Cybersecurity: Identify the Threats, Recognize the Risks, Protect Your Franchise

By Ryan Dargis

Cybersecurity issues are all around and have the full attention of regulators. Asset management firms should have programs in place to identify threats, implement protections and communicate breaches. The SEC has communicated that it will evaluate advisors' programs during examinations. Here are sources of attack and their methods, a framework for safeguards and the mandated responsibilities for boards and management.

There is a constant flow of industry, regulatory and media commentary and discussion around the threats our increasingly technology-dependent way of life pose to individuals, households, firms, and governments. Whether it is how we deposit a personal check, clear a credit card transaction, report investment portfolio performance, or relay diplomatic communication, the explosion in our online-dependent existence has created a corresponding increase in the risks from those who wish to exploit that interconnectedness to our disadvantage. As a result, cybersecurity — the ability to safeguard data and electronic-based methods of conducting business — has become one of the most important and challenging new aspects of risk management. This is particularly true for industries dependent on the incredible opportunities the efficiencies the Internet and technology have created.

The dimensions of cyber-risk are well-known, and growing. Initially, examples of cybercrime were limited to hackers attempting to take advantage of network vulnerabilities to demonstrate their technological acumen. From there, the breadth of cyber-risks has evolved into denial-of-service attacks and poaching client data to more-disturbing activities such as placing malware to disrupt business operations; fraud; syphoning funds; causing public embarrassment; altering foreign policy; and weakening national security.

It's particularly important to note that malicious activity often originates within a firm's four walls. As the breadth of cybercrime has expanded, the challenge to respond has grown as well. Firms intent on meeting the risks must change the way they view cybercrime. It no longer is simply an issue of installing sufficient hard- and software designed to detect and thwart online criminal activity. Firms now need to inculcate cybersecurity into their overall risk oversight and security infrastructure.

Ryan Dargis

Within the financial services sector, asset management firms need to recognize cybersecurity threats, implement protections to mitigate the risks, and communicate breaches to clients and authorities. The media report daily the evidence of the threats posed. The risks are real and now have the full attention of regulators. The impact of ignoring these threats could be enormous to your enterprise.

The Securities and Exchange Commission's (SEC's) recent publication from the Office of Compliance Inspections and Examinations (OCIE) is one important indication that regulators are paying increased attention to the importance of cybersecurity. In its National Exam Program Risk Alert[1], the OCIE published the results of a broad industry survey gauging the recognition and risk-mitigation steps broker-dealers and registered investment advisers (RIAs) are taking about cybersecurity. The survey looked at firms' governance and oversight policies; network protection steps; control of remote access to data and information; and vendor and service provider oversight. The survey results reflect the growing recognition of these risks but also illustrate that there is room for improvement, particularly within the RIA community to accelerate how it is addressing these new risks. Although the survey indicated increasing application of enterprise-wide inventories of technology solutions, in other categories of review, the RIA community is generally lagging behind the broker-dealers in addressing important aspects of cyber-risk identification and oversight. These include areas such as: fraud and malware detection within networks; use of the Financial Services Information Sharing and Analysis Center to share intelligence; vendor cybersecurity analysis; creation of a Chief Information Security Officer and securing additional insurance coverage related to cybersecurity.

What are the practical implications for the RIA community generally and fund boards in particular? One important facet is the reliance on service providers. In addition to outsourcing back-office services to banks, custodians and fund administrators, firms are also increasingly farming out middle-office tasks to service providers in a drive to increase efficiency and manage costs appropriately. Service providers should be expected to address the full spectrum of risk and vulnerabilities and how each is addressed via a multi-layered and redundant web of mitigants. The web should start at the security of data itself, both local and off site, through network security up to web security and user education. All facets should wrap holistically into a comprehensive and demonstrable security policy.

The OCIE's findings should reinforce the importance of this growing risk while also signaling that future regulatory action, whether in the form of exams or rule-making, will include a heightened emphasis on cybersecurity. Firms should be prepared to not only respond to the threat but also address this increased level of scrutiny. The risks of inaction are obvious. Firms should not think solely about physical network damage but also recognize the financial and reputational risks associated with cybercrime. A comprehensive information security program for you and your service providers is one critical way you can limit your overall risk while at the same time protect and even enhance your franchise.

1. OCIE, National Exam Program Risk Alert, Volume IV, Issue 4, February 3, 2015

Ryan Dargis is Senior Vice President, Institutional Product Manager at Northern Trust.