Stay connected

FPA FINANCIAL PLANNING ASSOCIATION

Journal of Financial Planning®

EXPANDING THE BODY OF KNOWLEDGE IN THE FINANCIAL PLANNING PROFESSION

ATTENTION MEMBERS:

Please remember to change your address when relocating. Update your profile at **onefpa.org/myprofile**

August 2017 | Vol. 30 | No. 8
FPAJournal.org

10 QUESTIONS

Steven Ryder on Protecting Client Data, Preventing Phishing Scams, and Encrypting Devices

by Carly Schulaka

WHO: Steven Ryder

WHAT: President and founder of True North Networks LLC, IT and cybersecurity expert

WHAT'S ON HIS MIND: "A lot of this is common sense, and it is not a significant expense in the scheme of things."

After more than 15 years of providing IT support and managed services to hundreds of small- and medium-sized businesses—including a specialization in RIA firms—Steven Ryder has heard plenty of horror stories involving cybersecurity breaches and client data vulnerabilities.

The stories have a common theme of human error, and a lesson for advisers: the most important thing a financial advisory firm can do to thwart cybersecurity risks and protect their client data is to get people trained on how to identify and handle those risks.

Ryder will share his knowledge and guidance with advisers at the FPA Annual Conference, October 2–4 in Nashville, where he'll give an education session on cybersecurity issues and how to stay protected.

The *Journal* recently sat down with Ryder to learn more about how advisers can best protect their client data, the role staff training plays in successful cybersecurity efforts, how to encrypt moble devices, and more.

1. *Under current regulations, what obligation do financial advisers have to safeguard client data?*

Besides the obvious obligations with the SEC Office of Compliance Inspections and Examinations (OCIE) that require the adviser protect their client data, it's a fiduciary responsibility to take care of your client data. I think it's critically important, whether there is regulation or not, that protecting client data is the responsibility of all of us, including any type of company that safeguards client data.

There's more regulation, such as the proposed Main Street Cybersecurity Act of 2017 that would require the National Institute of Standards and Technology to develop simple, basic controls for helping small businesses guard against common cybersecurity risks. And New York state has come out with their own requirements for financial services companies: they require a certification statement to be signed on an annual basis by the chief information security officer on behalf of the company that

they are compliant with a number of things they need to do to protect client information against any cybersecurity breaches.

So it's both—certain regulations are enforcing it, but I also think there's a fiduciary responsibility to take care of your client information. (For a list of the primary focus areas for the SEC's Cybersecurity Examination Initiative, see sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf. For specifics on the New York state regulations, see dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf.)

2. *What are some of the most common cybersecurity risks for financial planning firms?*

I think the biggest risk is phishing. The Identity Theft Resource Center (idtheftcenter.org) has a telling chart that shows all the different types of breaches—brute force attacks, skimming, employee error, negligence. Most of them are very low on the X-Y axis, but if you look at phishing, it is off the charts. Hackers realize that the weakest link in the security chain is the end user.

We do a lot of work with SonicWall, and [according to them] in 2015, there were 3.8 million ransomware attacks; in 2016, there were 638 million ransomware attacks (phishing emails often contain ransomware).

A lot of the effort around preventing phishing is really social engineering, training, education, awareness—those types of things are critically important to make sure people aren't just wiring money. I met with a potential client yesterday that was interested in our services. They wired out $300,000 to the wrong place. Someone intercepted an email, changed one character of the email address and then emailed into the email chain acting like the person, saying, "Here's where to wire the money." And it's gone. They've called the FBI, they've called everybody they can. The money is long gone.

Security is a layered approach. You have a firewall, you have monitoring, you look at log files, you block websites—there's a whole layer of things that you do. But the most important thing you can do is get people trained and educated so they know what to look for.

Protecting client data is the responsibility of all of us.

3. *Should financial planning firms be concerned with possible insider threats?*

I think there's always a risk of that. Statistically it's a small risk, but it's important to safeguard data, making it difficult for people to take data off the network. Whether you're concerned about disgruntled employees or someone else stealing information, it's critically important to monitor ingoing and outgoing email for files that might be getting transferred, and locking down information so people can't put thumb drives in, capture data, and take it off the network.

4. *The SEC's Office of Compliance Inspections and Examinations (OCIE) has said that in 2017 it will continue its initiative to examine for cybersecurity compliance procedures and controls. What is the likelihood of an OCIE visit?*

If you look at the numbers, the OCIE monitors 4,000 broker-dealers, 12,000 investment firms, and 640,000 representatives. Their oversight is a lot of financial firms, so the likelihood [of an examination] may be small, but having the correct cybersecurity procedures in place is still critically important. Think of the R.T. Jones case. R.T. Jones didn't really have a policy in place to protect against a breach. They were fined $75,000.

So, I wouldn't say statistically the likelihood is high because of the number of firms the OCIE monitors; however, that doesn't mean you should not prepare for an audit, because I think you run the risk of something happening. And, God forbid, if something happens, the likelihood of them coming in is very high.

And what the SEC and the OCIE and even the State of New York are asking people to do is not ridiculous. A lot of this is common sense, and it is not a significant expense in the scheme of things.

5. *According to Pricewaterhouse Coopers, the most common type of cyberattack in 2016 was phishing. Can you tell us more about how advisers can best educate their clients to prevent phishing scams?*

There are a lot of resources out there to help with this. We use a company called KnowBe4.com that does security awareness training. Another company called Wombat also does awareness training. There's an organization called SANS that has a website called Securing the Human (securingthehuman.sans.org) that has great monthly newsletters and they're free. We subscribe to those as well.

Another company that a lot of RIAs use is Entreda, which has a comprehensive cybersecurity controls and compliance offering that includes employee training and awareness.

At True North Networks, we do random phishing tests for our clients. We send "phishing" emails and if someone clicks on it, we get a report that we send to the firm. We say, "These people have

FPA FINANCIAL PLANNING ASSOCIATION

KNOWLEDGE CIRCLES

Learn Your Way.

FPA's Knowledge Circles are gathering places for like-minded members who want to engage in dialogue about best practices and innovations on particular topics. Knowledge Circle participants also serve as content experts who help guide the creation of FPA content and educational programs.

Join a Circle:

- **Business Success**
- **Income Tax and Estate Planning**
- **International/Cross-Border**
- **Investment Planning**
- **Public Policy and Regulation**
- **Retirement Planning**
- **Theory in Practice (Academic/Practitioner)**
- **Women and Finance**

Become a Host:

Hosts will start conversations, encourage engagement, and nurture the continued growth of their community. Each Knowledge Circle has up to three hosts (minimum 12-month commitment).

For more information go to **OneFPA.org/Community/Knowledge-Circles**

clicked on this; here are some training videos."

Then we follow up the random phishing tests with online training videos. A lot of it is educating folks on what to look for in emails and to be really careful about what you're doing. I recommend that if you get an email you think is legit but you're not 100 percent positive, open it up on your phone, because your phone is generally not attached to the network.

For example, our website lists jobs available at our company. So, somebody might email jobs@truenorthnetworks.com, and I'll get a PDF or I'll get a Word document and sometimes I'm skeptical. Is it legit? From a business perspective, I don't want to not respond to a legitimate person who's trying to apply for a job here. So if I don't know who that person is, I will open that PDF or Word document on my phone, because I don't want to infect the network and would rather risk infecting my individual phone.

6. *How often do you recommend a financial planning practice conduct cybersecurity training for employees?*

Employees should get cybersecurity training at least annually; preferably semi-annually, and if you want, on a quarterly basis. Any time a new employee comes on, get them set up on training and continue to try to catch people off guard.

KnowBe4.com, Entreda (entreda.com), and Wombat (www.wombatsecurity.com) are three firms that specialize in phishing exams, phishing tests, and training.

7. *Your company, True North, routinely provides network security audits. What's involved in such an audit, and what do financial planning firms typically learn from an audit?*

It's going to vary by client, but let's take a look at the New York policy. New York just came out with new cybersecurity guidelines that call for annual penetration testing and bi-annual vulnerability assessments for financial firms in the state of New York, although there are exceptions for smaller firms.

Penetration testing is an attack from the outside. How do I get through the firewall? Are there any open ports?

The vulnerability assessment is more on the inside of the network. Are machines up to date? Are there any routers or switches or any vulnerabilities that haven't been updated, as far as patches, for any other network type of equipment?

We do an assessment and it is a snapshot in time. We do it and I say, "Do all these things and you're good," but an hour later, the current managed provider could open a port on the firewall, they could open a port on a server, there could be a new update for a Windows patch that hasn't been applied. It's a snapshot in time, which is why you can't just do this once every five years. You should do it at least annually to get a snapshot of where things are at. It's important for auditing purposes to test providers.

Some things a firm might typically learn from an audit are: is your IT provider doing their job? Are they patching your systems? Is the firmware on routers and switches and firewalls all current and up to date? Are there any ports?

The audits may also reveal vulnerabilities. I've seen horror stories where we've done a security assessment and there's a remote desktop port open on a firewall that should not be open, but many IT companies don't understand security. So, they open this port on a firewall and a random computer will try to exploit that port.

Over the years, there have been many examples of this, but the worst case was when I showed someone 35 pages of single-line entries of random user names and passwords from a computer

trying to hack into the network. Nobody was looking at the server logs, nobody was seeing that the vulnerability existed. I recommended the port be shut down immediately, because eventually the computer will guess a correct user name and password sequential and get into the network unknown to them.

Here's another example: somebody will have a vendor, and that vendor has to remote in to the machine just to help out so they'll open up a port on the firewall. It's all with good intentions. The person will go in, help out, and they're done, but they forget to close the port on the firewall. This is where vulnerability or penetration testing can help.

Some people think that "security by obscurity" is the norm. It isn't.

Assessments are not just about cybersecurity; it's also about data integrity and data security. Here's another example that has nothing to do with cyber, but it shows why it's really important to look at assessments.

Several years ago, I was called in to do an audit. We looked at the environment and at the security assessments, and everything was pretty secure. Then I found that the back-ups had not run since February (and I was called in in June). The owner of the company was taking home blank tapes with nothing on them for four months. When I told the owner he had been taking home blank tapes for months, he said that was not possible; he had a log file and a binder with all the documentation that had all the back-ups. When I looked at the log file, I found that the last log entry was in February. You can imagine, the IT person is no longer there. If they had a fire within that four-month period, they would've been done; they'd have nothing.

8. *Major cyberattacks, like the recent WannaCry ransomware campaign, get a lot of media exposure, but we tend to hear about attacks like these after the fact. Are there ways for financial advisers to be proactive in learning about attacks as early as possible?*

How much information can you take in? It is almost impossible for a financial firm to stay on top of everything because they're monitoring their clients' money, they're managing their client accounts, they have to stay on top of the market, they have client needs. So, thinking about a financial advisory firm, it's important to have an IT partner—whether it's an employee, a managed partner, or any other IT company—that keeps you informed and is aware of what's going on in the industry to alert you of things that are happening.

For example, we've got a team of 30 people here who are keeping everybody alert and aware, and are communicating with each other. If somebody sees something, we say something, and we try to get information out immediately to our client base. With WannaCry for example, we were seeing information before it was in the press and we released information very quickly to our clients. And fortunately, not a single one of our clients got WannaCry.

9. *What recommendations do you have for securing mobile devices?*

Mobile devices are less of a concern than PCs, but it's still a concern because a lot of phones have contact information in them that can be gathered. The first thing we usually tell people is, encrypt your devices.

With Apple devices, once you put a password in, it automatically encrypts. With Android, you have to go through a different process to encrypt your device. And when I think of mobile devices, that also includes laptops, so make sure your laptop is encrypted in the event that it's lost or stolen. The biggest risk may be a laptop because there's likely to be a lot more data on it.

Another type of mobile device is the thumb drive. If you allow people to transfer documents to thumb drives—which I don't advise you to allow—enforce that that thumb drive is encrypted as well.

Microsoft has BitLocker that has encryption; it's free, it's part of the operating system. And, it's a good idea to have even a rudimentary way to wipe mobile devices. With iPhones and iPads, you can wipe those devices usually with a mobile management-type software. You can even wipe your iPad with Office 365.

10. *You will present an education session on cybersecurity at the FPA Annual Conference in Nashville in October. What do you hope attendees take away from your presentation?*

I hope they take away some tips or tricks that can make them feel more comfortable with securing their client data, and I hope they get a sense of the importance of doing so.

Some people think that "security by obscurity" is the norm. It isn't. I don't care whether you're a sole proprietor or a larger firm with multiple locations—everybody is vulnerable.

I'm not trying to scare anybody, but I want people to understand that good cybersecurity processes and training is also good business. This is not just about security; it's also about giving your clients a feeling that you care and you're doing what you can to protect their information. ■

Carly Schulaka is editor of the Journal. *Contact her at CSchulaka@OneFPA.org.*