CYBER SECURITY: WHAT NFA GUIDANCE MEANS FOR CCOs

BY LINDA LERNER, HARVEY RISHIKOF AND JENNY CIEPLAK OF CROWELL & MORING LLP

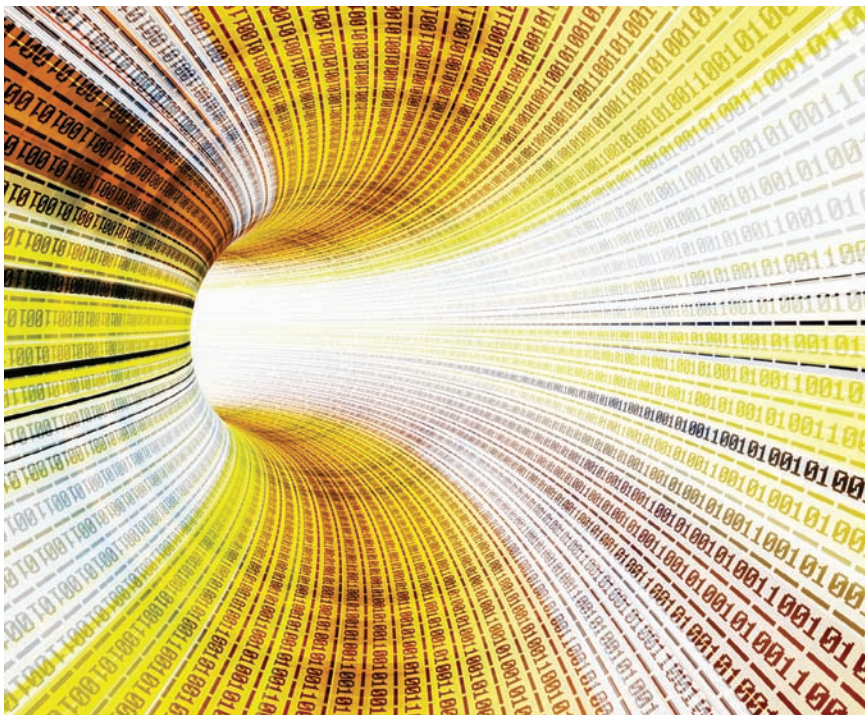
The **National Futures Association** recently adopted new cyber security guidance containing the self-regulatory organization's standards for Information Systems Security Programs (ISSPs). Cyber security has become a priority for both compliance teams and regulators, with the **Securities and Exchange Commission**, **Commodity Futures Trading Commission** and **Financial Industry Regulatory Authority** having previously issued their own guidance on the issue.

While the requirement to have an ISSP is not new, the NFA cyber security guidance puts another tool in the SRO's examination toolbox, allowing it to assess penalties for failing to have a conforming ISSP. The guidance applies to all futures commission merchants, retail foreign exchange dealers, commodity trading advisers, commodity pool operators, introducing brokers, swap dealers and major swap participants—referred to collectively as "regulated entities—that are NFA registrants. But all regulated entities, even those that are not NFA registrants, are required by CFTC Regulation 160.30 to adopt "policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information."

While the CFTC regulation is far less detailed than the NFA cyber security guidance, the CFTC will likely impose more detailed requirements soon. Thus, even unregistered firms should find the guidance instructive, as assistance with existing compliance requirements and as an indication of what the CFTC's new regulations will look like.

In many cases, regulated entities are also subject to the SEC's rules, and in practice one ISSP should be able to satisfy the requirements of the CFTC and NFA as well as the SEC. But firms should confirm that both their futures and swaps business and their securities business comply with the policy's terms. Regulated entities that are part of an affiliated group can use a parent entity's ISSP, but should be aware that NFA will review the parent's ISSP against the standards set out in its cyber security guidance subject to the type, size and complexity of the group's operations.

While a strong ISSP cannot prevent all security breaches, a robust set of policies and procedures that are carefully followed will likely be a factor considered by regulators in assessing penalties both in the event of a breach and in regular exams.



WHAT SHOULD REGULATED ENTITIES DO NEXT?

Develop an ISSP, or check that existing ISSPs conform to generally accepted standards

NFA suggested a number of third-party resources that are useful in developing cyber security policies. For example, the **National Institute for Standards and Technology** has released a detailed framework that refers organizations to what NIST considers the best of the industry-created provisions for each facet of an ISSP. The cyber security guidance also referenced for review standards promulgated by the **SANS Institute**, the Open Web Application Security Project and the Control Objectives for Information and Related Technology.

Regulated entities have an obligation to conduct a security and risk analysis, deploy protective measures against identified threats and vulnerabilities and develop an incident response and recovery plan. A vulnerability analysis should:

- Take into account the types of sensitive information stored by the regulated entity and to which it has access;
- Identify the personnel and vendors who have access to sensitive information (and whether any changes should be made in access levels);
- Examine security breaches at other industry participants;
- Review the security measures the regulated entity has in place, and consider ways to improve those measures; and
- Involve consulting business units and information technology, back-office, risk management and internal audit personnel.

One relatively new trend among the procedures NFA recommended is the use of application whitelists, which prevent any unauthorized software from operating on a computer system. Other recommendations included physical and electronic access controls; using supported and updated software; regularly backing up systems, which should also be addressed in a firm's disaster recovery plan; and using web filtering technology to block access to potentially malicious websites.

Continued on page 15

(CONTINUED FROM PAGE 11)

CYBER SECURITY: WHAT NFA GUIDANCE MEANS FOR CCOs

An ISSP should identify who is responsible for compliance with various aspects of the policy—for example, who is responsible for initiating and conducting periodic reviews; who must be contacted to conduct diligence on a vendor before that vendor is onboarded; and who will serve on an emergency team to respond rapidly to security incidents.

No ISSP is complete without an incident response plan. Among other things, such a plan should include emergency contact information for the emergency response team (which should be communicated to all employees and vendors) and internal escalation procedures. Regulated entities that are part of affiliated groups or have multiple business lines should be sure these escalation procedures include coordination among other affiliates or business lines that may have been affected by a security breach.

As part of creating an incident response plan, regulated entities should identify parties that must be notified of any security breach. These parties include regulatory authorities and law enforcement, SROs, designated contract markets, derivatives clearing organizations, swap execution facilities, data repositories and other market participants with which the regulated entity's systems are interconnected, as well as customers and employees. The incident response plan should include a description of the relevant information to be delivered to each such party, and procedures for investigation of breaches, including the use of an outside vendor to investigate, if desired.

Ensure management review and approval in writing

The cyber security guidance requires that an NFA registrant's ISSP be approved in writing by the registrant's CEO, chief technology officer or another executive-level officer, and stated that management should provide information about the ISSP to the board of directors.

Discussions about the ISSP at the board level should be documented in minutes, which should be available for review by NFA officials in exams. Even for non-registrants, involving management and directors in information security fosters a culture of compliance and can help demonstrate that information security is understood to be part of the board's duty of care.

Conduct periodic review of the ISSP

NFA recommended that ISSPs be reviewed every 12 months. This review should include vulnerability assessments, consideration of product developments in the world of cyber security, and a tabletop or dry run exercise to test the effectiveness of the incident response plan using hypothetical scenarios. Upon the conclusion of a review, the CEO, CTO or another executive-level officer should reapprove the policy—even if it has not changed—and the board should receive an update documented in board minutes.

Ensure security of information held by third-party service providers

If a vendor will have access to protected information, its contract should include provisions requiring the vendor to ensure the security of that information. In addition, regulated entities should conduct due diligence of vendors that have access to protected information, including reviewing vendors' security policies and infrastructure. This due diligence should be updated annually, and records should be kept of the results.

REGULATORS WILL EXPECT MUNICIPAL ADVISORS TO IMPLEMENT SUPERVISORY POLICIES AND PROCEDURES THAT ARE REASONABLY DESIGNED TO DETECT VIOLATIONS OF RULE G-20 WITHIN THEIR ORGANIZATION

Ensure the security of mobile devices

If mobile devices such as laptops, thumb drives and phones can be connected to a regulated entity's network, or if personnel otherwise have the ability to store or access sensitive information on mobile devices, use appropriate technology such as encryption and wiping software to ensure the security of that information upon a theft or loss of the mobile device.

Ensure that personnel are required to turn in company-provided mobile devices upon termination, or, if able to access sensitive information through their personal devices, that such access is terminated.

Encrypt data at all times

NFA recommended encrypting sensitive data when in transmission and when stored on mobile devices. However, firms should consider encrypting extremely sensitive data even when stored on a firm's computers and servers, as recommended by FINRA, to protect data in case of an intrusion.

Conduct periodic employee training

NFA recommended that employees be trained at the time they are hired, and receive annual refresher training.

Conduct independent testing of security systems

The CFTC has recommended that independent testing be conducted every two years. Regulated entities should maintain documentation of the results of such testing, and should also document how the results were used in the review and update of the entity's ISSP.

Consider cyber insurance

While the NFA cyber security guidance does not mention cyber insurance, FINRA's recent report on cyber security mentioned it as another proactive measure firms can take. Although regulators will not view cyber insurance as a substitute for a robust ISSP, it is generally helpful in demonstrating a commitment to security. Additionally, cyber insurance may be an effective tool for an organization to help it protect its assets.

Join an information-sharing organization

Groups such as the **Information Sharing and Analysis Organizations** and **Information Sharing and Analysis Centers** provide up-to-date information about cyber threats, which can be used to inform a firm's ISSP.

Maintain records

NFA registrants must retain records relating to their ISSPs pursuant to NFA Rule 2-10. It is a sound policy for all regulated entities to maintain ISSP-related records to show a history of compliance in the event that an audit or a security breach occurs. Records should be kept of all activities regarding the ISSP, including management and board review and approval, periodic reviews and updates, vendor due diligence, employee training and independent testing.

The cyber security guidance acknowledged that many smaller NFA registrants may not have ISSPs in place that conform to its requirements, and that NFA plans to develop an "incremental, risk-based examination approach" for smaller introducing brokers, CPOs and CTAs. NFA also suggested that it may provide additional, more detailed guidance in the future—registrants should continue to monitor NFA communications for additional information.

***Linda Lerner** is a partner in the New York office of **Crowell & Moring. Harvey Rishikof** is senior counsel and **Jenny Cieplak** is counsel in the firm's Washington, D.C. office.*