THE REVIEW OF
SECURITIES & COMMODITIES REGULATION
AN ANALYSIS OF CURRENT LAWS AND REGULATIONS AFFECTING THE SECURITIES AND FUTURES INDUSTRIES

Vol. 51 No. 12 June 20, 2018

# THE FUTURES INDUSTRY AND CYBERSECURITY

*The regulatory framework for cybersecurity in the derivatives markets is evolving to meet the growing threat of cyberattacks. The authors describe these regulatory initiatives, focusing on the SEC's recent cybersecurity examinations and the CFTC's first cybersecurity enforcement action. They conclude with key cybersecurity takeaways for derivatives industry organizations.*

By William Ridgway, Jonathan Marcus, and Alexander Kasparie *

Cyberattacks on financial institutions and infrastructures have grown more frequent, complex, and sophisticated. And the motivation behind such attacks is shifting from financial gain to disruption, such as through nation-state attacks, which threaten to undermine confidence in the financial system. Recognizing the gravity of these risks, financial regulators have made cybersecurity a priority. Indeed, the CFTC recently joined the growing list of regulators that police this area in bringing its first enforcement action relating to cybersecurity.[1] That action underscores the need for robust oversight of cybersecurity and the ease with which a regulated entity can find itself in the crosshairs of an enforcement action. Given the increasing regulatory scrutiny and sophistication of the threats, futures industry market participants would do well to take a fresh and comprehensive look at their cybersecurity preparedness, governance, internal controls, and defenses.

## THE REGULATORY FRAMEWORK

Regulations and interpretive notices from the CFTC, the SEC, and the National Futures Association ("NFA"), the self-regulatory organization for the U.S. derivatives industry, set forth the evolving regulatory framework for cybersecurity in the derivatives markets. Although these regulations focus on different areas, they collectively embody a set of requirements and best practices for market participants to follow.

As a starting point, futures commission merchants and introducing brokers are required to "adopt policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information" under CFTC Regulation 160.30. The NFA's interpretive guidance similarly

[1] CFTC No. 7693-18, 2018 WL 816833 (Feb. 12, 2018).

* *WILLIAM RIDGWAY is a partner, JONATHAN MARCUS is of counsel, and ALEXANDER KASPARIE is an associate at Skadden, Arps, Slate, Meager & Flom, LLP. Their e-mail addresses are william.ridgway@skadden.com, jonathan.marcus@skadden.com,* and *alexander.kasparie@skadden.com*. The views expressed herein are those of the authors and are not necessarily the views of Skadden Arps or its clients.

***RSCR Publications LLC*** Published 22 times a year by RSCR Publications LLC. Executive and Editorial Offices, 2628 Broadway, Suite 29A, New York, NY 10025-5055. Subscription rates: $1,197 per year in U.S., Canada, and Mexico; $1,262 elsewhere (air mail delivered). A 15% discount is available for qualified academic libraries and full-time teachers. For subscription information and customer service call (937) 387-0473 or visit our website at www.rscrpubs.com. General Editor: Michael O. Finkelstein; tel. 212-876-1715; e-mail mofinkelstein@gmail.com. Associate Editor: Sarah Strauss Himmelfarb; tel. 301-294-6233; e-mail sarah.s.himmelfarb@gmail.com. To submit a manuscript for publication contact Ms. Himmelfarb.  ISSN: 0884-2426. 

requires members[2] to "adopt and enforce a written [information systems security program] reasonably designed to provide safeguards appropriate to the member's size, complexity of operations, type of customers and counterparties, the sensitivities of the data accessible within its systems, and its electronic interconnectivity with other entities."[3] Finally the SEC's Regulation S-P requires registered broker-dealers and investment advisers to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information."

Financial regulators have raised the bar in more recent guidance, demanding heightened accountability, senior leadership engagement, and more prescriptive cybersecurity requirements. For example, in April 2015, the SEC's Division of Investment Management issued a guidance update identifying the cybersecurity of registered investment companies and registered investment advisers as a critical issue and detailing possible measures to address cybersecurity risks.[4] The guidance focused on previously identified ways of addressing cybersecurity risk, namely: risk assessment, effective governance, incident response planning, participation in cyber threat information-sharing bodies, assessing the risk posed by third-party vendors, and considering cyber insurance. The guidance formed part of the SEC's ongoing Cybersecurity Initiative and drew from (1) conversations with fund boards and senior management at investment advisers, (2) the Office of Compliance Inspections and Examinations' ("OCIE") review of investment adviser cybersecurity practices,[5] and (3) the SEC's March 2014 Cybersecurity Roundtable. Subsequently, on September 15, 2015, OCIE announced the areas of focus for its second round of cybersecurity examinations: governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response.[6]

In August 2017, OCIE released a summary of its observations from cybersecurity examinations that it conducted pursuant to its Cybersecurity Examination Initiative, which focused on written policies and procedures regarding cybersecurity, with an increased emphasis on testing and validating that such policies and procedures were implemented and followed.[7] Overall, OCIE observed improvements in cybersecurity preparedness since its 2014 initiative, but also noted areas for improvement and concern, including:

- **Policies and procedures that were insufficiently detailed**. Some policies and procedures were not reasonably tailored because they provided employees with only general guidance, identified limited examples of safeguards for employees to consider, were very narrowly scoped, or omitted specific procedures for implementing policies.

[2] All registered Futures Commission Merchants, Retail Foreign Exchange Dealers, Introducing Brokers, Swap Dealers, Major Swap Participants, Commodity Pool Operators, and those registered Commodity Trading Advisors who direct client accounts or provide tailored investment advice must be NFA Members. CFTC-registered Associated Persons of NFA Members must be NFA Associate Members. NFA, Membership and Directories, https://www.nfa.futures.org/registration-membership/membership-and-directories.html (last visited May 7, 2018).

[3] NFA, NFA Rule Book, Interpretive Notices-9070 – NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs (Aug. 20, 2015), *available at* https://www.nfa.futures.org/rulebook/rulesPDF.aspx?Section=9&RuleID=9070.

[4] SEC IM, *Cybersecurity Guidance* (Apr. 2015), https://www.sec.gov/investment/im-guidance-2015-02.pdf.

[5] SEC OCIE, OCIE Cybersecurity Initiative (April 15, 2014), http://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf; SEC OCIE, Cybersecurity Examination Sweep Summary (Feb. 3, 2015), https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf (summarizing the results of its examinations).

[6] SEC OCIE, OCIE's 2015 Cybersecurity Examination Initiative (Sept. 15, 2015), https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.

[7] SEC OCIE, Observations From Cybersecurity Examinations (Aug. 7, 2017), https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf.

- **Inconsistent enforcement of policies**. A number of firms did not enforce their own policies and procedures or, in some cases, the written policies and procedures did not reflect the firms' actual practices.

- **Inadequate system maintenance leading to violations of Regulation S-P**. The SEC's Regulation S-P requires investment advisers to adopt policies and procedures that address technical and physical safeguards to protect customer records and information. But OCIE staff found Regulation S-P violations among firms that did not adequately conduct system maintenance, such as installing software patches to address security vulnerabilities or implementing additional operational safeguards.[8]

The CFTC has also issued further guidance on cybersecurity. In September 2016, the agency released rules for all derivatives clearing organizations, designated contract markets, swap execution facilities, and swap data repositories, intending to supplement the agency's previous requirement that futures market participants conduct testing according to "generally accepted standards and industry best practices."[9] The rules require these entities to conduct five kinds of cybersecurity testing: (1) vulnerability testing, (2) penetration testing, (3) controls testing, (4) security incident response plan testing, and (5) enterprise technology risk assessments. The rules specify the frequency of those tests, whether independent contractors must perform those tests, and the tests' scope.[10] The rules also require the registrant's senior management and board of directors to review these reports and remediate any issues identified through testing.

### *The CFTC's First Cybersecurity Enforcement Action*

The CFTC reinforced its emphasis on cybersecurity with its first enforcement action earlier this year. In that case, the CFTC settled charges against a registered futures broker for allegedly failing to diligently supervise its information systems security program in the wake of the alleged exposure of customer data for nearly ten months.

The broker had in place an information systems security program under Commission Regulation 160.30, but, as with many brokers and other financial institutions, it had delegated certain aspects of its information security program to an outside IT provider, including the performance of risk assessments of network access routes, the evaluation of vulnerabilities, the maintenance of firewall rules to allow network access only from known IP addresses, and the detection of unauthorized network activity. After installing a network attached device to store backup data, however, the IT provider left an Internet access port in the device open by default, "allowing permission-less access to the [device's] contents[.]"[11]

The IT provider failed to identify or perform a risk assessment of the access port in compliance with the information systems security program; provided network risk assessments that incorrectly informed the broker's officers that there were no security abnormalities or concerns based on the provider's testing; and continued to overlook network security concerns even after the third party that accessed the files made a series of Internet posts — some of which were reported in the media and on cybersecurity websites — describing its ability to access sensitive information at other entities via the same type of access port.[12]

Although the IT provider committed the security errors, the CFTC concluded that the broker violated the diligent supervision rule, observing that while it was permitted to delegate the performance of its information systems security program, it "cannot abdicate its responsibilities" to "diligently supervise the IT provider's handling of all activities relating to the FCM's business as a Commission registrant." The CFTC pointed to "the fact that for nearly 10 months, a significant amount of [the broker's] customers' records and information were unprotected and vulnerable to cyber-exploitation" and that it only learned of the problem when notified by the third party that identified the exposed information.[13]

---

[8] The SEC has already brought several enforcement actions against registered firms for cybersecurity failings, including fining a bank $1 million in June 2016 for failing to secure its internal client information systems and prevent a breach. Rel. 34-78021 (2016).

[9] System Safeguards Testing Requirements, 81 Fed. Reg. 64,272; 64,319 (Sept. 19, 2016) (codified at 17 C.F.R. pts. 37, 38, and 49); System Safeguards Requirements for Derivatives Clear Organizations, 81 Fed. Reg. 64,321, 64,340 (Sept. 8, 2016) (codified at 17 C.F.R. pt. 39).

[10] *Id.*

[11] CFTC No. 7693-18, 2018 WL 816833 (Feb. 12, 2018).

[12] *Id.*

[13] *Id.*

Although the CFTC faulted the broker for its oversight, it credited the broker's response to the breach, an instructive lesson for other firms. The CFTC cited the fact that the broker initiated a comprehensive review of its network security; improved its encryption of customers' records and information; and hired a cybersecurity firm to perform a penetration test of its network to further ensure its security.[14] The CFTC also noted that the penalty — a $100,000 civil fine and a requirement to provide follow-up reports on its network security — reflected the broker's substantial cooperation, which included providing information that assisted the Commission in investigating the matter efficiently.

Notably, the CFTC's order relied not on Commission Regulation 160.30 — which governs requirements for information security policies and procedures — but on Commission Regulation 166.3, which broadly imposes supervisory obligations on market participants, signaling a more expansive enforcement reach for cybersecurity matters.[15]

## KEY TAKEAWAYS

The various regulations, interpretive notices, and enforcement actions from the NFA, CFTC, and SEC highlight the need for derivatives industry organizations to adopt measures to protect their businesses and mitigate potential legal exposure, including the following:

***Tailoring the Cybersecurity Plan to Emerging Threats –*** An organization's cybersecurity strategy must be tailored to its threat environment, and cyberattacks against the financial industry have taken a more destructive turn. The industry is now coping with denial-of-service attacks of unprecedented strength, powered by the exploitation of internet-connected devices (i.e., the internet of things), such as cameras, webcams, and digital video recorders. Organizations must think carefully about their internet-exposed infrastructure and that of their vendors — everything from an online portal to their building's heating, ventilation, and air-conditioning system — and brace for heightened levels of disruption to operations if attacked.

A similar trend is taking shape with regard to ransomware, the malware that holds its victims' data hostage through encryption until a ransom is paid.[16] Ransomware became a dominant threat in 2017, causing over $5 billion in damages.[17] These attacks will not subside anytime soon, but many hackers have transitioned to cyber extortions targeting the financial sector, armed with more sophisticated malware and demanding steeper payments. Some criminals have taken to stealing sensitive files and threatening their release rather than locking them down with encryption; others have been looking to hold hostage a business' internet-connected technologies and infrastructure.

The emergence of more destructive attack patterns requires market participants to evaluate cyber-risk differently. Compared to more run-of-the-mill breach of customer data or theft of intellectual property (which can still be harmful), destructive attacks call for unique defensive strategies and must be met with an effective business continuity plan to minimize operational downtime. Indeed, some destructive attacks may even imperil the safety of employees or customers, a risk factor that has not traditionally been part of the cybersecurity calculus.[18]

---

[14] *Id.*

[15] *See, e.g.*, Paul J. Pantano, Jr., Neal E. Kumar and Stephanie L. Klock, *The Duty of Diligent Supervision: To Whom and What Does It Apply and What Does It Require?*, 37 Futures & Derivatives L. Rep., no. 11, Dec. 2017, 2 (explaining recent settlements indicate the CFTC's new administration has made "diligent supervision by Commission registrants a high priority").

[16] Cybercriminals often demand these ransoms be paid in bitcoin, another area under close scrutiny by regulators. *See, e.g.*, SEC Rel. No. 2018-53 (announcing charges against two co-founders of a purported financial services start-up for allegedly orchestrating a fraudulent initial coin offering); CFTC No. 7678-18 (Jan. 24, 2018) (announcing charges and a restraining order against two individuals and a corporation alleging commodity fraud and misappropriation related to the ongoing solicitation of customers for a virtual currency).

[17] Steve Morgan, *Global Ransomware Damage Costs Predicted to Exceed $5 Billion in 2017*, Cybersecurity Ventures (May 18, 2017), https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/.

[18] *See, e.g.*, Kim Zetter, *A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever*, Wired (Jan. 8, 2015), https://www.wired.com/2015/01/german-steel-mill-hack-destruction/ (describing the "massive damage" to a German steel mill's system caused by a hack); David Kravets, *Feds: Hacker Disabled Offshore Oil Platforms' Leak-Detection System*, Wired (Mar. 18, 2009), https://www.wired.com/2009/03/feds-hacker-dis/ (noting the federal indictment of a disgruntled former employee for disabling a key monitoring system); Chuck Squatrigilia, *Polish Teen Hacks His City's Trams, Chaos Insures*, Wired (Jan. 11, 2008),

Almost all companies in the financial sector have business continuity plans on the books, but many have not stress-tested their plans against these evolving threats. One method for doing so is to enlist employees or a cybersecurity firm to attempt to execute attacks through so-called "red teaming," which should help companies identify any shortcomings before a real attack is executed. At a minimum, stress testing will demonstrate that senior leadership is paying attention to these risks.

The financial sector must also determine whether the company's insurance covers these new risks. Cyber insurance has traditionally focused on privacy breaches, but businesses now increasingly seek policies that provide business interruption coverage, including for systems failure, cyber extortion, and digital asset restoration, as well as for business interruption caused by a third party, such as a cloud provider. In light of these new threats, companies should consider expanding their insurance coverage accordingly.

***Monitoring Vendors*** – For many organizations in the financial sector, the most daunting cybersecurity problems arise from third-party vendors that access their networks. Hackers understand this and routinely exploit third-party vulnerabilities to break into otherwise well-protected networks. Indeed, a September 2017 survey conducted by the Ponemon Institute found that 56% of respondents had experienced a data breach caused by a vendor, an increase of 7% over the last year.[19] At the same time, as the financial sector grows more interconnected, organizations have little choice but to rely on third parties, despite their potential vulnerabilities. Given these trends, the financial sector must place special emphasis on reviewing and improving cybersecurity oversight of third-party vendors.

The CFTC's recent enforcement action reinforces that message. The order demonstrates that the CFTC takes the diligent supervision rule seriously and aims to hold registrants accountable for the cybersecurity failures of their vendors. Regulated entities should therefore consider whether and how they may retain additional in-house or other external IT personnel in order to provide further layers of oversight. For smaller entities, one potential solution is to retain a "virtual Chief Information Security Officer," a non-employee who may serve as a high-level consultant to advise internal security officers and senior executives, and possibly help coordinate incident response.[20] Especially in light of the CFTC's and SEC's requirements that boards and senior executives adequately supervise the cybersecurity preparedness of their company, companies must ensure the board and senior management receive adequate guidance on these issues.[21]

***Training Employees*** – The NFA requires member firms to educate and train their employees on cybersecurity matters.[22] Given the NFA's guidance, and the CFTC's emphasis on holding organizations accountable for their failure to properly oversee those entrusted with cybersecurity, companies must ensure they have adequate training procedures.[23] The National Institute of Standards and Technology offers one model for designing such a program,[24] but regardless of the model, implementing a strong training program is critical to address the heightened regulatory scrutiny of cybersecurity preparedness.

***Using Table-Top Exercises*** – In October 2017, the Futures Industry Association's Market Technology Division hosted a cybersecurity simulation in which a

*footnote continued from previous page…*

https://www.wired.com/2008/01/polish-teen-hac/ (discussing the damage and injuries caused by a hack of public trams).

[19] *See* Data Risk in the Third-Party Ecosystem: 2nd Annual Study by Ponemon Institute (Sep. 2017).

[20] John Falck & Michael Philips, *Information and Cyber Security for the Futures Industry: A Perspective by VSEC, LLC* (Oct. 12, 2017), *available at* http://www.johnlothiannews.com/wp-content/uploads/2017/10/Information-and-Cyber-Security-for-the-Futures-Industry-1.pdf.

[21] *See, e.g.,* Brian V. Breheny, et al., *SEC Issues Interpretive Guidance on Cybersecurity Disclosures*, Skadden, Arps, Slate, Meagher & Flom LLP (Feb. 23, 2018), https://www.skadden.com/insights/publications/2018/02/sec-issues-interpretive-guidance.

[22] NFA, *Interpretive Notice 9070 – NFA Compliance Rules 2-9, 2-2-36 and 2-49: Information Security Systems Programs* (Aug. 20, 2015), https://www.nfa.futures.org/rulebook /rules.aspx?RuleID=9070&Section=9.

[23] According to a March 2017 study by IBM Security, in 2016 more than half of the cyberattacks against the financial services and healthcare industries were carried out by employees who maliciously stole or unwittingly distributed sensitive data. *IBM Security, IBM X-FORCE Threat Intelligence Index 2017: The Year of the Mega Breach 19* (Mar. 2017).

[24] Patricia Toth & Penny Klein, National Institute of Standards and Technology, U.S. Department of Commerce, *A Role Based Model for Federal Information Technology/Cybersecurity Training* (2014), *available at* https://csrc.nist.gov/CSRC/ media/Publications/sp/800-16/rev-1/draft/documents/sp800_ 16_rev1_3rd-draft.pdf.

fictitious derivatives clearing house and an exchange suffered a massive cyberattack.[25] The exercise produced a 15-page report with a number of recommendations to ensure the continuity and security of the futures market in the event a major market participant fell prey to an attack.[26] Scenario-driven exercises such as these are a powerful tool to help an organization perform better during real-world cyberattacks. Table-top exercises have long been employed to test emergency response and business continuity plans in government and the private sector, and are becoming commonplace in the cybersecurity toolkit. As the National Institute of Standards and Technology observes, these exercises are necessary to "validate" an incident response plan and minimize the duration, impact, and cost of a breach to an organization.[27]

## CONCLUSION

The financial services industry and the critical infrastructure it supports are attractive targets for hackers, cyber-criminals, and hostile nation states. That risk is heightened by the industry's interconnectedness. Those linkages magnify the damage an attack can cause, as a problem at one firm or exchange can easily cascade throughout the entire system. In tackling these threats, firms face increasing scrutiny from their regulators. Given the operational, financial, and reputational costs at stake, derivatives market organizations must continually evaluate their security posture and vulnerabilities to protect their businesses and ensure compliance with new rules and guidance from their regulators. ■

[25] Futures Industry Association, 2017 Cybersecurity Scenario Workshop, "Operation Blow Torch," Summary Report (Nov. 7, 2017), *available at* https://fia.org/sites/default/files/FIA%20Cybersecurity%20Scenario%20Workshop%202017%20-%20Summary%20Report%20-%20Final.pdf.

[26] *Id.*

[27] Tim Grance et al, U.S. Department of Commerce, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities* 4-1 et seq. (2006), *available at* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf.