Financial Advisor Forecast: Stormy With Scattered Data Breaches

By Joel Wertman, Esq. and David Shannon, Esq.

Financial Advisor
June 23, 2014

In the wake of recent major cyber security breaches at retailers and banks, the SEC held a cyber security roundtable meeting in March to discuss the current data breach climate and how financial advisors and firms can protect themselves from cyber attacks. Speakers at the event emphasized that financial institutions of all sizes face daily threats, with top risks identified as operational risks, employee theft, and hackers. Steps for addressing inadequate cyber security and reducing potential vulnerabilities were discussed. The long and short of it? Due to increased cyber risk threats to the financial sector, the SEC is making data security a priority in 2014.

SEC Disclosure Guidance: A History

The SEC initially provided Disclosure Guidance related to cyber security in October 2011. The viewpoint was that federal securities laws, in part, are designed to elicit disclosure of timely, comprehensive, and accurate information about risks and events that a reasonable investor would consider important to an investment decision. It was conceded that no existing disclosure requirement explicitly referred to cyber security risks and cyber incidents, but a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents.

The SEC further recognized that registrants had migrated toward increasing dependence on digital technologies to conduct their operations, which led to more frequent and severe cyber incidents. These incidents open up registrants to a variety of liabilities, including liability for remediation costs resulting from stolen assets or information; repairing system damage; increased cyber security protection costs; lost revenue resulting from unauthorized use of proprietary information or the failure to retain or attract customers following an attack; litigation; and reputational damage adversely affecting customer or investor confidence. The 2011 Disclosure Guidance also provided a framework for how and when how a registrant should disclose the risks of a cyber attack and its consequences.

Fast forward to 2014: current updates from the SEC's Office of Compliance Inspections and Examinations (OCIE) indicate that OCIE is exploring ways to test the preparedness of investment advisers and investment companies related to cyber security issues. In preparation for such tests, financial firms and advisors should consider a number of measures to reduce cyber security risks.

Ways Financial Advisors Can Reduce Cyber Liability

Whether the financial firm is a large business with hundreds of employees or a small investment advisor with less than ten employees, a proper data security plan should be implemented. The entire firm must be committed to the plan and work to initiate and follow through with the data security measures. A proper plan will identify and address the following issues.

(1) Data Risk Assessment: A financial advisor should begin by conducting a thorough risk assessment of its data storage and security system. Surveys and data mapping should be conducted to determine what data is on the firm's computer servers and how the systems are protected. C-Suite executives, IT, Legal and HR must all be part of the assessment to ensure the company understands the full extent of its data use, storage and risk.

(2) Purge Old Data: Financial firms collect a tremendous amount of electronic data – all of which contains Personally Identifiable Information (PII). Firms must implement security protocols to delete, destroy or securely archive old data. A data breach can be a significant issue for a business but when a breach involves decades of old data it can be devastating. A proper plan to purge and delete old data is essential to reducing liabilities.

(3) Encrypt Electronic Data: Computer systems that store clients' PII, including servers, desktop computers and tablets, must be encrypted. While encryption is not a guarantee to prevent a data breach, most states' data breach statutes have safe harbor exemptions that will limit a company's liability if the entity can demonstrate lost or stolen data was encrypted.

(4) Prepare for a Data Breach Response: After a company has conducted a risk assessment and improved its security, a proper response plan should be drafted and practiced. IT staff should conduct regular meetings to ensure data security remains a priority and protocols are being followed. Management should ensure that vendors are complying with the company's data security policies and procedures.

(5) Cyber and Data Breach Insurance Should be Obtained: Even the best plans and procedures cannot prevent all data breaches from occurring. Hackers are constantly probing computer systems to exploit weaknesses. Human error will inevitably lead to missing laptops and malware infiltrating systems. In the event of such likely circumstances, a cyber insurance policy provides a business with protection and coverage for a variety of data breach related events. Cyber insurance can now cover business interruption, cyber ransom and first and third-party liability. Additional benefits include immediate access to experienced forensic and legal professionals to investigate and coordinate an immediate response to a data breach.

Conclusion

The heightened climate conducive to data breaches and the SEC's renewed emphasis on data security are strong reasons for financial advisors and firms to develop programs and policies that minimize the threat and related damages associated with a data breach. By treating data security as the "massive" risk that it is, an investment advisor can reduce exposures to devastating and costly liabilities.

JOEL WERTMAN and DAVID SHANNON *are shareholders in the Philadelphia, PA office of Marshall Dennehey Warner Coleman & Goggin. Joel is a member of the Securities and Investments Professional Liability Practice Group. Dave is co-chair of the Privacy and Data Security Practice Group.*

This article appeared online at *Financial Advisor* magazine (www.fa-mag.com) on June 23, 2014.