Michelle W. Cohen Member
michelle@ifrahlaw.com
Ifrah Law PLLC, Washington, DC

US banking regulators consider enhanced cyber risk standards

Recognising the risks to banking entities and their service providers from technology failures and cyber hacks and the need to enforce national standards to protect critical banking services, in October 2016 the Board of Governors of the US Federal Reserve System, the Office of Comptroller of the Currency ('OCC'), and the Federal Deposit Insurance Corporation ('banking agencies') issued a 'Joint advance notice of proposed rulemaking' seeking comment on certain proposals relating to enhanced cyber risk management standards ('Advance NPRM'). Michelle W. Cohen of Ifrah PLLC discusses the Advance NPRM.

Comments on the Advance NPRM[1] are due by 17 January 2017. Following the deadline, the banking agencies will utilise the comments and their own analyses to further refine their proposals. A subsequent notice of proposed rulemaking, followed by a comment period, will precede final, issued rules.

The agencies assert that rules are needed to address cyber security in this industry due to the interconnectedness of the US financial system: unlike other industries, an incident at one interconnected entity may have broad-reaching impacts beyond that particular entity. Thus, the banking agencies issued the Advance NPRM seeking comment on enhanced standards for "the largest and most interconnected entities under their supervision[2]" and for third parties which provide services to those entities. The Advance NPRM proposes a 'tiered' implementation. The most stringent standards would be imposed on those entities that are critical to the functioning of the financial sector, also referred to as 'sector-critical systems.' While the banking agencies have existing programs that contain expectations for cyber security practices at financial institutions and third party service providers, the enhanced standards would be added to the existing framework and would establish more stringent, binding standards.

Coverage

The banking agencies propose to apply enhanced standards to certain entities with total consolidated assets of $50 billion or more - on an enterprise basis. This standard is to cover those entities where a disruption could have "a significant impact on the safety and soundness of the entity, other financial entities, and the U.S. financial sector[3]."

The Advance NPRM proposes that each agency would apply the new standards to the large institutions subject to their jurisdiction. For instance, the Federal Reserve Board could apply the enhanced standards to all US bank holding companies with total consolidated assets of $50 billion or more, the US operations of foreign banking organisations with total US assets of $50 billion or more and all US savings and loan holding companies with total consolidated assets of $50 billion or more. The Board may also apply the standards to non-bank financial companies the Board supervises under the Dodd Frank Act[4].

The OCC proposes to apply the new standards to any national bank, federal savings association or federal branch of a foreign bank that is a subsidiary of a bank holding company or savings and loan holding company with total consolidated assets of $50 billion or more, among others. Similarly, the FDIC is considering applying the standards to any state non-member bank or state saving association that is a subsidiary of a bank holding company or savings and loan holding company with total consolidated assets of $50 billion or more.

Importantly, the banking entities are considering whether to apply the standards to third party service providers which provide services to covered depository institutions and their affiliates. Regarding other financial entities that are not covered by the new standards, those entities (such as community banks) would remain subject to existing guidance, standards and examinations.

Questions posed

The banking agencies seek comment on whether they should consider broadening or narrowing the scope of entities to which the new standards would apply. The Advance NPRM asks what alternative size thresholds could be used, including whether a covered entity under the new requirements could be defined by the 'number of connections' an entity and its service providers have to other entities in the financial sector, versus an asset size standard. The banking agencies also question whether it is preferable to require covered banking entities to maintain service agreements with third party providers rather than applying new requirements directly to the third party providers.

Sector critical standards

The banking agencies propose establishing a two-tiered approach. Enhanced standards would apply to all covered entities' systems. A higher set of expectations, called 'sector-critical standards,' would apply to systems of those covered entities that are deemed 'critical' to the financial sector. Based on prior definitions in the Sound Practices Paper issued in 2003[5], the banking agencies are considering deeming 'critical' (and subject to sector-critical standards) those systems that support the clearing or settlement of at least 5% of the value of transactions in one or more of the markets for federal funds, foreign exchange, commercial paper, US Government and agency securities and corporate debt and equity securities. The agencies may also consider

1. Enhanced Cyber Risk Management Standards, Joint advance notice of proposed rulemaking, https://www.federalreserve.gov/newsevents/press/bcreg/bcreg20161019a1.pdf
2. Advance NPRM at 8.
3. Ibid. at 13.
4. Ibid.
5. Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, available at https://www.sec.gov/news/studies/34-47638.htm
6. Advance NPRM at 25.
7. http://www.wsj.com/articles/u-s-bank-regulator-notifies-congress-of-major-data-security-breach-1477684445
8. 'U.S. Bank Regulator Notifies Congress of Major Data Security Breach,' https://www.donaldjtrump.com/policies/cyber-security

continued

including in this category those systems that support the clearing or settlement of at least 5% of the value of transactions on other markets (e.g., exchange traded and over-the-counter derivatives) or that support the maintenance of a significant share (e.g., 5%) of the total US deposits or balances due from other depository institutions in the US.

The Advance NPRM notes that the agencies may consider other factors to identify sector-critical standards, such as substitutability and interconnectedness. Further, third party service providers that support a covered entity's sector-critical systems would be subject to the same standards. The banking agencies seek comment on several issues relating to coverage of sector-critical standards, including:

- Whether covered entities have access to sufficient information to determine whether any of their systems would be considered sector-critical systems.
- Whether covered entities should self-identify and report their systems are sector-critical, or whether the banking agencies should identify these systems.
- What factors should be considered in measuring interconnectedness.
- How the banking agencies should weigh the costs of imposing sector-critical standards on smaller banking organisations.

Enhanced cyber risk management standards

The proposed standards are organised into five categories:

Cyber risk governance

The agencies are considering rules for financial institutions to develop and maintain a formal cyber risk management strategy and a framework of policies and procedures to implement the strategy. One proposal would be for the board of directors, or a board committee, to approve an entity's cyber risk management strategy and hold senior management accountable for implementing appropriate policies. As an 'enhanced standard,' the banking agencies are considering requiring covered entities to develop a written, board-approved, enterprise-wide cyber risk management strategy. The plan would explain how the entity plans to address its cyber risk and how the entity would maintain an acceptable level of residual cyber risk. The banking agencies are also contemplating requiring the board of directors to review and approve the enterprise-wide cyber risk appetite and tolerances. Importantly, the banking agencies may require the board of directors to have adequate expertise in cyber security or to maintain access to resources or staff having such expertise. (Interestingly, in the last Congress, legislation was introduced to require publicly-traded companies to disclose whether any member of the board is a cyber security expert, although it did not become law).

The banking agencies are also focusing on independence - proposing that those individuals with responsibility for cyber risk oversight be independent of business line management. These individuals would also 'need to have direct, independent access to the board of directors and would independently inform the board of directors on an ongoing basis for the firm's cyber risk exposure and risk management practices [...][6].' In its 'Questions on Cyber Risk Governance,' the banking agencies ask for analyses of the incremental costs and benefits of establishing cyber security expertise (or access to expertise) of the board of directors, and whether covered entities already have governance structures in place that are consistent with the proposed standards.

Cyber risk management

Under proposed enhanced standards, covered entities 'to the greatest extent possible' would be required to integrate cyber risk management into the responsibilities of at least three independent functions. Importantly, a system would need to be in place whereby information regarding risks can be shared with senior management, including the CEO. The banking agencies may require that covered entities establish an independent risk management function, reporting to the chief risk officer and board of directors. Further, the agencies may mandate an audit function to assess whether an entity's cyber risk management complies with applicable laws and regulations, and is appropriate considering the entity's size, interconnectedness, and risk. While these are some suggestions, the banking agencies seek input on several issues, including understanding the types of policies that covered entities currently follow when reporting cyber risks and vulnerabilities to the CEO and board of directors.

Dependency management

The banking agencies are proposing a requirement that a covered entity integrate an internal dependency management strategy into the overall risk management plan. One proposal would require covered entities to maintain an inventory of all business assets prioritised based on how critical the assets are to the business assets supported, the company's mission, and the financial sector. The banking agencies are also considering mandating that covered entities conduct periodic tests of back-ups of their business assets.

Regarding external dependency management, one proposal under consideration is to require that covered entities integrate an external dependency management strategy into the entity's overall risk management plan. The banking agencies also propose requiring covered entities to maintain a current, complete list of all external dependencies and business functions, and to periodically test alternative solutions in case an external partner fails to perform.

Incident response, cyber resilience, and situational awareness

Here, the banking agencies focus on preparedness. The agencies are considering requiring covered entities to establish strategies to allow an entity to meet its core business functions, in the event of a disruption. Several

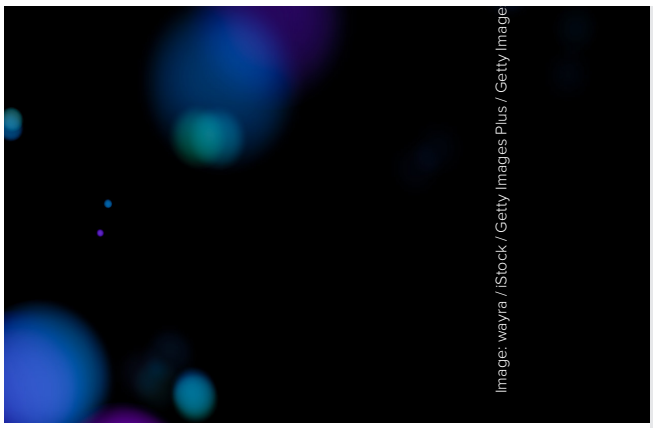
Image: wayra /iStock / Getty Images Plus / Getty Images

methods of preparation are proposed, including mandating that covered entities arrange for secure, offline storage of critical records, such as loan data and daily deposit account records. For 'sector-critical' institutions, the banking agencies may require those entities to establish a recovery time objective ('RTO') of two hours for their sector-critical systems in which to recover from a disruptive cyber event.

Recent developments

About a week after the banking agencies released the Advance NPRM, the Comptroller of the Currency reported a data breach involving more than 10,000 records downloaded by a former employee onto thumb drives in November 2015. This reporting followed several earlier data breaches at the Federal Deposit Insurance Corporation ('FDIC') involving private information of approximately 160,000 Americans, also due to former employee actions[7]. A House of Representatives' investigation revealed significant shortcomings with the FDIC's cyber security practices.

Since the issuance of the Advance NPRM, the US elected a new President, Donald Trump. It is possible the Advance NPRM comment deadline could be pushed back, or that the further rulemaking may be slowed to allow for the Presidential transition. Trump has stated he views cyber security as a priority and he would "order an immediate review of all U.S. cyber defenses and vulnerabilities, including critical infrastructure, by a Cyber Review Team of individuals from the military, law enforcement, and the private sector[8]." Based upon Trump's apparent cyber security focus, the upcoming Presidential and staff transition and the complexity of the Advance NPRM, I anticipate the rulemaking will continue well into the first year and a half/second year of the Trump Administration. However, we can expect further Congressional inquiries and Executive Office studies, particularly in light of the recent breaches at the Comptroller's Office and the FDIC.

Spotlight on Tesco Bank's alleged use of sequential card numbers following attack

Following the cyber attack on Tesco Bank in November 2016, it has been alleged that use of sequential card numbers on Tesco Bank's debit cards might have left users more vulnerable to the attack, according to a Financial Times report on 11 December 2016.

The report claims that issuing sequential card numbers makes it easier for hackers to guess expiry dates and security codes without alerting the bank to risk of fraud. "Typically, banks randomise the long number to make it more difficult for fraudsters to guess them," comments Emma Wright, Partner at Kemp Little. The report states the Financial Conduct Authority ('FCA') has contacted several lenders to check if they are engaging in the practice. "The FCA has detailed requirements about internal risk controls that financial institutions must put in place to protect their systems. Using sequential numbers seems like a fairly basic error," adds Wright.

Tesco Bank was subjected to a sustained cyber attack on 5 November 2016, forcing it to repay £2.5m of losses to 9,000 customers and leading to a criminal investigation by the National Crime Agency. The consequences could be grave as Wright notes, "the FCA can issue unlimited fines if it considers the lack of control and reporting mechanisms in place to identify risks to be particularly serious or can even restrict or revoke an institution's FCA authorisation."

ENISA updates its Good Practice Guide

The European Union Agency for Network and Information Security ('ENISA') published an updated version of its National Cyber Security Strategy Good Practice Guide ('the Guide') on 14 November 2016, which includes a proposed National Cyber Security Strategy ('NCSS') lifecycle.

"The aim of this second version is to support EU Member States in their efforts to develop and update their NCSS and analyses the status of NCSSs in the EU," explains Sofie van der Meulen, Attorney at Law at Axon Lawyers. The Guide presents six steps for the design and development of an NCSS and 15 objectives for implementation.

The first version of the Guide was released in 2012 and the update aims to recognise recent developments, including the adoption of the EU Security of Network and Information Systems Directive in July 2016. Van der Meulen notes "the Guide further underpins the need to increase measures to address cyber threats and draws attention [to] several challenges, such as cooperation and trust between stakeholders and the need for adequate resources."

Van der Meulen believes that "aside [from] providing useful insights for private, civil and industry stakeholders involved in the lifecycle of an NCSS, this guide provides useful information and inspiration for data protection officers."