CalSurance®

Risk Reduction & Loss Prevention

August 2014

REGULATORS' INCREASED FOCUS ON CYBER SECURITY

By Chad Weaver and Megan Hayati

It is no secret that corporate cyber security, or the protection of electronically stored private data, is increasingly becoming a topic of attention. Stories of multimillion dollar cyber security breaches such as the recent breaches at Target and eBay are becoming commonplace. However, cyber security is not only an issue for large international retailers. The financial industry's approach to cyber security is increasingly under scrutiny from the Financial Industry Regulatory Authority (FINRA) and the U.S. Securities and Exchange Commission (SEC). In fact, the SEC and FINRA have declared that cyber security is a priority for 2014. Specifically, the regulators are focusing on cyber security in two ways: 1) Regulation and 2) Enforcement Actions.

SEC Regulation

In April of this year, the SEC's Office of Compliance Inspections and Examinations issued a Risk Alert stating that it will be examining more than 50 registered broker-dealers and investment advisers to help the SEC determine what additional steps it should take to address cybersecurity threats, and to identify areas where the SEC and the industry can collaborate to protect investors and markets from cyber threats. The SEC examination sweeps will specifically focus on the following:

- Identification of risks/cybersecurity governance;
- Protection of firm networks and information;
- Risks associated with remote customer access and funds transfer requests;
- Risks associated with vendors and other third parties; and
- Detection of unauthorized activity.

FINRA Regulation

In January of 2014, FINRA announced that it would begin conducting an assessment of firms' approaches to managing cyber security threats. In doing so, FINRA will, among other things, evaluate and assess a firm's cyber-attack plans, reporting lines in the event of a cyber-breach, and a firm's contractual arrangements with third party service providers such as technology vendors or a breach coach.

FINRA's focus on regulation of broker-dealer cyber security issues centers around two SEC Regulations, SEC Regulation S-P, Rule 30 and SEC Regulation S-ID. Regulation S-P requires registered broker-dealers, investment advisers and investment companies to establish written policies and procedures reasonably designed to secure the confidentiality of customer records and information. SEC Regulation S-ID was created to prevent identity theft and requires, among other things, that financial institutions have reasonable policies and procedures for (a) "identify[ing] relevant red flags"; (b) detecting those red flags; (c) responding appropriately to red flags once detected; and (d) updating the identity theft program.

FINRA Rules 3010 and 3012 require member firms to establish, maintain and enforce a supervisory system and written procedures

reasonably designed to ensure compliance with applicable securities laws and rules, including Regulation S-P and S-ID. Therefore, pursuant to FINRA Rules 3010 and 3012, each member firm must establish, maintain and enforce a supervisory control system to test and verify that its supervisory procedures are reasonably designed to achieve compliance with applicable securities laws and rules, including Regulation S-P and S-ID.

FINRA Enforcement Actions

When a breach does occur, FINRA has taken formal disciplinary action against firms, imposing severe penalties and fines. On average, these fines amounted to around $200,000 when FINRA found that the firm's policies or procedures were not enough to protect sensitive private customer data.

For example in 2011, FINRA found that a brokerage firm had violated Regulation S-P, FINRA Rules 2110 and 3010, and FINRA Rule 2010 by failing to adequately protect customer records in the firm's electronic portfolio management system. Specifically, the firm allowed employees to share computer sign on credentials and did not place controls or procedures on the use or dissemination of username and passwords which allowed access to customer information. FINRA found that the firm failed to adequately supervise its representatives in the field by failing to establish procedures mandating the installation of security software or applications on representative-owned computers that were used away from home office. The representatives used these computers while in the field or at home to access the firm's portfolio management system online. FINRA found that the firm did not have a system to regularly inspect these registered representative-owned personal computers. After the firm was notified by FINRA that its customer's information and records were vulnerable to security breaches, the firm immediately disabled access to portfolio management system and retained an outside consultant who found no evidence of a breach. Nevertheless, FINRA found that the nonpublic personal information of the firm's customers was not properly safeguarded and fined the firm $450,000.

The Importance of Cyber Insurance

In addition to the implementation of elaborate prevention systems, financial institutions and broker dealers are increasing exploring cyber insurance. Recognizing that most traditional insurance policies do not cover all cyber breach incidents, many firms are evaluating the benefits of maintaining an additional policy for cyber liability. In doing so, the firms are recognizing that insurance carriers can be helpful with assembling a team of qualified professionals and experts in the event of a cyber breach. Further, during its sweep inquiries to numerous broker dealers, FINRA specifically inquired of the firms as to whether they maintain cyber insurance. Indeed, the maintenance of cyber insurance may soon be considered a best practice by the Regulators.

About the Authors: Chad Weaver is a partner of Edgerton & Weaver, LLP, a complex litigation firm in California that specializes in defending professional liability claims, particularly claims relating to financial institutions and their agents. Megan Hayati is an associate of the firm.

For inquiries about cyber insurance, or to receive a free, no obligation quote, please contact CalSurance Associates at bd@calsurance.com or call (800) 745-7189.