Cybersecurity Breaches at Advisers: More Common Than You Think

By E.J. Yerzak, CISA, CISM, CRISC
Vice President of Technology, Ascendant Compliance Management, Inc.*

Think cybersecurity breaches won't happen to your firm? It may be time to reconsider.

Cybersecurity breaches are becoming much more common at investment advisers than firms may realize. While the industry is certainly buzzing about cybersecurity as the latest hot button regulatory and operational risk, executives may nonetheless perceive their firms to be at low risk for a data breach—erroneously assuming that their firms are either too small to be a target, that their IT departments have the latest technology and won't be hacked, or that their firms are too far removed from maintaining custody of physical funds or securities to have anything of value worth hacking. This false sense of security could prove costly, in terms of both financial costs and reputational harm, as the following actual incidents reveal.

Consider the investment adviser who had been using a data storage vendor for years. As would be expected, the adviser had performed some initial due diligence on the vendor. However, when the adviser called the vendor several years later to request an onsite visit to the vendor, the vendor revealed that it had transferred the adviser's files to a location hundreds of miles away. Not only was the adviser's business continuity plan rendered inaccurate, but the adviser had no idea who had access to the files at the new location, or when the change had taken place.

Or consider the investment adviser who, in response to a client request for his own performance information, proceeded to send the client a file containing information about all of the firm's clients—everything ranging from names to social security numbers, addresses, and AUM. In this case, a data breach incident resulted from an employee inadvertently sending the master file instead of a report generated from the master file containing only that client's information.

In addition to unintentional incidents caused by vendors and employees, there are also significant incidents involving hackers who are actively trying to get into your systems, either directly or indirectly. One adviser suffered an outage of its website when a hacker gained access to its account at a hosting provider. While the website was still accessible to the firm internally, the hacker changed settings so that parties outside the firm's office could not access the website, and the adviser didn't even realize the outage for some time because its own access was not impacted.

Hackers are targeting investment advisers who process wire transfers by going after the firms' clients. Gaining unauthorized access to a client's email account can often unearth a trove of useful information for a hacker – things like the name of the investment adviser with which the client has been communicating, copies of account statements sent to the client, and copies of the client's signature in certain email attachments. These items can then be used by the hacker to initiate a fraudulent wire transfer request to the adviser, purporting to originate from the client.

In addition, hackers have targeted advisers through their clients' email accounts by looking for recently opened accounts. In one instance, a hacker who had gained access to a client's email account managed to ascertain that the client had not yet created a username or password at a custodial website to access the client's statements as instructed by the adviser in an email. Perhaps recognizing an opportunity, the hacker accessed the custodial website and created an account on behalf of the client. (Remember, the hacker already had gained access to the client's email account, which also would have enabled him to reset the client's password anyway.) It wasn't until the hacker attempted to change the address of the client on the custodial website that the activity was flagged.

Finally, and perhaps the most likely of incidents to occur, is the threat of ransomware. Ransomware attacks appear to be on the rise. Several advisers report falling victim to the Cryptolocker virus and similar variants, which work by encrypting an employee's entire hard drive and any connected network shared

Continued on page 16

Continued from page 15

folders and drives to render them unusable by the employee. Typically these attacks are initiated when an employee is tricked into clicking on a malicious link containing the malicious payload. Users generally realize they have received the Cryptolocker virus when a message displays on the screen demanding a ransom, usually in Bitcoin, in exchange for the hacker providing the key to unlock the firm's data. Even when a ransom is paid, there is no guarantee that the files will be decrypted, and the employee's machine should be deemed compromised until a full forensic analysis can confirm that no additional malware or backdoors have been left open by the hacker for future attempts.

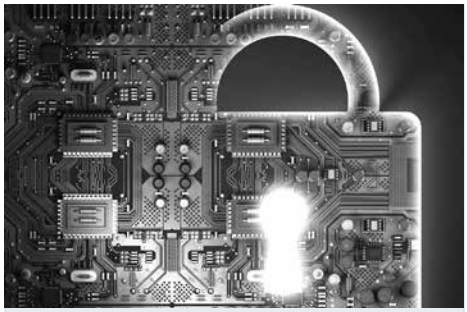
Data breaches are not limited to electronic hacking attempts. Lax physical security controls often play a significant role in data breaches as well, as one firm's social engineering exercise revealed. A student actress hired by the firm was able to completely bypass the firm's electronic controls by bringing in a tray of catered food and asking the receptionist and several employees where the main conference room was located. Not only did several employees fail to question the actress, they held the door for her! The actress was then able to plug in several innocuous thumb drives into various workstations before leaving. Although the particular incident involved a social engineering test of which only the head of the IT department was aware, it highlighted the alarming vulnerabilities in the firm's physical security controls and lack of awareness by firm personnel. On the other hand, the exercise proved to be very valuable and effective cybersecurity training.

Social engineering attacks appear to be on the rise. As investment advisers adopt more robust cybersecurity controls, the hackers have shifted tactics to go after the weakest link at many firms—the people. Using detailed information gleaned from firm organizational charts and personnel biographies posted on firm websites, and information from social media accounts including previous employment, schools, interests, affiliations, connections, posts, and check-ins, cybercriminals can often piece together sufficient information through which they can launch a convincing spear-phishing campaign to induce the recipient to either click on a malicious link purporting to be from a colleague or connection, or to unwittingly divulge confidential information after baiting just enough accurate information to seem legitimate.

In fact, if a hacker is armed only with a firm's email addresses, the hacker can distribute a fictitious email to such employees disguised as a security advisory to install a Windows patch, Adobe patch, or to confirm that a VPN still works. Clicking the link may do nothing at all on your machine, or it may launch malware such as a password-sniffer or ransomware virus.

Cybersecurity threats are not showing any signs of abating, and they are not limited to major retailers. Investment advisers are not immune to cyber threats, and the SEC has stepped up its examination focus in this area as it looks for the next adviser to make an example out of for the rest of the industry. If the latest cybersecurity threats at your peers are not enough to motivate changes in procedures, more cybersecurity enforcement actions may prove to be a very effective deterrent instead. Investment advisers are not alone in struggling to address the mounting cybersecurity risks that appear to be impacting firms of all shapes and sizes.

Cybersecurity breaches are not something that's simply happening to other firms. As the SEC revealed in its February 2015 Examination Sweep Summary, 74% of the examined investment advisers had reported being subject to a cyber-related incident. If 74% of a sample of advisers are reporting such incidents, it is not a stretch to extrapolate that advisers in general are experiencing cybersecurity incidents with sufficient regularity, and these incidents are likely happening to your peers. Only time will tell whether advisers can learn from these cyberattacks and breaches, and whether they can enhance their cybersecurity risk assessment processes to better protect their firms from becoming the next breach headlines.



IAA's Free Cybersecurity Webinar Series

More information is available in a recorded five-part Cybersecurity webinar series—covering issues from the creation and oversight of a cybersecurity program to enforcement, insurance, and public policy considerations—that is available free to IAA members at https://www.investmentadviser.org/eweb/DynamicPage.aspx?webcode=EvInf&Reg_evt_key=55f43630-f506-42c1-8f30-a02f2c577073&Paying=Fees.

The webinar series was co-hosted by the IAA and the law firm of K&L Gates.

**E.J. Yerzak, CISA, CISM, CRISC, is Vice President of Technology and Compliance Services Consultant at Ascendant Compliance Management. He can be reached at eyerzak@ascendant-compliance.com or (860) 596-8118. This article is intended to provide general information.*

E.J. Yerzak, Vice President of Technology and Compliance Services Consultant, Ascendant Compliance Management