TD Ameritrade Institutional

ADVISOR SOLUTIONS

VOLUME 9 | Q2 2017 | tdainstitutional.com

PRESIDENTIAL INFLUENCE

Experts weigh in on the economic impact of past presidents

IS YOUR DATA SAFE?

Your clients trust you with their data. Are you doing what you can to protect it?

MISSION STATEMENT

How Compass Ion's mission to help clients lead lives of significance helps support firm growth

Matthew Kane

IS YOUR DATA SAFE?

BY REBECCA McREYNOLDS

Data breaches exposed more than 4 billion personal records worldwide in 2016, according to the latest report from Risk Based Security, a cybersecurity consulting and analytical firm.[1] And those are just the ones we know about. Increasingly, hackers are targeting smaller businesses that don't have the security protocols in place to even know if they've been hacked.

Cybersecurity is a particular concern for registered investment advisors (RIAs). Your clients trust you with their most important personal and financial information, and a data breach could not only cost you that trust, it could cost you your livelihood. "When it comes to cybersecurity, there are no spectators in the stands," warns Dan Skiles, President of Shareholders Service Group and a former member of the FPA National Board of Directors. "We are all players in the field."

dvisors

To measure the scope of the cybersecurity risk in the industry, and to understand how advisors are managing that risk, the Financial Planning Association (FPA) Research and Practice Institute launched an in-depth examination into both advisor perception of cybersecurity and the actions firms are taking to protect themselves and their clients. Sponsored by TD Ameritrade Institutional, the research report, *Is Your Data Safe? The 2016 Financial Advisor Cybersecurity Assessment*, found that while the majority of advisors consider cybersecurity a high priority, many don't feel completely prepared to fend off an attack.

---

[1] "2016 Reported Data Breaches Expose Over 4 Billion Records," Risk Based Security, Jan. 25, 2017. (found here: https://www.riskbasedsecurity.com/2017/01/2016-reported-data-breaches-expose-over-4-billion-records/)

This research highlights two key takeaways for advisors, says Bryan Baas, Managing Director, Risk Oversight and Controls for TD Ameritrade Institutional. "First, cybersecurity risk is not going away. Cybersecurity is a laser focus for regulators, customers, and the industry," he says. "And second, while we have experienced a significant amount of momentum toward improving security in the last 12 to 18 months, we can't lose that pace."

Are You Prepared?

Among the key findings of the research is that while 81% of advisors ranked cybersecurity a high priority for their firm, only 44% "completely agree" that they fully understand all of the issues and risks associated with cybersecurity. Even more of a concern? Only 36% of advisors are confident that their teams understand all of the issues and risks.

"Sometimes advisors spend too much time on security systems and completely forget about the training. The two go hand-in-hand. One is not more important than the other."

—DAN SKILES
PRESIDENT,
SHAREHOLDERS
SERVICE GROUP

In fact, among firms with more than one employee, a third of advisory firms report that they have no cybersecurity training programs for current or new employees, according to the survey. Since support staff is on the front lines of client service and managing information systems, this lack of training exposes a huge vulnerability for the majority of advisor firms, Baas says. "Training your employees can be the easiest and simplest way to combat cyberattacks," he adds.

Another industry-wide concern is that only 26% of advisors are confident that they understand all of the cybersecurity requirements laid out by the Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE), and only 18% are confident they would pass an OCIE exam today. (See sidebar, *Translating the OCIE Requirements*, for more information.)

On a more positive note, 29% of the advisors surveyed "completely" agree that they are fully prepared to manage and mitigate the risks associated with cybersecurity. Those firms that are meeting the risk head-on are helping to provide a roadmap that the rest of the industry can follow.

Threat Assessments and Current Risks

The good news is that among the firms surveyed, only 4% reported that they had ever had client data compromised as a result of a security breach. A more troubling number, though, is that 7% of all respondents didn't know if they had ever been breached, so the number of breaches could be significantly higher. If you don't know if you've been breached, how can you tell if your systems are secure?

To address that issue, the first order of business is to conduct a formal analysis of your systems, scanning for vulnerabilities and identifying any soft spots in your system, Baas says. This includes understanding how your data is protected, who is responsible for that protection, and who has access to that data. For example, consider whether you can readily answer these questions:

- Is your encryption software up-to-date?
- Are your firewalls and antivirus software regularly maintained and updated?
- If you work with third-party vendors, do you understand how they are protecting your data?
- Is access to your data compartmentalized, so that access is limited to only those who need it to do their job?

A formal cybersecurity review tops the OCIE's requirement list, but among the firms surveyed, only 56% reported that they had conducted a formal cybersecurity review. That jumps to 72% for larger firms.

Best Practices

- **Create an Incidence Response Plan detailing what should happen in the event of a cyber attack.**
- **Only allow company-provided hardware and devices to connect to the company network.**

Training Your Employees

The research shows a clear disconnect between the importance advisory firms place on cybersecurity and the amount of training firms provide for their employees. Fewer than half of firms (44%) with more than one team member provide mandatory training for their staff, with the largest portion of firms (35%) providing training only once a year. Two-thirds (65%) of firms with training programs report that team members receive less than two hours of training every year.

"Sometimes advisors spend too much time on security systems and completely forget about the training," notes Skiles. "The two go hand-in-hand. One is not more important than the other."

Preparing your team begins with identifying one person within the firm who is primarily responsible for creating, implementing, and monitoring cybersecurity policies and procedures, Baas says. "Once you have designated someone to have the oversight and implementation of cybersecurity, you need to support them," he says. "Send them to conferences and then let them do the training."

The challenge for most smaller firms, though, is that employees are already juggling multiple responsibilities. So in firms with less than $250,000 in annual revenue, the responsibility typically falls on the CEO. As a result, the person with that responsibility

spends fewer than 20 hours a year managing or implementing cybersecurity protocols.

Best Practices

- **Create a clear, mandatory training program for all staff members, and make training an ongoing process.**
- **Make sure each employee understands his or her role in mitigating cybersecurity risk.**

Communicating With Clients

"The bad guys are looking for the quickest way in and the fastest way out, and for advisors, that is through your clients," Baas warns. The numbers bear that out. Among the known security breaches in the report, 60% were a result of client emails being hacked.

Unfortunately, most advisors believe their clients are not well versed on the issues surrounding cybersecurity. According to the survey, only 11% of advisors think their clients are "very aware" of the general risks associated with data security, and that puts advisors at risk.

But that doesn't mean that clients aren't concerned about it. A 2016 survey by Kaspersky Lab, a global cybersecurity firm, found than nearly two-thirds of consumers are worried about data breaches at companies to which they provide personal and financial information.[2]

So even if your clients aren't asking you directly, advisors should be talking to them about cybersecurity, and explaining all of the steps the firm is taking to keep the client's data secure.

Best Practices

- **Map out your cybersecurity plan and share it proactively with clients.**
- **Educate your clients about cybersecurity threats and provide guidance on how they can protect their personal information.**

While cybersecurity remains a constant threat, it also creates an opportunity for advisors to be more proactive in educating clients about the risks and the procedures in place to meet OCIE. In fact, 35% of respondents believe that their approach to dealing with cybersecurity is a competitive advantage, according to the survey. "Providing education and awareness is an important service that you can provide to your clients," Baas says. ■

Translating the OCIE Requirements

Cybersecurity is among the Securities and Exchange Commission's top examination priorities for 2017. Unfortunately, most registered investment advisory (RIA) firms aren't confident that they could pass an SEC cybersecurity exam, according to *Is Your Data Safe: The 2016 Financial Adviser Cybersecurity Assessment* by the Financial Planning Association (FPA). The SEC's Office of Compliance Inspections and Examinations (OCIE) has laid out exactly what examiners will be looking for, but it can be a daunting list for RIAs. To help get firms up to speed, Brian Edelman, CEO of Financial Computer, explains what the regulators are looking for within six designated areas.

BRIAN EDELMAN
CEO, Financial Computer

1. Government and Risk Assessment: Regulators want proof that you have conducted a thorough analysis of your systems to identify—and close—any vulnerabilities, and that you have a written cybersecurity policy that is tailored to your business.

2. Access Rights and Controls: Document who has access to what data and how that access is controlled. Do you have multi-level logins and authentication? Are team members allowed to access that data remotely? If so, are they allowed to use public wi-fi, and can they use their personal computers or smartphones? (Hint: No and no. See *Safely Bring Your Own Device to Work*, from the Q2 2016 issue of *Advisor Solutions*.)

3. Data Loss Prevention: This includes the full laundry list of security software, Edelman says: whole disc encryption, anti-virus and anti-malware software, a personal firewall, cybersecurity monitoring, and encrypted backups. Examiners may also look at how firms monitor the content transferred outside of the firm, either by employees or vendors, via email or uploads.

4. Vendor Management: Using outside vendors does not shift your fiduciary responsibility to protect client data. The OCIE wants to see your due diligence in vetting third-party vendors and proof that they are fulfilling their contracts in relation to client data.

5. Training: Employees are your first line of defense against cyber attacks, so it's critical that they are trained in how to spot suspicious activity and when to alert the IT department. You should also expect regulators to review how cybersecurity training is built into each employee and vendor's regular, ongoing training.

6. Incidence Response: This outlines what steps the firm and its staff will take in the event of a cybersecurity attack. Who needs to be alerted and in what order? Who is responsible for making each phone call? You also need to show that you regularly run tests on your system to make sure it works.

No, following these guidelines won't eliminate the risk of a cyberattack. But they can help prepare you and your firm should an attack occur, Edelman notes.

[2] From Client Perception white paper