Cybersecurity and Privacy News

Financial industry cybersecurity concerns grow, New York acts

By J. Preston Carter, J.D., LL.M., Mark S. Nelson, J.D., John M. Pachkowski, J.D.

Inside

Executive Summary

With growing concerns over cyber risks, federal and state regulators have increased efforts to develop new cybersecurity standards. New York became the first state to require banks, insurance companies, and other regulated financial institutions to establish and maintain a cybersecurity program to protect consumers and the industry, with regulations taking effect March 1, 2017. Meanwhile, federal banking regulators are considering cyber risk management standards and resilience standards for large financial institutions and their service providers. In addition, the Securities and Exchange Commission has adopted regulations to strengthen the technology infrastructure of the securities markets, and the Commodity Futures Trading Commission has adopted related rules on system safeguards.

This White Paper will discuss New York's new requirements, explore issues under consideration by federal banking agencies, and explain requirements imposed by federal securities and commodities regulators.

Introduction

A recent survey by Deloitte & Touche LLP of trends in risk management practices noted "Banks, securities companies, investment management firms, insurers, and payment and clearing systems are prime targets for cybercriminals looking to steal money or data, or compromise critical infrastructure, spurred by the large amounts of money involved and the increased use of online and mobile banking." The Deloitte survey added that "[i]mproving management of cybersecurity risks has been an increasing concern of financial services institutions and has also been receiving greater attention from regulators and policy setters." Given these increased concerns, federal and state regulators have increased efforts to develop new cybersecurity standards.

New York's financial services industry cybersecurity regulation takes effect

New York State's first-in-the-nation cybersecurity regulation took effect March 1, 2017. Intended to protect New York's financial services industry and consumers from cyberattacks, the regulation requires banks, insurance companies, and other financial services institutions regulated by the Department of Financial Services to establish and maintain a cybersecurity program designed to protect consumers' private data and ensure the safety and soundness of New York's financial services industry.

The final risk-based regulation (23 NYCRR 500) includes certain regulatory minimum standards while encouraging firms to keep pace with technological advances. It also provides protections to prevent cyber breaches, including:

- controls relating to the governance framework for a robust cybersecurity program, including requirements for a program that is adequately funded and staffed, overseen by qualified management, and reported on periodically to the most senior governing body of the organization;
- risk-based minimum standards for technology systems, including access controls, data protection including encryption, and penetration testing;
- required minimum standards to help address any cyber breaches, including an incident response plan, preservation of data to respond to such breaches, and notice to the DFS within 72 hours of material events; and
- accountability, by requiring identification and documentation of material deficiencies, remediation plans, and annual certifications of regulatory compliance to the DFS.

Who is covered? The regulation defines covered entities as "any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law." (Sec. 500.01) Under this definition, the rules would apply to New York State-chartered or licensed banks, insurance companies, licensed lenders, check cashers, and money transmitters, but not to federally-chartered institutions.

Exemptions—Covered entities with fewer than 10 employees, including independent contractors; less than $5 million in gross revenue in each of the last 3 fiscal years; or less than $10 million in year-end assets are exempted from some, but not all, of the regulation's requirements.

72-hour breach response required

Other exemptions:

- An employee, agent, representative, or designee is exempt to the extent that it is covered by the cybersecurity program of a covered entity.
- A covered entity that does not utilize information systems or access nonpublic information is exempt from the requirements of certain enumerated sections.
- A covered entity under Article 70 of the Insurance Law that does not access nonpublic information other than information relating to its corporate parent company is also exempt from the requirements of certain enumerated sections.
- Provided they do not otherwise qualify as a covered entity, persons subject to Insurance Law section 1110 or 5904 and any reinsurer accredited or certified pursuant to 11 NYCRR 125 are exempt from the requirements.

A covered entity must file a notice of exemption as set forth in Appendix B of the regulation within 30 days of the determination that it is exempt. If a covered entity ceases to qualify for an exemption, it has 180 days from the end of the fiscal year of disqualification to comply with all applicable requirements of the regulation. (Sec. 500.19)

What information is covered? The cybersecurity programs must protect nonpublic information stored in a covered entity's information system.

Nonpublic information—Nonpublic information means all electronic information that is not publicly available and is:

1. business related information that, if disclosed, would cause a material adverse impact to the covered entity's business, operations, or security;
2. any information concerning an individual that because of name, number, personal mark, or other identifier can be used to identify that individual, in combination with any one or more of the following data elements: (i) Social Security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit, or debit card number, (iv) any security code, access code, or password that would permit access to an individual's financial account, or (v) biometric records; or
3. any information or data, except age or gender, derived from a health care provider or an individual and that relates to the physical, mental, or behavioral health or condition of any individual or a member of the individual's family, the provision of health care to any individual, or payment for the provision of health care to any individual.

Information system—A covered entity's information system is defined as a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems. (Sec. 500.01)

What must covered entities do to comply?
Each covered entity must maintain a cybersecurity program designed to protect the confidentiality, integrity, and availability of its information systems. (Sec. 500.02)

Cybersecurity program—The program must be based on the entity's risk assessment and perform the following core cybersecurity functions:

1. identify and assess internal and external cybersecurity risks that may threaten the security or integrity of nonpublic information stored on the covered entity's information systems;

Third-party vendors must meet 'minimum cybersecurity practices'

2. use infrastructure, policies, and procedures to protect the covered entity's information systems and nonpublic information from unauthorized access or use;
3. detect cybersecurity events, which are any acts or attempts to gain unauthorized access to, disrupt, or misuse an information system or information stored on it;
4. respond to identified or detected cybersecurity events to mitigate any negative effects;
5. recover from cybersecurity events and restore normal operations and services; and
6. fulfill regulatory reporting obligations. (Sec. 500.02)

Implement a cybersecurity policy—Each covered entity must implement and maintain a written cybersecurity policy setting forth its procedures to protect its information systems and nonpublic information stored on the systems. The policy must be based on the covered entity's risk assessment and address specified areas to the extent applicable. (Sec. 500.03)

Designate a Chief Information Security Officer—Each covered entity must designate a Chief Information Security Officer (CISO), who may be employed by the entity, an affiliate, or a third party service provider. The CISO is responsible for overseeing and implementing the covered entity's cybersecurity program and must, at least annually, develop a written report, for internal review, which addresses specified cybersecurity issues. (Sec. 500.04)

Conduct penetration testing and vulnerability assessments—The cybersecurity program must include continuous monitoring or periodic penetration testing and vulnerability assess-

ments. In penetration testing, assessors try to circumvent or defeat the security features of an information system. If an entity does not continuously monitor changes in information systems to detect vulnerabilities, it must conduct annual penetration testing and a bi-annual vulnerability assessment. (Sec. 500.05)

Leave an audit trail—Each covered entity must securely maintain systems that reconstruct material financial transactions (for at least five years) and include audit trails designed to detect and respond to cybersecurity events that have a reasonable likelihood of materially harming any material part of the entity's normal operations (for at least three years). (Sec. 500.06)

Limit access privileges—User access privileges to information systems that provide access to nonpublic information must be limited and periodically reviewed. (Sec. 500.07)

Ensure security of applications—The cybersecurity program must include written procedures and standards to ensure the use of secure development practices for in-house developed applications, and for evaluating the security of externally developed applications that are used in the covered entity's technology environment. (Sec. 500.08)

Conduct periodic risk assessments—Each covered entity must conduct periodic risk assessments to consider cybersecurity risks facing the entity; criteria for assessing the confidentiality, integrity, security, and availability of the entity's information systems and nonpublic information; and requirements describing how these risks will be addressed. (Sec. 500.09)

Employ qualified cybersecurity personnel and intelligence—Each covered entity must utilize qualified cybersecurity personnel, provide them with cybersecurity updates and training, and verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures. (Sec. 500.10)

Develop third-party service provider security policies—Third-party vendors must meet "minimum cybersecurity practices." Policies and procedures must be developed to ensure the security of information systems and nonpublic information accessible to third-party service providers. Those policies must be based on the entity's risk assessment and include guidelines for due diligence and/or contractual protections relating to those service providers. (Sec. 500.11)

Some exemptions for smaller companies

Utilize multi-factor authentication—To protect against unauthorized access to information, each covered entity must utilize multi-factor authentication for any individual accessing the entity's internal networks from an external network, unless the entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls. (Sec. 500.12)

Limit data retention—As part of its cybersecurity program, each covered entity must include policies for the secure disposal on a periodic basis of any nonpublic personally identifiable or health information that is no longer necessary for business operations, except where the information is otherwise required by law to be retained, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained. (Sec. 500.13)

Train and monitor—Also, as part of its cybersecurity program, each covered entity must implement risk-based policies and procedures to monitor the activity of authorized users and detect unauthorized access or use of nonpublic information, and must provide regular cybersecurity awareness training for all personnel. (Sec. 500.14)

Encrypt nonpublic information—Each covered entity must implement controls, based on its risk assessment, to protect nonpublic information held or transmitted by the entity both in transit over external networks and at rest. Controls include encryption, but if encryption is infeasible, the CISO can approve compen-

sating controls, which the CISO must review annually. (Sec. 500.15)

Establish an incident response plan—Each covered entity must establish a written incident response plan addressing specified areas. The plan must be designed to promptly respond to, and recover from, any cybersecurity event materially affecting the confidentiality, integrity, or availability of the entity's information systems or the continuing functionality of any aspect of its business or operations. (Sec. 500.16)

Give notice of cybersecurity events—A covered entity must notify the Superintendent of Financial Services as promptly as possible but no later than 72 hours after a determination that a cybersecurity event has occurred that either:

- impacts the covered entity of which notice is required to be provided to any government body, self-regulatory agency, or any other supervisory body; or
- has a reasonable likelihood of materially harming any material part of the entity's normal operation. (Sec. 500.17)

Submit annual notice of certification—By February 15 of each year, beginning in 2018, each entity must submit to the superintendent a written statement covering the prior calendar year, certifying that the entity is in compliance with the regulation's requirements. The entity must also maintain for examination by the DFS all records, schedules, and data supporting the certificate for a period of five years. (Sec. 500.17)

Confidentiality. Information provided by a covered entity pursuant to these rules is subject to exemptions from disclosure under the Banking Law, Insurance Law, Financial Services Law, Public Officers Law, or any other applicable state or federal law. (Sec. 500.18)

Enforcement. The rules will be enforced by the superintendent. (Sec. 500.20)

When is compliance required? Compliance is phased in over periods measured from the final rule's March 1, 2017, effective date. (Secs. 500.21 and 500.22). Compliance and reporting deadlines are as follows:

180 days: Aug. 28, 2017—establish a cybersecurity program and cybersecurity policy; designate a CISO; establish limits on access privileges; employ qualified cybersecurity personnel and intelligence; and establish an incident response plan.

Feb. 15, 2018—submit certification of compliance with requirements effective Aug. 28, 2017.

1 year: March 1, 2018—receive the CISO's first annual report; conduct penetration testing, vulnerability assessment, and risk assessment; implement multi-factor authentication; and provide personnel training.

18 months: Sept. 1, 2018—establish an audit trail; secure applications; limit data retention; implement monitoring of authorized user activities; and encrypt nonpublic information.

Feb. 15, 2019—submit certification of compliance with all requirements effective as of Sept. 1, 2018.

2 years: March 1, 2019—develop third-party service provider security policies.

Feb. 15, 2020—submit certification of compliance with all requirements. (Secs. 500.21 and 500.22)

Banking agencies shape parameters of enhanced cyber risk management standards

Recognizing the interconnectedness of the U.S. financial system and that a cyber incident or failure at one interconnected entity may not only impact the safety and soundness of the entity, but also have potentially systemic consequences for others, the OCC, Fed, and FDIC issued an Advance Notice of Proposed Rulemaking (ANPR), in October 2016, that could result in certain financial institutions being required to establish enhanced cyber risk management standards.

The enhanced standard would increase the operational resilience of these entities and

reduce the impact on the financial system of a cyber event experienced by one of these entities. The agencies envision that the enhanced standards would be applied in a two-tiered approach imposing more stringent standards on the systems of those entities that are critical to the functioning of the financial sector.

Interplay with agencies' cybersecurity guidance. The enhanced standards would be another supervisory program that would govern cybersecurity practices at financial institutions.

Currently, information technology risk is assessed under the Uniform Rating System for Information Technology (URSIT) standards. The URSIT framework includes elements to assess data security and other risk management factors necessary to determine the quality, integrity, and reliability of the financial institution's or third-party service provider's IT. The agencies noted that the proposed enhanced standards would not replace the URSIT ratings but could be used, in part, to inform the cyber-related elements of the URSIT rating for covered entities.

Other agency guidance documents that would be complemented by the enhanced standards include:

- The FFIEC's IT Handbook, which provides guidance to examiners in reviewing financial institutions and services provided by third parties.
- The *Interagency Guidelines Establishing Information Security Standards,* which implement provisions of the Gramm-Leach-Bliley Act that required the banking agencies to establish appropriate administrative, technical, and physical controls to safeguard financial institutions' customer information.
- The FFIEC Cybersecurity Assessment Tool, which helps institutions identify their risks and determine their cybersecurity preparedness by providing a repeatable and measurable process for financial institutions to measure their cybersecurity preparedness over time.

In addition to the various agency guidance, the OCC, Fed, and FDIC relied on the *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* that was issued by the OCC, Fed, and SEC in April 2003, commonly referred to as the "Sound Practices Paper." The paper was issued in response to the September 11th terrorist attacks and focused on minimizing the immediate systemic effects of a wide-scale disruption of critical financial markets and on establishing the appropriate back-up capacity for recovery and resumption of clearance and settlement activities in wholesale financial markets. The agencies noted that they took the Sound Practices Paper into consideration as they developed the proposed enhanced standards.

Enhanced standards complement existing cybersecurity guidance

Covered entities. The enhanced standards would apply to a discrete segment of the financial system, namely entities with total assets on a consolidated basis of $50 billion or more. The $50 billion asset threshold would apply on an enterprise-wide basis, since cyber risks in one part of an organization could expose other parts of the organization to harm.

Agency-supervised institutions—The following entities, if they meet the asset threshold, would be subject to the enhanced standards:

- U.S. bank holding companies;
- U.S. operations of foreign banking organizations;
- U.S. savings and loan holding companies;
- national banks;
- federal savings associations;
- federal branches;
- state member banks; and
- state nonmember banks.

According to the most recent data published by the Fed, as of Sept. 30, 2016, there were 36 BHC/bank combinations that meet the $50 billion asset threshold.

In addition to the financial institutions supervised by the three banking agencies, any sub-

sidiaries of these financial institutions would be subject to enhanced standards.

The Fed is also considering applying the enhanced standards to financial market utilities (FMUs) designated by the Financial Stability Oversight Council for which the Fed is the Supervisory Agency pursuant to the Dodd-Frank Act.

Service providers—As part of the regulatory process, the agencies are considering whether to apply the enhanced standards to third-party service providers when they provide services to depository institutions and their affiliates that are covered entities. The agencies noted that this treatment would "ensure consistent, direct application of the standards regardless of whether a depository institution or its affiliate conducted the operation itself, or whether it engaged a third-party service provider to conduct the operation." They added, "Direct application of the standards to these service providers could have potential benefits, including facilitating supervisory action in the event that a covered service was not meeting a proposed standard and establishing an obligation for meeting the standard on the depository institution or its affiliate, as well as on the third-party provider of the covered service."

Community banks—The agencies were explicit in their ANPR that community banks would not be covered by the enhanced standards, but that these banks would still continue to be subject to existing guidance, standards, and examinations related to the provision of banking services by third parties.

Focus of enhanced standards. The enhanced standards would require covered entities to:

- demonstrate effective cyber risk governance;
- continuously monitor and manage their cyber risk within the risk appetite and tolerance levels approved by their boards of directors;
- establish and implement strategies for cyber resilience and business continuity in the event of a disruption;
- establish protocols for secure, immutable, transferable storage of critical records; and
- maintain continuing situational awareness of their operational status and cybersecurity posture on an enterprise-wide basis.

Enhanced standard seek to increase the operational resilience and reduce impact of cyber events

Enhanced standard categories. The enhanced standards would cover five categories of the cyber 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.

Category 1: Cyber risk governance—The cyber risk governance category would articulate the strategy that a covered entity would take to maintain an acceptable level of residual cyber risk—the entity's remaining cyber risk after mitigating controls—and maintain resilience on an ongoing basis. This would entail participation by the board of directors, who would review and approve the covered entities' risk appetite and tolerance.

Category 2: Cyber risk management—In general, the enhanced standards would require covered entities to integrate cyber risk management into the responsibilities of at least three independent functions, such as the three lines of defense risk-management model. The three lines of defense risk-management model emphasizes operational management, risk management and compliance, and an audit function.

The agencies noted integrating cyber risk management into the three lines of defense risk-management model would allow covered entities to more accurately and effectively identify, monitor, measure, manage, and report on cyber risk.

As part of the Category 2 requirements, the agencies are considering explicitly requiring

the audit function to assess whether the cyber risk management framework of a covered entity complies with applicable laws and regulations and is appropriate for the entity's size, complexity, interconnectedness, and risk profile.

Category 3: Internal dependency management—For purposes of the enhanced standards, the term "internal dependency" refers to a covered entity's business assets—workforce, data, technology, and facilities—that the covered entity depends upon to deliver services, as well as the information flows and interconnections among those assets.

Standards within the internal dependency management category are intended to ensure that covered entities have effective capabilities in place to identify and manage cyber risks associated with their business assets throughout those assets' lifespans. Another key aspect of the internal dependency management category is having current and complete awareness of all internal assets and business functions that support a firm's cyber risk management strategy.

Category 4: External dependency management—The term "external dependency" refers to a covered entity's 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.

Standards within the external dependency management category are intended to ensure that covered entities have effective capabilities in place to identify and manage cyber risks associated with their external dependencies and interconnection risks throughout these relationships. In addition, the standards would seek to ensure that covered entities continually assess and improve, as necessary, their effectiveness in reducing the cyber risks associated with external dependencies and interconnection risks enterprise-wide.

Category 5: Response, resilience, and situational awareness—Standards within the incident response, cyber resilience, and situational awareness category would be designed to ensure that covered entities plan for, respond to, contain, and rapidly recover from disruptions caused by cyber incidents, thereby strengthening their cyber resilience as well as that of the financial sector.

Community banks would be not covered by the enhanced standards

A covered entity would fulfill the standards under this category if it can demonstrate the capability to operate critical business functions in the face of cyberattacks and continuously enhance their cyber resilience. In addition, a covered entity would be required to establish processes designed to maintain effective situational awareness capabilities to reliably predict, analyze, and respond to changes in the operating environment.

Sector-critical standards. The second tier of the enhanced cyber risk management standards would impose more stringent standards for systems of covered entities that are critical to the functioning of the financial sector. One of the more stringent standards would require covered entities to minimize "residual cyber risk," which means substantially mitigating the risk of a disruption or failure due to a cyber event.

A second sector-critical standard would require covered entities to establish a recovery time objective, or RTO, of two hours for their sector-critical systems to recover from a disruptive, corruptive, or destructive cyber event. The ability to meet the two-hour RTO should be validated by testing. The two-hour time period is comparable to the RTO called for in the Sound Practice Paper.

Takeaways. The agencies' ANPR is only the first step in the regulatory process. The agencies are currently analyzing a number of comments submitted by various stakeholders. Any future Notice of Proposed Rulemaking will no doubt take into account the comments submitted by the stakeholders.

Although the agencies explicitly stated that the enhanced standards would not apply to community banks, there are always industry concerns that standards set for only a small subset of financial institutions would be construed as a "floor" and that slowly those standards would eventually apply to the whole of the industry.

The ANPR sought comments on how best to implement the enhanced standards. The agencies provided three possible approaches:

- propose the standards in combination with a regulatory requirement to maintain a risk management framework;
- propose regulations that impose specific cyber risk management standards; or
- propose a regulatory framework that includes details on the specific objectives and practices a firm would be required to achieve in each area of concern in order to demonstrate that it maintains an appropriate cyber risk management program.

It should be noted, however, that the current attitude toward the "regulatory state," expressed in President Trump's executive actions, might chill any further action on the enhanced standards.

SEC and CFTC rules emphasize resiliency of securities and commodities markets

The Securities and Exchange Commission and the Commodity Futures Trading Commission have both adopted final rules implementing new requirements aimed at focusing key market participants' attention on the resiliency of their cybersecurity-related systems and controls. For the SEC, these requirements are contained in Regulation Systems Compliance and Integrity (SCI), which modernized the prior approach taken by the agency in its Automation Review Policy (ARP). The CFTC's similar requirements are housed in two regulations known as System Safeguards Testing Requirements, which apply to two different sets of market participants (Exchange Final Rules; Clearing Final Rules).

Regulation SCI—The SEC's Regulation SCI contains basic requirements for SCI entities, including reporting and review provisions, and key implementation dates. The SEC also published an FAQ and additional guidance on Regulation SCI. But securities regulations applicable in the cybersecurity setting go beyond Regulation SCI. Disclosure, enforcement, and corporate governance issues are discussed in more detail below.

The SEC's Regulation SCI contains basic requirements for SCI entities ... But securities regulations applicable in the cybersecurity setting go beyond Regulation SCI.

Rule 1005 of Regulation SCI also imposes recordkeeping requirements under which SCI SROs must keep related documents pursuant to Exchange Act Rule 17a-1, and non-SCI SROs must keep one copy of all relevant documents for five years. All entities subject to Regulation SCI must promptly furnish requested documents to the Commission. Records also must remain accessible to the Commission even after an entity is no longer in business or has ended its registration with the Commission. Rule 1002(b)(5) also prescribes a record keeping requirement for no or de minimis SCI events. Moreover, Regulation SCI contains numerous notification and reporting requirements.

The CFTC's System Safeguards—Meanwhile, the CFTC adopted regulations similar to Regulation SCI for swap execution facilities (SEFs), designated contract markets (DCMs), swap data repositories (SDRs), and derivatives clearing organizations (DCOs). The bulk of the agency's system safeguards rules are housed in multiple regulations:

- SEFs—CFTC Regulation 37.1401.
- DCMs—CFTC Regulation 38.1051.
- SDRs—CFTC Regulation 49.24.
- DCOs—CFTC Regulations 39.18 and 39.34.

Entities regulated by the CFTC must address the following categories of risk analysis and oversight: (i) enterprise risk management and

Regulation SCI—Basic Requirements	
Who must comply (Rule 1000).	"SCI Entities" including: (i) SCI self-regulatory organization; (ii) SCI alternative trading system; (iii) Plan processor; and (iv) Exempt clearing agency subject to ARP.
"SCI systems" (Rule 1000).	Broadly defined, but potentially modified by "critical SCI systems" (6 categories and a catch-all for functionalities with few alternatives) and by "indirect SCI systems" (reasonably likely to pose a security threat to SCI systems, if breached).
"SCI events" (Rule 1000).	An event at an SCI entity that constitutes a system: (i) disruption; (ii) compliance issue; or (iii) intrusion.
Operational capability/ maintenance of fair and orderly markets (Rule 1001(a)).	Maintain written policies and procedures reasonably designed to ensure SCI systems and indirect SCI systems (regarding security standards) have the needed capacity, integrity, resiliency, availability, and security.
Systems compliance (Rule 1001(b)).	Maintain written policies and procedures reasonably designed to ensure SCI systems comply with the Exchange Act, applicable securities regulations, and the entity's rules and governing documents.
SCI personnel (Rule 1001(c)).	Maintain written policies and procedures for identifying, designating, and documenting responsible SCI personnel.
SCI review (Rule 1003(b)(1)).	Review SCI entity's compliance with Regulation SCI once each calendar year.
Penetration testing (Rule 1003(b)(1)(i)).	Do penetration test review at least once every three years.
SCI systems assessment (Rule 1003(b)(1)(ii)).	Assess SCI systems that directly support market regulation or market surveillance at a frequency determined by a risk assessment, but at least once every three years.
BC-DR testing (Rule 1004).	Designate SCI entity's members/participants to participate in testing of BC-DR plans at least once every 12 months. Coordinate testing of BC-DR plans on industry- or sector-wide basis with other SCI entities.
Corrective action (Rule 1002(a)).	An SCI entity, once its responsible SCI personnel have a reasonable basis to conclude an SCI event has occurred, must take corrective action that, at a minimum, mitigates potential harm to investors and market integrity while seeking to remedy the SCI event as soon as reasonably practicable.

governance; (ii) information security; (iii) business continuity and disaster recovery (BC-DR) planning and resources; (iv) capacity and performance planning; (v) systems operations; (vi) systems development and quality assurance; and (vii) physical security and environmental controls. The evaluation of these topics must adhere to generally accepted standards and best practices.

SEFs, DCMs, SDRs, and DCOs must respond to CFTC requests to produce records regarding system safeguards activities. These entities also must comply with the internal review and reporting provisions, including senior managements' and the board of directors' receipt and review of the required assessments, and documentation of any vulnerabilities and deficiencies with an eye to either remediating them in a timely manner given the nature and magnitude of the risk, or accepting the associated risk.

Some entities within the CFTC's regulations must meet heightened standards. For example, a SEF or DCM that is a critical financial market must also satisfy the requirements contained in CFTC Regulation 40.9 (currently reserved). A systemically important DCO or Subpart C DCO must be capable of much faster recovery times (two hours) than other DCOs (next business day), in-

Regulation SCI—Notice, Reports, and Other Requirements		
Initial Notification of SCI event (Rule 1002(b)(1)).	Immediately	Form SCI not required (Exhibit 6 can include optional attachments)
Notification of SCI event (Rule 1002(b)(2)).	Within 24 hours	Form SCI (Exhibit 1)
Update of SCI event (Rule 1002(b)(3)).	Regular basis or upon reasonable Commission request	Form SCI not required (Exhibit 6 can include optional attachments)
Interim SCI event report (Rule 1002(b)(4)).	Within 30 days of occurrence	Form SCI (Exhibit 2)
Final SCI event report (Rule 1002(b)(4)).	5 business days after resolution and investigation by SCI entity closed if within 30 days of occurrence	Form SCI (Exhibit 2)
Quarterly report of no or de minimis impact SCI events (Rule 1002(b)(5)(ii)).	30 days after calendar quarter end	Form SCI (Exhibit 3)
Quarterly report of material system changes (Rule 1003(a)(1)).	30 days after calendar quarter end	Form SCI (Exhibit 4)
Supplemental report of material system changes (Rule 1003(a)(2)) (Report not required if information in Rule 1002(b) notification).	Promptly	
Report of SCI review with senior managers' response (Rule 1003(b)(3)). Review must be submitted to both the Commission and the SCI entity's board of directors.	60 days after submitted to SCI Entity's senior managers	Form SCI (Exhibit 5)
Dissemination of information about SCI event (Rule 1002(c)). An exception exists if dissemination would compromise security or an investigation. Special requirements apply to major SCI events.	Promptly	

Regulation SCI—Key Implementation Dates	
Effective Date	February 3, 2015
General compliance date	November 3, 2015
Compliance date for ATSs newly meeting SCI ATS volume threshold	6 months after ATS meets Regulation SCI volume threshold for the first time
Compliance date for industry- and sector-wide SCI entity coordinated testing of BC-DR plans	November 3, 2016

CFTC System Safeguards—Basic Testing Requirements

Required Testing	Minimum Frequency	Who May Conduct Testing
Controls Testing	Based on appropriate risk analysis (can be on rolling basis). Covered DCM/SDR/DCO key controls: At least every three years.	Covered DCM/SDR/DCO must use independent contractors for key controls. SEF/DCM can use independent contractors or employees who are not responsible for development/operation of tested systems or capabilities (Covered DCMs, SDRs, and DCOs can use employees for other testing).
ETRA	Based on appropriate risk analysis. Covered DCM/SDR/DCO: Based on appropriate risk analysis, but at least annually.	Entities can use independent contractors or employees who are not responsible for development/operation of tested systems or capabilities.
External Penetration Testing	Based on appropriate risk analysis. Covered DCM/SDR/DCO: Based on appropriate risk analysis, but at least annually.	Covered DCM/SDR/DCO must use independent contractors, but may do other testing with employees who are not responsible for development/operation of tested systems or capabilities.
Internal Penetration Testing	Based on appropriate risk analysis. Covered DCM/SDR/DCO: Based on appropriate risk analysis, but at least annually.	Entities can use independent contractors or employees who are not responsible for development/operation of tested systems or capabilities.
SIRP Testing	Based on appropriate risk analysis. Covered DCM/SDR/DCO: Based on appropriate risk analysis, but at least annually.	Entities can use independent contractors or employees.
Vulnerability Testing	Based on appropriate risk analysis. Covered DCM/SDR/DCO: Based on appropriate risk analysis, but at least quarterly.	Entities can use independent contractors or employees who are not responsible for development/operation of tested systems or capabilities.

cluding from wide-scale disruptions, under CFTC Regulation 39.34.

Moreover, covered DCMs, as defined in the applicable regulation, and SDRs, may have additional duties regarding some system safeguards requirements. A covered DCM is a DCM whose annual total trading volume in 2015 or a later calendar year is at least 5 percent of the combined annual total trading volume of all CFTC-regulated DCMs for the particular year. The data used in making this determination is a production requirement for DCMs under the system safeguards regulation.

The various forms of testing required by Regulation System Safeguards must be "broad enough" to encompass the testing that an entity's risk analysis and oversight program and its current cybersecurity threat analysis indicate is needed to identify risks, such as an intruder's ability to interfere with operations, to impair or degrade automated systems, to compromise data integrity, or to take unauthorized actions. Testing divides into six areas: (i) controls testing; (ii) enterprise technology risk assessment (ETRA); (iii) external penetration testing; (iv) internal penetration testing; (v) security incident response plan (SIRP) testing; and (vi) vulnerability testing.

SEC disclosure issues—The SEC issued CF Disclosure Guidance: Topic No. 2 in 2011 to address the emerging disclosure issues surrounding cybersecurity. The guidance, which has not been updated since, acknowledges the fine line

CFTC System Safeguards—Key Implementation Dates		
Effective Date	SEFs/DCMs/SDRs/DCOs	September 19, 2016
Books & Records	SEFs/DCMs/SDRs	September 19, 2016
All Other Provisions (Clearing Final Rules)	DCOs	September 19, 2016
Production of Annual Total Trading Volume	DCMs	October 19, 2016
Vulnerability Testing	SEFs/DCMs/SDRs/DCOs	March 20, 2017
SIRP Testing	SEFs/DCMs/SDRs/DCOs	March 20, 2017
Penetration Testing (Internal and External)	SEFs/DCMs/SDRs/DCOs	September 19, 2017
Controls Testing	SEFs/DCMs/DCOs (Key controls testing by covered DCMs and SDRs)	September 19, 2017 (September 19, 2019)
ETRA Requirements	SEFs/DCMs/SDRs/DCOs	September 19, 2017
Updated BC-DR Plans	SEFs/DCMs/SDRs	September 19, 2017
All Other Provisions (Exchange Final Rules)	SEFs/DCMs/SDRs	September 19, 2017

between revealing company vulnerabilities and keeping investors informed of company developments. As a result, a company must disclose enough information to meet SEC requirements and investors' needs, but does not have to give would-be hackers a roadmap to the company's technological weak spots.

As a result, companies may need to consider various aspects of their periodic and annual reports or other SEC filings with respect to cybersecurity. For example, a company may wish to update its risk factors section to include cybersecurity risks, although under Item 503(c) of Regulation S-K, this section must be specific to the company and should not include general risks applicable to any issuer or offering. A company also may need to decide whether to disclose material pending legal proceedings related to data breaches, such as direct or derivative law suits; Item 103 of Regulation S-K suggests some parameters for making litigation-related disclosures.

Moreover, Congress has thus far not enacted cybersecurity laws that would directly impact public company disclosures. But in the 114th Congress, former Rep. Jim McDermott (D-Wash) introduced the Cybersecurity Systems and Risks Reporting Act (H.R. 5069), which would have invoked the Sarbanes-Oxley Act's executive certification and internal controls provisions. Senators Jack Reed (D-RI) and Susan Collins (R-Maine) also introduced the Cybersecurity Disclosure Act of 2015 (S. 2410), which would have required companies to disclose if their boards have cybersecurity expertise.

SEC enforcement—The SEC's Office of Compliance Inspections and Examinations continued its recent trend of listing the examination of SCI entities and cybersecurity among its market-wide examination priorities. OCIE also has flexibility overall to determine its examination needs based on its assessment of risks in the marketplace and at entities. OCIE previously conducted a cyber sweep of broker-dealers and investment advisers and published the results in a series of Risk Alerts (September 2015; February 2015; April 2014).

Resulting SEC enforcement matters are few in number, but two of them point out a common cybersecurity issue. In one settled administrative proceeding, the SEC alleged that registered

investment adviser R.T. Jones Capital Equities Management, Inc. willfully violated the safeguards requirement of Rule 30(a) of Regulation S-P by failing to adopt written policies and procedures to deal with personally identifiable information of clients and others stored on an unencrypted third-party-hosted webserver. An unknown intruder gained access and copy rights to the data, but later investigations by multiple cyber consultants were unable to determine if the data was in fact accessed or compromised. R.T. Jones was censured and agreed to pay a $75,000 civil money penalty after the Commission considered the firm's remedial steps and cooperation in the matter.

In another settled administrative proceeding, the SEC penalized Morgan Stanley Smith Barney LLC (MSSB), a registered broker-dealer and investment adviser, for similar violations of Regulation S-P regarding an employee who downloaded data on 730,000 customer accounts to a personal server that cyber forensics indicated was "likely hacked" by a third party. The employee obtained the data by leveraging a defect in MSSB's customer data analysis portal security that allowed him to generate reports on a wider set of customers. Some of the misappropriated data turned up for sale on multiple Internet sites. MSSB was censured and fined $1 million, but the Commission considered MSSB's cooperation and remedial efforts. The Commission likewise penalized the employee by imposing associational and penny stock bars; the employee also pleaded guilty to a federal criminal charge and was ordered to pay $600,000 in restitution and sentenced to three years' probation.

Company boards, M&A, liability—Derivative suits against company boards over data breaches have struggled to take hold, but public company directors must remain focused on cyber-related disclosures, cyber insurance policies, and liability. One example is the dismissal with prejudice of a shareholder suit against Target Corporation after the company's special litigation committee issued its report on a data breach.

Some entities within the CFTC's regulations must meet heightened standards.

In an even more recent example, the U.S. District Court for the Northern District of Georgia dismissed a shareholder derivative suit against Home Depot, Inc. over a data breach accomplished by hackers using "BlackPOS" malware (the Target breach employed related malware) to gain access to point of sale payment card data systems. The Home Depot decision has been appealed to the Eleventh Circuit with briefing set to begin in April.

Cyber insurance and related commercial general liability and errors and omissions policies also raise many questions for company boards. In the Target example, the SEC staff had separately queried the company about its insurance coverage via the agency's filing review process.

But mergers and acquisitions may become a new area of concern for boards. For example, Verizon Communications Inc. recently announced that it will pay $350 million less to acquire Yahoo! Inc.'s operating business, a deal now valued at $4.48 billion, after disclosures about prior data breaches at Yahoo! The amended merger agreement assigns Yahoo! much of the potential liability for the breaches and provides that the breaches will not be a factor in determining if a "Business Material Adverse Effect" has occurred. The Yahoo! breach also is now the subject of a federal prosecution (additional DOJ statement) of a group of alleged perpetrators that includes two officers in the Russian Federal Security Service. ■