FEBRUARY 2016

COMMENTARY

Commodity Futures Trading Commission Proposes Cybersecurity Best Practices

On December 16, 2015, the Commodity Futures Trading Commission ("CFTC") approved two proposed rules which would require regulated entities to conduct specific tests of their cybersecurity capabilities, remediate vulnerabilities, and institute board-level review of the testing results.[1] The CFTC safeguard proposals, which are substantively similar but focus on different regulated entities, would amend existing rules for derivative clearing organizations, designated contract markets, swap execution facilities, and swap data repositories ("regulated entities") and require these entities to implement certain cybersecurity best practices.[2] Though this is not the CFTC's first foray into cybersecurity,[3] these proposals come at a time of increased regulatory and public focus on cyber threats and require the attention of regulated entities.

Cyber Threat Environment

In issuing these safeguard proposals, the CFTC recognized the "consistent, growing cybersecurity threat to the financial sector" by state-sponsored and non-state adversaries with increasing technical sophistication and capability.[4] As noted by the CFTC, half the exchanges worldwide were attacked between July 2012 and July 2013 and, as the director for the Center for Cyber and Homeland Security testified recently, one U.S. bank disclosed that it faced 30,000 cyber attacks in one week alone.[5] Further, the CFTC safeguard proposals demonstrate that the CFTC understands that cyber attacks are expanding beyond traditional theft or fraud for monetary gain into more destabilizing threats to companies and markets, such as disruption of operations, data and intellectual property theft and espionage, extortion, destruction of data, and degradation of the capabilities of automated systems.[6] In some cases, a successful attack may go undetected for weeks or years, while an adversary has access to critical internal systems.[7] With the proliferation of potential entry points for hackers, including mobile devices and cloud-based data, as well as third-party service providers with access to corporate systems, the challenge in protecting against attacks is only growing.[8] In short, the threat motivating the CFTC is serious, diverse, and complex.

Current Proposals

The CFTC's safeguard proposals emphasize testing, remediation, and appropriate cybersecurity governance.

At the heart of the proposed amendments are five essential types of testing, which reflect industry best practices expressed in guidance from governmental and private experts. While the specific scope of testing is not mandated, to account for the circumstances of particular organizations, testing must be broad enough to cover all systems and controls necessary to identify vulnerabilities that could allow an attacker (either internal or external) to:

> (i) Interfere with the [firm's] operations or with fulfillment of its statutory and regulatory responsibilities; (ii) Impair or degrade the reliability, security, or adequate scalable capacity of the [firm's] automated systems; (iii) Add to, delete, modify, exfiltrate, or compromise the integrity of any data related to the [firm's] regulated activities; or (iv) Undertake any other unauthorized action affecting the [firm's] regulated activities or the hardware or software used in connection with those activities.[9]

Vulnerability Testing. Under the proposed rules, regulated entities would be required to regularly test their automated systems to determine what vulnerabilities exist on the systems and what information an attacker could discover through a "reconnaissance analysis," a review of public information that may identify system vulnerabilities.[10] As explained by the CFTC, this type of testing is a key component of assessing system risk, and analyzing the results can help identify and prioritize issues for remediation.[11]

The proposed rule also sets out a frequency expectation for this testing.[12] As with the other testing requirements, the proposal is explicit that a regulated entity's determination of the appropriate frequency for testing must be based on a regulated entity's particular risk assessment. However, at a minimum, the proposed rule calls for quarterly testing.[13]

The final element of the vulnerability testing rule relates to the independence of the testing professionals. The proposed rules require the use of outside independent contractors to conduct at least two of the quarterly tests, permitting the other tests to be conducted by independent employee testers (i.e., employees not involved in the development or operation of the systems being tested).[14]

Penetration Testing. The second type of testing proposed by the CFTC is "penetration testing." Distinct from vulnerability testing, which identifies potential weaknesses, penetration testing identifies ways those weaknesses could be exploited in the real-world from two distinct angles. "External" penetration testing attempts to "penetrate…automated systems from outside the systems' boundaries," while "internal" penetration testing refers to attempts to penetrate the systems from "inside the systems' boundaries."[15] Put another way, external testing simulates an outside hacker trying to gain access to an organization's system, while internal testing simulates an employee (or a hacker who has gained access to the system) using his or her access for improper purposes. This type of testing allows a firm to identify the amount of damage an attacker could do before the firm is able to detect and respond to the attack, and how effective the firm's responses are.[16]

Though testing frequency must be determined by a regulated entity's risk analysis, as with each of the proposed tests, the minimum frequency for penetration testing under the proposed rules would be annually for both external and internal testing.[17] The CFTC is further proposing that independent contractors be used for the external tests, though employees with sufficient independence may conduct the internal testing.[18]

Control Testing. The CFTC next proposes control testing. "Controls" refer to the steps and systems an organization puts in place to protect automated systems and the organization's data and information. Certain controls, designated as "key controls," are of particular importance, since they are either critically important for effective system protection or they are "intended to address risks that evolve or change more frequently."[19] The goal of this testing is to ensure that an organization's system-safeguard controls are implemented and operating correctly and are effective in accomplishing their safeguarding roles.[20]

Under the proposed rules, control testing would be done no less frequently than every two years, and independent contractors would be required to test at least those controls identified as "key controls."[21]

Security Incident Response Plan Testing. The CFTC also proposes that firms test their security incident response plans, written plans that document how an organization goes about "identifying, responding to, mitigating, and recovering from" a cybersecurity incident.[22] According to the proposed rules, an appropriate plan involves the organization's internal classification system for security incidents, its communication protocols after an incident has been identified, and aspects of the response process.[23] Under the proposed rules, regulated entities would be required to test these plans to ensure that they are effective, identify weaknesses in the plan, enable updating and improvement, and "maintain organizational preparedness and resiliency."[24] The rules are flexible on the precise method for testing these plans, with options ranging from checklists to comprehensive exercises.[25]

The proposed rules allow either outside contractors or employees (presuming they have sufficient independence) to conduct these tests, but they would be conducted no less than annually.[26]

Enterprise Technology Risk Assessment. The final type of testing required under the proposals is an Enterprise Technology Risk Assessment ("ETRA"). In contrast to the other testing, which is more tactical, the ETRA is an analysis designed to give organizational leaders a strategic view of the threats and vulnerabilities the organization faces in the context of the controls it has in place to combat those risks.[27] The ETRA should help an organization understand cyber risks, including risks to others (such as other market participants), the probability and impact associated with those risks, and their relative priority.[28] When done well, this assessment can inform the ongoing testing process and allow for better risk management, including identifying areas where new controls, training, or other processes are needed.[29]

The proposed rules would require that the assessment be done at least annually, either by outside contractors or independent employees.[30] The CFTC is clear that the safeguard proposals are not a substitute for any other obligation to continually monitor and assess risk. Rather, the proposals would ensure that a formal, documented process is completed at least once a year.[31]

Of course, testing alone is not sufficient to create a robust cybersecurity program. Along with testing, the proposed rules require that regulated entities review the results of those tests, and once a covered firm has identified vulnerabilities and deficiencies, the firm is expected to resolve them consistent with the underlying security expectations set out by law, and to do so in a timely fashion based on the firm's risk analysis.[32]

In addition, the proposed rules set out additional governance expectations. Under current rules for derivative clearing organizations, it is explicit that any testing done must be reviewed by senior managers.[33] The proposed rules clarify that senior management review is required for designated contract markets, swap execution facilities, and swap data repositories as well, and further make it plain that board of director review of testing reports is required for all these regulated entities.[34] Cybersecurity is not merely an information technology issue. Rather it is an "enterprise-wide risk management issue" and the CFTC believes that board-level attention is essential to effectively combat threats.[35]

Commentary

The proposed amendments to existing rules, standing alone, are hardly surprising or revolutionary. As noted by the CFTC, the sources of these proposals are well-known best practices that many firms already follow.[36] Indeed, the CFTC believes that at least the major components of these proposals are already implicitly required under existing law and that the proposed rules are much more about clarity and aligning expectations than they are about a radical change to how covered firms do (or should do) business.[37]

With the issuance of these proposed rules, the CFTC is signaling that cybersecurity is a top priority going forward. Issued only a few years after the original system safeguard rules,[38] the CFTC is joining other financial regulators (like the Federal Financial Institutions Examination Council and the New York Department of Financial Services)[39] in recognizing cybersecurity as one of the key challenges, if not the most significant challenge, for regulated entities in the near term. As the CFTC has recognized, in our interconnected financial markets, cyber attacks are not just a threat to a particular

firm, nor is the concern only about information theft. Attacks that undermine a firm's ability to perform its market function, such as those that implicate data integrity or operating ability, could ripple out to the broader system, victimizing even those entities that themselves have put in place strong security protocols and ultimately disrupting important financial markets.[40] By creating a standard set of procedures, the CFTC is aiming to create more certainty and confidence among market participants as well as to ward off threats to the financial stability of our markets and the broader economy.

For regulated entities, these proposals (which, as noted, the CFTC largely sees as simply clarifying existing law and promoting accepted best practices) should be recognized as a warning from the CFTC that it is serious about cybersecurity and that it will not tolerate excuses for failing to implement a robust cybersecurity program. Regulated entities can expect to see this emphasis reflected in examinations and enforcement actions,[41] and they would do well to conduct effective and appropriate ongoing risk assessments to help ensure compliance with evolving cybersecurity rules and best practices.

Further, putting aside regulatory concerns, firms that have yet to engage in a serious cybersecurity effort should take the CFTC's proposals and concerns as a wakeup call. The threat is real and growing and the impact of a cyberattack on a firm's operations, finances, and reputation could be devastating. Moreover, in the near term, firms without a thoughtful cybersecurity program will simply not be able to compete, as market participants, recognizing and reflecting the CFTC's concerns, will demand certain protections as a condition of doing business. The time for building and enhancing cybersecurity programs is now, and in proposing these amendments, the CFTC has provided firms with a good starting point.

Lawyer Contacts

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com/contactus/.

Lisa M. Ledbetter
Washington
+1.202.879.3933
lledbetter@jonesday.com

Mauricio F. Paez
New York
+1.212.326.7889
mfpaez@jonesday.com

Stephen J. Obie
New York
+1.212.326.3773
sobie@jonesday.com

Ethan Levisohn, an associate in the Washington office, assisted in the preparation of this Commentary.

Endnotes

1 System Safeguards Testing Requirements for Derivatives Clearing Organizations, 80 Fed. Reg. 80113 (proposed December 23, 2015) (to be codified at 17 C.F.R. pt 39); System Safeguards Testing Requirements, 80 Fed. Reg. 80139 (proposed December 23, 2015) (to be codified at 17 C.F.R. pts. 37, 38, 49). Please note that many of the CFTC's statements, conclusions, and proposals discussed here are referred to in both proposed rules. Except where noted, where the proposals are substantively similar, for ease of reference, this commentary cites only to the derivative clearing organizations proposal.

2 This commentary focuses on the key aspects of the common proposals in the Notices of Proposed Rulemaking (NPRMs) that update existing safeguard rules by requiring certain practical cybersecurity protocols. The proposed rules for designated contract markets,swap execution facilities, and swap data respositories also contain related amendments that clarify certain aspects of required risk analysis and oversight programs (such as explicitly adding enterprise risk management and governance as a category of risk analysis and oversight for these entities) and make aspects of those programs mandatory, in line with existing rules for derivative clearing organizations. The CFTC anticipates future rulemakings related to these entities to bring further clarity.

3 *See, e.g., CFTC and SEC Announce Focus on Cybersecurity*, Jones Day Commentary (April 2014).

4 System Safeguards Testing Requirements for Derivatives Clearing Organizations, 80 Fed. Reg. at 80114-80115.

5 *Id.* at 80114; System Safeguards Testing Requirements for Derivatives Clearing Organizations (Statement of Commissioner Sharon Y. Bowen), 80 Fed. Reg. at 80113, 80137.

6 *Id.* at 80115.

7 *Id*.

8 *Id*.

9 *Id*. at 80131.

10 *Id*. at 80117, 80134-80135.

11 *Id*. at 80117.

12 The rules do not propose to apply the minimum frequency and outside contractor requirements for any of the five tests to swap execution facilities or smaller designated contract markets at this time.

13 *Id*. at 80118, 80135. The proposed rules also note that the testing must include automated vulnerability scanning and, where called for by the risk analysis, that the testing should be done on an authenticated basis, using usernames and passwords to more fully simulate user activity. *Id*. at 80117-80118, 80135.

14 *Id*. at 80118, 80135.

15 *Id*. at 80119, 80133.

16 *Id*. at 80119.

17 *Id*. at 80119, 80135.

18 *Id*. at 80119-80120, 80135.

19 *Id*. at 80120, 80134.

20 *Id*. at 80120.

21 *Id*. at 80120, 80135.

22 *Id*. at 80121. Though the proposed rules do not specifically require that an organization implement a security incident response plan, they do define what the plan should contain and the testing requirement presumes that such a plan is required, though it may be a part of a broader business continuity plan. *Id*. at 80121, 80136.

23 *Id*. at 80121, 80135-80136.

24 *Id*. at 80121, 80134.

25 *Id*.

26 *Id*. at 80121-80122, 80135-80136.

27 *Id*. at 80122, 80133.

28 *Id*. at 80122.

29 System Safeguards Testing Requirements, 80 Fed. Reg. at 80158.

30 Safeguards Testing Requirements for Derivatives Clearing Organizations, 80 Fed. Reg. at 80122, 80136.

31 *Id*. at 80122.

32 *Id*. at 80122-80123, 80136.

33 17 C.F.R. § 39.18(j)(3).

34 System Safeguards Testing Requirements, 80 Fed. Reg. at 80183, 80186, 80189.

35 System Safeguards Testing Requirements for Derivatives Clearing Organizations, 80 Fed. Reg. at 80122-80123, 80136.

36 *See, e.g.,* System Safeguards Testing Requirements for Derivatives Clearing Organizations, 80 Fed. Reg. at 80126-80131.

37 *See, e.g., id*. at 80117, 80126-80131.

38 17 C.F.R. §§ 37.1400 *et seq*., 38.1050 *et seq*., 39.18, 49.24.

39 *See* FFIEC Cybersecurity Assessment Tool; Letter from Anthony J. Albanese, Acting Superintendent of Financial Services, to Financial and Banking Information Infrastructure Committee (FBIIC Members (Nov. 9, 2015) (discussing potential cybersecurity regulatory requirements).

40 *See, e.g.,* System Safeguards Testing Requirements for Derivatives Clearing Organizations (Statement of Chairman Timothy G. Massad), 80 Fed. Reg. at 80113, 80137; System Safeguards Testing Requirements for Derivatives Clearing Organizations (Statement of Commissioner Sharon Y. Bowen), 80 Fed. Reg. at 80137

41 Indeed, the CFTC already examines entities for compliance with system safeguard rules and, as noted, believes that many of these proposals are already covered by those rules. System Safeguards Testing Requirements for Derivatives Clearing Organizations (Statement of Chairman Timothy G. Massad), 80 Fed. Reg. at 80137 ("The proposal also complements what we as a Commission already do. We focus on these issues in our examinations to determine whether an institution is following good practices and paying adequate attention to these risks at the board level and on down.").