CORE COMPLIANCE & LEGAL SERVICES, INC.

Risk Management Update
December 2015

THE HUMAN ELEMENT OF CYBERSECURITY

Regulation of Cybersecurity

Beginning in 2014, both the Securities Exchange Commission ("SEC") and FINRA began to examine the heightened risk financial services firms face regarding unauthorized access to the electronic data that these firms routinely maintain as part of their businesses. As part of this initiative, the SEC and FINRA began evaluating the methods used by broker-dealer and investment advisory firms to protect their electronic data ("Cybersecurity"), and in April 2014 the SEC released the SEC Office of Compliance Inspections and Examinations ("OCIE") Risk Alert titled "OCIE Cybersecurity Initiative". This Risk Alert highlights suggested methods of data protection, as well as providing regulatory caution to firms that are not taking steps to implement robust cybersecurity measures. This enhanced regulatory scrutiny of cybersecurity continues today and remains a hot topic for regulators.

Cybersecurity Enforcement Action

On September 22, 2015, the SEC announced that "a St. Louis-based investment adviser has agreed to settle charges that it failed to establish the required cybersecurity policies and procedures in advance of a breach that compromised the personally identifiable information of approximately 100,000 individuals, including thousands of the firm's clients". The release further stated:

> *"The federal securities laws require registered investment advisers to adopt written policies and procedures reasonably designed to protect customer records and information. An SEC investigation found that R.T. Jones Capital Equities Management violated this "safeguards rule" during a nearly four-year period when it failed to adopt any written policies and procedures to ensure the security and confidentiality of PII and protect it from anticipated threats or unauthorized access."*

The SEC's order found that R.T. Jones Capital Equities Management ("the Firm") violated Rule 30(a) of Regulation S-P under the Securities Act of 1933. Without admitting or denying the findings, the Firm agreed to cease and desist from committing or causing any future violations of Rule 30(a) of Regulation S-P. The Firm also agreed to be censured and pay a $75,000 penalty.[1]

This enforcement action sets a precedent and firms should now consider having specific and robust policies and procedures to address cybersecurity a must.

---

[1] *See* "SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior To Breach," SEC Press Release 2015-202 (September 22, 2015), available at http://www.sec.gov/news/pressrelease/2015-202.html.

The Human Element of Cybersecurity

Understanding that the issue of cybersecurity has greater implications than just regulatory penalty, firms across the industry began developing policies and procedures to address their cybersecurity risks. These policies and procedures have for the most part focused on the technical aspects of cybersecurity such as firewalls, penetration testing, and password protection. One area that has not been uniformly addressed is what we call the "human element" of cybersecurity. This Risk Management Update focuses on user awareness training, which should be included as a core part of a firm's cybersecurity policies and procedures.

According to the 2015 Verizon Data Breach Investigations Report, approximately two-thirds of breaches involved a compromised user. Robust cybersecurity measures are vulnerable to human error, such as clicking on a link in an email and being infected with a computer virus or using public Wi-Fi to check corporate email.

Needs Analysis

Cybersecurity may be foreign to many compliance professionals but training is a well-established compliance regimen. The fundamentals of training are applicable and begin with a needs analysis. Below is a list of common actions that can lead to big problems:

- Passwords written down within reach of the computer
- Sharing passwords
- Papers with sensitive information left on desks
- Use of USB drives that are not encrypted
- Unreported loss of a smartphone
- Unsecure emails with sensitive information
- Confirming wire instructions on the phone without verifying the identity of the client

Some firms have employees that are cyber-savvy, but many do not. The needs analysis will help identify relevant areas for training. Relevance serves two functions: it addresses specific needs and it helps keep employees engaged.

The Training Plan

After performing a needs analysis, the next step should be to develop a written training plan. Training is an ongoing process and not a one-time event. The training plan should take a comprehensive view of the subject matter, training methods and follow up.

The most common training methods are live presentations, webinars and online self-study. Live presentations tend to be the most effective; however, interactive online presentations where employees have an opportunity to ask questions and interact can also be effective. Online self-study is expedient, but in some cases may be less effective since there is no interaction with a trainer.

"Repetition is the mother of all learning." For the training program to be effective there must be follow up to reinforce the training. A good method is to have a pre-planned series of training but also take advantage of contemporaneous training opportunities. For example, if you read about a cyber-attack that involved one of your training topics, this is a great opportunity to discuss the incident and reinforce the training. Also, consider sending periodic emails with information surrounding cybersecurity as this helps keep employees continually informed and cybersecurity at the forefront of their thinking.

Training that "Resonates"

Design the program to effectively communicate not only the nature of cyber-threats and the technical means to stop them, but also the everyday practical and "housekeeping" methods employees can utilize to assist with cybersecurity. Structure the training in a way that is easily understandable and relevant to employees. The use of analogies that correlate to their own lives can be helpful, such as:

- Locking doors and windows (securing entries/exits is akin to making sure all network access points are password protected)
- Using deadbolts and secure locks (multiple locks is analogous to two-factor authentication)
- The use of alarms, lights, security cameras etc. (is analogous to intrusion detection monitoring

Training in the context of home computers and personal devices can also be helpful. Employees are more familiar with their own computers than the IT infrastructure at your firm. Moreover, when they talk about their own sensitive information, the training gets personal and spurs interest. Cybersecurity principles are the same in the workplace and at home so the training is topical. Since many employees occasionally work from home their home computer is a network access point and needs to be protected. Finally, the firm should be concerned about the security of employees and their personal information so helping them will be appreciated.

Selected User Awareness Training Topics

- *Social Engineering:* Explain the various techniques hackers use to gain passwords and network access that do not involve traditional "hacking" activities. For example, calling into a firm pretending to be a client and requesting a password reset.
- *Mobile device security*: Outline effective steps for protecting PDAs and laptops including the use of timed password locks. Mobile devices should also have remote locate and remote wipe capability, when possible.
- *Encryption:* Provide examples of types of data that should be encrypted and how to perform encryption. Often overlooked is encryption of data on removable storage devices (*i.e.,* flash-drives, CDs etc.), laptops, home computers and mobile devices.
- *Email security*: Include instruction on how to recognize nefarious emails that include viruses, "phishing" (the activity of defrauding an online account holder of financial information by posing as a legitimate company), and "spoofing" (the creation of email messages with a forged sender address. It is easy to do because the core protocols do not

have any mechanism for authentication). Training should also reinforce the use of secure email when transmitting sensitive information.

- *Password security:* Discuss the most effective techniques for creating passwords. For example, avoiding the use of passwords that personally reflect the employee such as birthdates and addresses. Using a mixture of letters, numbers, and characters, and creating passwords that are at least 10 characters. Also, prohibit password sharing to the extent possible and keep such in a secure location.

Conclusion

There is a significant human element to cybersecurity which should not be ignored and can easily be addressed through user awareness training. Regulators have just begun their intense focus on Cybersecurity, so as the New Year approaches, firms should consider implementing a training plan that spans 2016 and beyond.

CCLS can help, as we provide both in person and online training. We also offer a six point Cybersecurity program. For more information, please do not hesitate to contact us at info@corecls.com or (619) 278-0020, or visit us as www.corecls.com. Thank you.

Authors: Kurt Nuñez, Compliance Consultant and Craig Watanabe, Sr. Compliance Consultant; Editor: Tina Mitchell, Lead Sr. Compliance Consultant, Core Compliance & Legal Services, Inc. ("CCLS"). CCLS works extensively with investment advisers, broker-dealers, investment companies, hedge funds, private equity firms and banks on regulatory compliance issues.