How Safe Are Your Clients' Assets?

APRIL 1, 2015 • JEFF SCHLEGEL

There are two categories of people: those who have been hacked and those who are going to be hacked. That's what an FBI official in the agency's cybercrime department told a standing-room-only client event on cybersecurity hosted last year by LJPR LLC, a Troy, Mich.-based registered investment advisor with roughly $700 million in assets under management. The gathering attracted nearly 300 people and also included the managing director for online security at Charles Schwab, LJPR's main custodian.

"Cybersecurity is one of the biggest concerns my clients have," says Leon LaBrecque, a managing partner at LJPR. "They're afraid somebody will steal their identity or their money or get loans in their names. We do tax returns, and we've had a couple of clients who've had their Social Security numbers co-opted and someone filed their tax returns before we did."

Cybercrime is the seedy underbelly of the Internet revolution, if not its Achilles' heel. Distressing news headlines about data breaches have become all too common, from stories of external data theft involving the likes of Target, JP Morgan, Home Depot, Sony and Anthem, to internal incidents such as the Morgan Stanley advisor accused of stealing account data from as many as 350,000 clients (some of that data later appeared for sale online).

According to a February report issued by the U.S. Securities and Exchange Commission, most of the firms examined by the agency said they were the subject of a cyber-related incident — 88% of broker-dealers and 74% of RIAs reported they experienced cyber-attacks directly or through one or more of their vendors. The majority of the cyber-related incidents involved malware and fraudulent e-mails.

In that vein, 54% of broker-dealers and 43% of advisors received fraudulent e-mails seeking to transfer client funds, and 26% of those broker-dealers reported losses related to fraudulent e-mails of more than $5,000. The SEC said no single loss topped $75,000, though one advisor had a loss of more than $75,000 stemming from a bogus e-mail. The client was made whole.

Furthermore, 25% of the broker-dealers that had losses tied to fraudulent e-mails said the incidents resulted from employees not following the firms' identity authentication protocols. And the one advisor that reported an outsized loss said employees didn't follow its identity authentication procedures.

Brian Hamburger, president and CEO at MarketCounsel, an Englewood, N.J.-based business and regulatory compliance consulting firm, says most of the juicy data that hackers want typically resides at broker-dealers and custodians. But smaller, independent advisors with less-robust defenses are also vulnerable.

"For better or worse, technology has a tendency to scale itself," he says. "So while cyber-attacks might be focused now on the large pools of aggregated data, it's easy to surmise that over time hackers will be able to scale their efforts and make it worth their while to go after firms that have less defenses, even if they have less attractive data."

Depending on what you read, it's easy to get spooked about this stuff. A report last year from Privide, a cybersecurity firm in Walnut Creek, Calif., said cyber thieves are increasingly targeting high-net-worth families and their professional advisors, including wealth managers.

Among the factoids in the report, some of which were attributed to other entities: 30 million new types of computer viruses and malware were discovered in 2013; one-third of the world's computers are infected with malware; 740 million personal records were exposed in data breaches in 2013; and nearly $5 billion was stolen from U.S. bank

accounts in 2012 by hackers using malware. In addition, European banks last July reported the discovery of new malware that could bypass the two-factor authentication used to protect customer bank accounts.

Anyway, you get the point we live in a scary world considering that much of our vital personal information in the computer age is potentially exposed to nefarious characters, some of whom would love to drain other people's bank and investment accounts for their own benefit.

So, what is the financial advisory profession doing to protect client assets? And should we be worried, or can we have a degree of confidence that the firms entrusted with our money have what it takes to thwart would-be cyber thieves?

Weakest Link

The good news is that financial services firms, including broker-dealers and custodians who store client assets, are increasingly vigilant about playing defense and keeping up with the latest threats. The not-so-good news is that sneaky minds are always cooking up new threats, and it costs money to combat those crooks.

Last year, the global consulting firm Deloitte issued a cybersecurity report that said financial services firms will need the highest increase in security spending to avert cyber-attacks, and that reaching an ideal state of protection would require a 13-fold rise to $292.4 million per company to fend off 95% of cyber-attacks.

Furthermore, the report found that 44% of global financial services firms said a lack of sufficient funding is the main barrier to implementing an effective IT security program.

Sounds disturbing, if not daunting, but it's not a hopeless situation for U.S. securities firms. "Clearly, it's a high-priority issue, but the broker-dealer community has shown pretty good resilience in dealing with cyber threats," says Daniel Sibears, executive vice president of regulatory operations and shared services at the Financial Industry Regulatory Authority. "They can't prevent all threats—I think everyone would admit that. But they've done a good job understanding what their vulnerabilities are, and they've put in place good incident response plans. And as incidents occur or gaps are identified through practicing incident response plans, improvements occur."

In a report on the cybersecurity practices of broker-dealers issued by Finra in February, the brokerage regulator cited more than a dozen areas where firms can add or make changes to help reduce their exposure to cyber threats. These include data storage at vendors and vendor access control; employee training and employee access control; data encryption; Wi-Fi and handheld device protection; and the filtering of e-mail content.

In short, the best defense is creating established procedures both internally and when dealing with third-party vendors, training employees on those procedures, and then actually following through on them. Or to put it another way, this is as much a people issue as it is a technology issue.

"It's everyone's responsibility at financial services firms to uphold various safeguards because the system is only as strong as the weakest link," Hamburger says. "Any available portal of vulnerability is the portal that potential thieves will pursue."

In its cybersecurity report, Finra cited an unnamed broker-dealer the agency took enforcement action against after hackers launched an SQL (a structured query language) injection attack on its database server to grab the confidential information of more than 200,000 customers. An injection attack is a technique in which an SQL query is used to try and extract information from a database.

At this particular broker-dealer, the stolen data included names, account numbers, Social Security numbers, addresses and dates of birth. Finra says the firm suffered several governance failures by storing unencrypted confidential customer data on a database connected to the Internet without effective password protection, by not performing adequate

testing on its defenses of that information, and by not establishing procedures to review the web server logs that would have revealed the data theft. Finra says the firm only became aware of the breach when hackers attempted to extort money from the firm, even though those breaches had been visible on the firm's web server logs.

According to the SEC, the vast majority of examined broker-dealers and RIAs (93% and 83%, respectively) have put written information security policies in place. Also, 89% of broker-dealers and 57% of advisors do periodic audits to gauge compliance with these policies.

When it comes to dealing with third-party vendors, broker-dealers again appear to be more vigilant on security matters than RIAs. The SEC found that 88% of examined broker-dealers require cybersecurity risk assessments of vendors with access to their firms' networks while only 32% of RIAs do.

Security Partnership

Bolstering security can start with something as basic as educating clients to be more careful with their data. "We remind our clients not to send sensitive information via e-mail, and I'd say 95% of them do a very good job with that," says William Pitney, founder of FocusYou, a financial planning firm in Foster City, Calif. "To protect our clients, we've implemented procedures to confirm and verify distribution requests."

Pitney says his firm always calls an account owner—not the spouse or another person—to verify a customer's transaction request. "Since my support staff has relationships with our clients, they are able to ask some personal questions to confirm their identity," he says.

Gilbert Armour, a financial planner in San Diego with independent broker-dealer SagePoint Financial Inc., says he also confirms all requested transactions by speaking to a real person instead of just acting on e-mail or written requests for redemptions or transfers. He notes his firm has encrypted all of its computers to guard against attacks or risks associated with theft.

Leon LaBrecque, the partner at LJPR, says his firm has had an ongoing dialogue with Schwab about how the custodian is staying on top of cybersecurity. "Look at the news; everything is subject to getting hacked," he says. Schwab, which has roughly $2.5 trillion in AUM, including the assets custodied there by independent RIAs, says it protects client accounts by incorporating numerous tools, operational controls and technologies that work together to protect client accounts and data.

"We continuously monitor our systems, and we work collaboratively with government agencies, law enforcement and other financial services firms to address potential threats," says spokeswoman Sarah Bulgatz. "All of the channels through which clients have access to Schwab are protected."

She adds that Schwab's websites use multilayered protections beyond the log-in name and password before granting access to an account. If the firm suspects unauthorized activity, the user is prompted to answer additional security questions, and failed log-in attempts are limited.

"We use automated alerts and other actions behind the scenes in our authentication and monitoring processes," Bulgatz says. "Pattern analysis and other advanced analytical systems play a role in detecting suspicious activity and deterring unauthorized access. Our fraud teams continuously monitor activity on Schwab.com, looking for suspicious behavior."

And Schwab provides a client with an alert when sensitive transactions occur in a client account—when money is moved in or out, when securities are purchased or sold, or when personal info is changed or updated. "We strongly believe that security is a partnership between us and the independent RIAs who custody their clients' assets with us, and we work hard to educate them about what they should do to keep their systems secure and their clients' personal information safe," Bulgatz says, noting the company's director of online security, Andrew Schofield, travels the country doing

educational workshops and seminars for RIAs.

Intelligence Sharing

One of the key takeaways from Finra's report on broker-dealer cybersecurity practices was the need for companies to participate in centralized information sharing organizations such as the Financial Services Information Sharing and Analysis Center (FS-ISAC) or the United States Computer Emergency Readiness Team (US-CERT).

Finra says some firms are reticent to participate because they fear information sharing might make them subject to regulatory scrutiny. But it notes both the Federal Trade Commission and the Department of Justice have said sharing cyber threat information isn't likely to raise antitrust concerns and can help secure the nation's information network.

FS-ISAC grew out of a presidential directive that required public-private information sharing in the country's critical infrastructure sectors, with each sector creating its own ISAC.

"The financial services is the most mature ISAC; it has more than 7,000 member firms. That's our primary noncommercial threat intelligence-sharing mechanism," says Andy Zolper, chief information technology security officer at Raymond James Financial. "It involves real-time capabilities where we share technical data about potential attacks we're seeing, and we're benefitting from similar information from other firms. The name of the contributing firm is anonymized, but I don't need to know the name of the firm. I just need to know they saw this kind of attack coming from this location exhibiting this type of characteristic, so that I can update my defenses based on that information.

"If you're not involved in FS-ISAC as a broker-dealer, you should do so right away," Zolper adds.

Cyber Insurance

In a worst-case scenario where a client's assets evaporate into the ether, who's responsible for making that client whole? Or, in a more likely situation, if personally identifiable information is stolen during a data breach and clients subsequently see their credit ratings savaged because their information was abused by cyber thieves, who's ultimately at fault?

"From a practical matter, it could be everyone," says Michael Biles, an attorney in the business litigation practice group at King & Spalding in Austin, Texas. "Typically in these situations, plaintiffs go after any deep pocket they can identify and sort it out through the litigation process. Ultimately, I think the entity responsible for maintaining the security of the system would be the most liable."

Biles co-authored a report entitled, "Cybersecurity: The Next Big Wave in Securities Litigation?" He says he hasn't yet seen much cyber-related litigation in the financial advisory space.

"We haven't got much guidance from the courts yet about whether you can convert those incidents into securities law violations," he says. "I'm not aware of any court opinion that sets the parameters for what your disclosure responsibilities are with respect to your computer system and data protection."

Zolper views the threat of cybercrime as a reputational risk for Raymond James Financial. "A legal and regulatory analysis might say an advisor was negligent and didn't exercise the proper standard of care," he explains. "But we operate under the assumption that Raymond James Financial is responsible. If we're holding that client data, then to a regulator that's considered Raymond James data and we're responsible for any breach.

"So when independent advisors buy their own computer equipment, we have a responsibility to ensure that the level of care for that data is met," he continues. "Part of my job is to work with financial advisors to provide education and provide recommended solutions."

Zolper says Raymond James self-insures itself to a certain level before its cyber-specific insurance kicks in, and that policy covers somewhere in the “eight-figure range.”

“Particularly in the broker-dealer space, if there’s a strict loss of funds our fidelity bond covers that regardless of whether it’s from a cyber-attack or fraud or something else,” he says. A fidelity bond is a type of business insurance that protects companies against losses caused by employee theft or other misdeeds. Zolper notes that Raymond James has had only minor non-technology breaches. “We’ve seen much more frequent fraud attempts than anything that would approach a data breach, per se.”

Charles Schwab says the company carries many types of insurance against a variety of risks, depending upon specific facts and circumstances. Among the broker-dealer firms examined by Finra, the regulator says 61% have bought stand-alone cybersecurity insurance, 11% have purchased a cybersecurity rider with their fidelity bond and 28% do not rely on any type of cybersecurity insurance. Large firms have typically bought stand-alone policies, while smaller and midsize firms with limited cybersecurity risk have typically purchased cybersecurity riders in connection with existing fidelity bond policies.

Individual advisor firms increasingly are looking to bolster their cyber coverage either by adding a cyber-rider to their existing errors and omission insurance policy or, and this is more prevalent at larger firms, buying a stand-alone cyber liability policy, says Alex Wayne, executive vice president at Alexander J. Wayne & Associates Inc. in Chicago, a wholesale broker specializing in errors and omissions coverage.

Insurance riders can cover wire transfer fraud, which Wayne says is a big concern for advisors, but not all of them do. Cyber liability policies cover notification and credit monitoring if the advisor has a data breach and clients’ personal identifiable information is compromised. They also cover against lawsuits resulting from a data breach.

The cost of a rider is usually around 10% of the premium for a sub-limit, Wayne says. The cost of an individual policy will vary based on the applicant’s revenue and the limits/retention elected. Premiums start at $1,000 and increase from there based on revenue. Cybercrime is a negative byproduct of the incredible explosion in technology that has brought a lot of positives to financial services. It’s here to stay, and advisors can’t just cross their fingers and hope nothing happens to them.

“The more informed people are about this issue, and not in a way that scares them, but the more aware they become, the better able they are to participate in the solution,” says Brian Hamburger from MarketCounsel.

And whatever that solution might be, it’s not a one-size-fits-all proposition. “Firms engage in different kinds of business and have different kinds of data,” says Daniel Sibears from Finra. “The thing to do is take it in bite-sized chunks, figure out where your vulnerabilities are, understand there are resources available to help build a solid cybersecurity infrastructure to help you be prepared, and have a good incident response plan if an event occurs.”