greater institutions the Notice aims to protect. The careful thought and openness reflected in the Notice and the 39 questions the Agencies posed to the public indicate that the Agencies are taking cybersecurity seriously and seek to increase the resilience of the U.S. financial sector in a rigorous but practical manner.

The complete publication, including footnotes, is available here.