Cyber Security: What's worse, the threat or cure?

BY MARC NAGEL

It seems that every day there is a report of a security breach at some company or another. Credit card numbers were stolen from Target and Neiman's. Social security numbers and personal information were stolen from Advocate Health Care. And now the discovery of the "Heartbleed" bug, that may represent a serious vulnerability to countless web sites.

The Commodity Futures Trading Commission (CFTC) has considered cyber security and on Feb. 26, 2014, issued an advisory (CFTC Staff Advisory No. 14-21), outlining best practices for meeting the cyber security responsibilities of CFTC registrants. These cyber security responsibilities arise from the Gramm-Leach-Bliley Act of 1999 that was intended to insure that financial institutions respect the privacy of their customers and protect the security and confidentiality of their customer's nonpublic personal information.

Under CFTC Regulations (17 CFR Part 160), the privacy rules apply to futures commission merchants (FCMs), introducing brokers (IBs), commodity trading advisors (CTAs) and commodity pool operators (CPOs). The privacy notices that are sent to you annually are required by Part 160.

The CFTC has now taken those privacy rules a step further by outlining best practices to be followed for the protection of customer nonpublic information. The CFTC's budget request for 2015, includes the following: "The Commission's examination expertise will need to be expanded to examine registrant's compliance with emerging risks in information security, especially in the area of cyber-security as required by the Financial Stability Oversight Counsel (FSOC)."

We can expect that the CFTC and self-regulatory organizations will focus some of their attention in this area. Specifically, the recommended "best practices" includes:

1. Designation of a specific employee to take responsibility for planning and management of the required controls.
2. Identification, in writing, of all reasonably foreseeable internal and external security risks.
3. Designing of safeguards to control the identified risks.
4. Training of staff to implement the program.
5. Regular testing to monitor the safeguards' controls, systems, policies and procedures.
6. Arranging for an independent party to test the safeguards' controls, systems, policies and procedures, at least every two years.
7. To the extent that the firm's third party service providers (independent software vendors, auditors, back office bookkeepers, etc) have access to customer records, selecting only service providers capable of maintaining appropriate safeguards and binding them contractually to implement and maintain those safeguards.

8. Regularly evaluating and adjusting the program.
9. Designing and implementing policies and procedures to be followed in the event that there is a breach or unauthorized disclosure.
10. Providing the Board of Directors with an annual assessment of the effectiveness of the program.

Since the enactment of Dodd Frank, the futures industry has been inundated with new and complex rules and regulations. This has put a tremendous strain on the futures industry, both in manpower and expense. While these new rules were well intentioned, very few will actually serve to protect customers from a repeat of the financial meltdown that prompted Dodd Frank in the first place.

The Gramm-Leach privacy laws have been with us for 15 years and cyber security has now become a critical issue. All of us are vulnerable to cyber thieves and their ability to exploit a breach in cyber security. Protecting the public in this area is both well intentioned and necessary. The recommendation of these best practices is a good first step but the more difficult part will be the implementation by futures firms. These rules cut across multiple departments, including, operations, IT, web development, risk, compliance and legal. It will be a significant challenge for a firm to get all these different competencies to work together to develop a comprehensive security plan. Today these are only recommendations; undoubtedly they will soon become mandates.

Marc Nagel is a compliance consultant with 35 years experience in the Futures industry. Most recently Marc served as COO and chief compliance officer for Dorman Trading. Marc is a licensed attorney and CPA and serves on the FCM Advisory Committee of the NFA. He can be reached at mn@marcnagel.com or at www.marcnagel.com.