protiviti®
Face the Future with Confidence

Large banks hit with new cybersecurity rules

October 28, **2016**

Three U.S. financial regulators have proposed new cybersecurity requirements to better protect customers and the broader financial market from online attacks.

The Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency (OCC) and the Federal Deposit Insurance Corporation (FDIC) issued an advanced notice of proposed rulemaking (ANPR) on October 19, 2016, which seeks to enhance cyber risk management standards for large financial services firms and their service providers. With the introduction of the enhanced standards, the supervisors aim to increase firms' operational resilience and reduce the impact on the financial system following a cyber event by requiring firms to prepare for, track and set out how they will respond to cyberattacks. Comments are sought by January 17, 2017.

The standards enhance the cybersecurity requirements originally outlined in the Gramm-Leach-Bliley Act (GLBA) (enacted over 15 years ago) and the Federal Financial Institutions Examination Council (FFIEC) *Information Technology Examination Handbook* (published over 10 years ago). The standards are meant to complement, but not replace, recently developed security guidance such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (released in 2013) and the FFIEC Cybersecurity Assessment Tool (2015).[1] However, the new guidance will implement *binding* minimum requirements for in-scope entities in a tiered manner to differentiate controls for newly defined "sector-critical systems" from all other systems.

Summary of Impact

- The proposed standards would impose minimum cybersecurity standards, building specific requirements based on concepts established in prior guidance.
- While the enhanced standards will be limited at first to large financial institutions and key service providers, it is expected that most other financial institutions will be measured against these same standards by regulators over time.

[1] See the Protiviti white paper, *Understanding the FFIEC Cybersecurity Assessment Tool: An Internal Audit Perspective*: www.protiviti.com/US-en/insights/understanding-ffiec-cybersecurity-assessment-tool.

- The proposed standards shift cyber risks toward a more enterprisewide view and responsibility, referencing the need for institutions to "***establish cyber risk tolerances consistent with the firm's risk appetite and strategy, and manage cyber risk appropriate to the nature of the operations of the firm***."

- To satisfy the enhanced requirements, it is essential for firms' independent risk management functions to ensure they have, and maintain, sufficient independence, stature, authority and resources. They also need direct access to the board of directors to ensure their operations are consistent with their cyber risk management framework. The reporting lines must be *clear and separate* from those of other operations and business units.

- The enhanced standards focus heavily on firms taking a risk-based approach when assessing and managing cyber concerns on their internal and external assets.

- The new rules require a heightened level of focus on cyber threats and "situational awareness," inferring that companies should build a flexible cyber risk management framework that can evolve alongside the changing threat environment.

Scope of Application

The Federal Reserve Board proposes to apply the enhanced standards on all U.S. bank holding companies (BHC) and U.S. savings and loan holding companies (SLHC) with total consolidated assets of $50 billion or more on an enterprise basis, as well as U.S. operations of foreign banking organizations, again with total U.S. assets of $50 billion or more. The board is also considering implementing the enhanced standards to nonbank financial companies and financial market utilities designated by the Financial Stability Oversight Council (FSOC), an agency of the U.S. Treasury Department, as performing critical functions for the U.S. financial system and financial market infrastructures, such as clearing and third-party payment service providers.

The OCC is considering applying standards to national banks, federal savings associations and their subsidiaries, or federal branches of a foreign bank subsidiary of a BHC or SLHC with $50 billion or more in total consolidated assets. This is in addition to national banks and federal savings associations and federal branches of foreign banks that do not have a parent holding company.

The FDIC proposes to also apply the standards to any state non-member bank or state savings association that is a BHC or SLHC subsidiary with assets of $50 billion or more, as well as those same organizations that do not have a holding company subsidiary.

As already mentioned, some third-party service providers will also be considered as part of the scope of application. Other financial entities, including community banks that are not covered entities, will continue to be subject to existing guidance and standards.

The Enhanced Standards

The enhanced cyber risk management standards proposed in the ANPR address five focus categories: cyber risk governance; cyber risk management; internal dependency management; external dependency management; and incident response, cyber resilience and situational awareness.

The five categories are examined in detail below:

Cyber Risk Governance

The new rules require firms to develop and maintain a formal cyber risk management strategy to underpin a robust cyber risk governance framework, which is integrated into the firm's overall strategic plan and risk governance structures. Financial institutions will be required to:

- Ensure that the board of directors or an appropriate board committee is responsible for approving the company's cyber risk management strategy and holding senior management accountable for establishing and implementing appropriate policies consistent with the strategy.
- Require the board of directors to have adequate cybersecurity expertise or to ensure access to resources or staff with such knowledge.
- Appoint a senior leader or leaders with responsibility for cyber risk oversight who are independent of business line management and who have direct, independent access to the board of directors to inform them of the firm's cyber risk exposure and risk management practices, including known and emerging issues and trends, on an ongoing basis.
- Develop a written, board-approved, enterprisewide cyber risk management strategy that articulates how the firm intends to address its inherent cyber risk, maintain an acceptable level of residual cyber risk and sustain resilience on an ongoing basis.
- Establish cyber risk tolerances consistent with the firm's risk appetite and strategy, and manage cyber risk appropriate to the nature of the operations of the firm.
- Reduce its residual cyber risk to the appropriate level approved by the board of directors.
- Identify and assess those activities and exposures that present cyber risk, and determine ways to assess the entity's residual cyber risk.
- Establish an enterprisewide cyber risk management framework that includes policies and reporting structures to support and implement the entity's cyber risk management strategy.

- Include mechanisms for identifying and responding to cyber incidents and threats within the cyber risk management framework, incorporating procedures for testing effectiveness and updating them as the threat landscape evolves.

Cyber Risk Management

The enhanced standards require firms to integrate cyber risk management into the responsibilities of at least three independent functions – the business units, risk management and internal audit – with appropriate checks and balances.

Business Units

The first line of defense, the business units, will have increased responsibilities for the management of cyber risk under the new rules. They will be required to:

- Assess the cyber risks associated with business unit activities and share risk information with senior management, including the chief executive officer, in a "timely manner" and on an ongoing basis, to enable senior management to address and respond to emerging cyber risks and cyber incidents as they develop.

- Adhere to procedures and processes necessary to comply with the firm's cyber risk management framework, which should be designed to ensure that the applicable business unit's cyber risk is effectively identified, measured, monitored and controlled and is consistent with the firm's risk appetite and tolerances.

- Assess the cyber risks and potential vulnerabilities associated with every business asset (workforce, data, technology and facilities), service and IT connection point, and update these assessments as threats, technology and processes evolve.

Independent Risk Management

The rules require firms to incorporate enterprisewide cyber risk management into the responsibilities of an independent risk management function, which will report to the chief risk officer and the board of directors on the implementation of the firm's cyber risk management framework throughout the organization.

The independent risk management function would be required to:

- Analyze cyber risk at the enterprise level to identify and ensure effective response to events with the potential to impact one or multiple operating units.

- Continually assess the firm's overall exposure to cyber risk and promptly notify the CEO and the board of directors when its assessment of a particular cyber risk differs from that of a business unit, as well as of any instances when a unit has exceeded the firm's established cyber risk tolerances.

- Continuously identify, measure and monitor cyber risk across the enterprise, and determine whether cyber risk controls are appropriately in place across the enterprise and are consistent with the entity's established risk appetite and tolerances.
- Identify and assess the firm's material aggregate risks on an ongoing basis and determine whether actions need to be taken to strengthen risk management or reduce risk given changes in the firm's risk profile or other conditions.
- Establish and maintain an up-to-date understanding of the structure of a firm's cybersecurity programs and supporting processes and systems, as well as their relationships to the evolving cyber threat landscape.
- Create and maintain sufficient independence, stature, authority, resources and access to the board of directors to ensure that the operations of the entity are consistent with the cyber risk management framework.

Audit Function

The third line of defense plays a key role in risk management, internal control and corporate governance. Internal audit will be required to:

- Evaluate the effectiveness of risk management, internal controls and governance processes.
- Advise management and the board of directors on whether a firm's policies and procedures are adequate to keep up with emerging risks and industry regulations.
- Assess whether the cyber risk management framework complies with applicable laws and regulations and is appropriate for its size, complexity, interconnectedness and risk profile.
- Incorporate an assessment of cyber risk management into the firm's overall audit plan. The evaluation would be required to include the entire security lifecycle, including penetration testing and other vulnerability assessment activities as appropriate based on the size, complexity, scope of operations and interconnectedness of the covered entity; the audit plan would be required to provide for an assessment of the business unit and independent risk management functions' capabilities to adapt as appropriate and remain in compliance with the covered entity's cyber risk management framework and within its stated risk appetite and tolerances.

Internal Dependency Management

Internal dependency refers to a firm's business assets – workforce, data, technology and facilities – as well as the information flows between them. The proposed standards aim to ensure firms have effective capabilities in place to identify and manage cyber risks associated with their business assets, which arise from a wide range of sources, including insider threats, data transmission errors or the use of legacy

systems acquired through a merger, for example. The focus here is on the continuous risk assessment of firms' business assets.

Under the new rules, firms will be required to:

- Integrate an internal dependency management strategy into the entity's overall strategic risk management plan. This strategy would define the roles and responsibilities for internal dependency management; establish policies, standards and procedures to identify and manage cyber risks associated with internal assets, including those connected to or supporting sector-critical systems; monitor effectiveness in reducing cyber risks associated with internal dependencies; and set up appropriate compliance mechanisms.
- Develop and maintain a current and complete awareness of all internal assets and business functions that support a firm's cyber risk management strategy.
- Track connections among assets and cyber risk levels throughout the lifecycles of the assets and support relevant data collection and analysis across the organization, which would help establish and implement mechanisms to prioritize monitoring, incident response and recovery of systems critical to the firm and to the financial sector.
- Support the reduction of the cyber risk exposure of business assets to the enterprise and the sector until the board-approved risk appetite and tolerances are achieved.
- Establish and apply appropriate controls to address the inherent cyber risk of firms' assets by: assessing the cyber risk of assets and their operating environments prior to deployment; continually applying controls and monitoring assets and their operating environments over the lifecycle of the assets; assessing relevant cyber risks to the assets (including insider threats to systems and data); and mitigating identified deviations, granted exceptions and known violations to internal dependency cyber risk management policies, standards, and procedures.
- Continually apply appropriate controls to reduce the cyber risk of business assets and periodically conduct tests of back-ups to business assets to achieve resilience.

External Dependency Management

"External dependencies" refers to firms' relationships with outside vendors, suppliers, customers, utilities, and other external organizations and service providers they depend on to deliver services, as well as the information flows and interconnections between the company and its external parties. This category includes the management of interconnection risks associated with noncritical external parties that maintain trusted connections to important systems.

Firms will be required to integrate an external dependency management strategy into their overall strategic risk management plans to address and reduce cyber risks associated with external

dependencies and interconnection risks. As part of an external dependency management strategy, firms are required to:

- Establish effective policies, plans and procedures to identify and manage real-time cyber risks associated with external dependencies, particularly those connected to or supporting sector-critical systems and operations, throughout their life spans.
- Monitor in real-time all external dependencies and trusted connections that support the firm's cyber risk management strategy.
- Develop and maintain a current, accurate and complete awareness of, and prioritize, all external dependencies and trusted connections enterprisewide based on their criticality to the business functions they support, the firm's mission and the financial sector.
- Prioritize monitoring, incident response and recovery of systems critical to the enterprise and the financial sector.
- Support the continued reduction of the cyber risk exposure of external dependencies to the enterprise and the sector until the board-approved cyber risk appetite and tolerances are achieved.
- Monitor the universe of external dependencies that connect to assets supporting systems critical to the enterprise and the sector.
- Establish and apply appropriate controls to address the cyber risk presented by each external partner throughout the life span of the relationship.
- Identify and periodically test alternative solutions in case an external partner fails to perform as expected.

Incident Response, Cyber Resilience and Situational Awareness

Standards within the incident response, cyber resilience and situational awareness category are designed to ensure firms plan for, respond to, contain and rapidly recover from disruptions caused by cyber incidents. This seeks to strengthen firms' cyber resilience as well as that of the financial sector. Financial institutions will be required to be capable of operating critical business functions in the face of cyberattacks and continuously enhance their cyber resilience. Additionally, firms will be required to establish processes designed to maintain effective situational awareness capabilities to reliably predict, analyze and respond to changes in the operating environment.

Under the proposals, firms will be required to:

- Establish and implement plans to identify and mitigate the cyber risks they pose through interconnectedness to sector partners and external stakeholders to prevent cyber contagion.

- Establish and maintain enterprisewide cyber resilience and incident response programs, which are supported by appropriate policies, procedures, governance, staffing and independent review. These programs would be required to include effective escalation protocols linked to organizational decision levels, cyber contagion containment procedures, communication strategies and processes to incorporate lessons learned back into the program.

- Establish plans to address recovery and resilience strategies for cyberattacks that may disrupt access, corrupt data or destroy data or systems. Firms are further required to establish recovery time objectives (RTOs) with recovery and resilience strategies, which address the potential for malware or corrupted data to replicate or propagate through connected systems or high-availability solutions.

- Establish and implement strategies to meet the firm's obligations for performing core business functions in the event of a disruption, including the potential for multiple concurrent or widespread interruptions and cyberattacks on multiple elements of interconnected critical infrastructure, such as energy and telecommunications.

- Establish protocols for secure, immutable, offline 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, formatted using certain defined data standards to allow for restoration of these records by another financial institution, a service provider or the FDIC in the event of resolution.

- Establish plans and mechanisms to transfer business, where feasible, to another entity or service provider with minimal disruption and within prescribed time frames if the original covered entity or service provider is unable to perform.

- Conduct specific testing that addresses disruptive, destructive, corruptive, or any other cyber event that could affect their ability to service clients.

- Maintain an ongoing situational awareness of the firm's operational status and cybersecurity posture to pre-empt cyber events and respond rapidly to them.

- Establish and maintain threat profiles for identified threats to the firm, establish and maintain threat-modeling capabilities, gather actionable cyberthreat intelligence and perform security analytics on an ongoing basis, and establish and maintain capabilities for ongoing vulnerability management.

Sector-Critical Standards

Under its proposed tiered implementation approach, all firms in scope will be subject to the enhanced standards, but those organizations defined as sector-critical systems will be subject to a higher set of expectations.

These sector-critical standards include requirements for firms to:

- Implement the most effective, commercially available controls.
- Establish an RTO of two hours for their sector-critical systems, validated by testing, to recover from a disruptive, corruptive or destructive cyber event. Testing programs would include a range of scenarios, including severe but plausible scenarios, and would challenge matters such as communications protocols, governance arrangements, and resumption and recovery practices.
- Measure (quantitatively) their ability to reduce the aggregate residual cyber risk of their sector-critical systems and their ability to reduce such risk to a minimal level, which would also take into account the risks associated with internal dependencies, external dependencies and trusted connections with access to sector-critical systems.

Implementation

The ANPR proposes various methods of implementation for these enhanced standards, which range from a policy statement or guidance to a detailed regulation imposing specific cyber risk management standards. Under the latter, the agencies could propose a regulatory framework, which would include details on the specific objectives and practices a firm would be required to achieve. The ANPR states that it would consider the clarity and potential costs and other burdens to firms with each option when making the final decision.

About Protiviti

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders face the future with confidence. Through our network of more than 70 offices in over 20 countries, Protiviti and our independently owned Member Firms provide our clients with consulting solutions in finance, technology, operations, data analytics, governance, risk and internal audit. We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies.

We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Contacts

Cory Gunderson
Managing Director and Global Financial Services Practice Leader
+1.212.708.6313
cory.gunderson@protiviti.com

Ed Page
Managing Director and Financial Services Industry IT Practice Leader
+1.312.476.6093
ed.page@protiviti.com

Scott Laliberte
Managing Director and Leader, IT Security and Privacy Practice
+1.267.256.8825
scott.laliberte@protiviti.com

Andrew Retrum
Managing Director
+1.312.476.6353
andrew.retrum@protiviti.com

Randy Armknecht
Director
+1.312.476.6428
randy.armknecht@protiviti.com

protiviti®