Cybersecurity: Preparing Your Team

Cybersecurity may be high on your priority list, but do you have a plan for training staff?

In a white paper released by FPA and TD Ameritrade Institutional, 81 percent of advisers said cybersecurity is high or very high on their firm’s priority list. But there appears to be a gap between being concerned about cybersecurity and actually providing mandatory training for staff.

The white paper, titled “Cybersecurity: Is Your Team Prepared?” reported that 11 percent of firm CEOs “completely agree” that their team is fully aware of what would be required to adhere to guidelines set out by the SEC’s Office of Compliance Inspections and Examinations (OCIE). And only 44 percent of firms with more than one team member provide mandatory training for employees.

Finding the right training for you and your staff is the ticket to closing that gap and safeguarding and preparing your firm for cyber attacks.

The white paper reported that the average team member receives less than two hours of cybersecurity training per year. But it offered some steps to take action on training.

1. Define clear goals when it comes to cybersecurity. Keep the OCIE requirements as well as the goals of your team in mind during training.
2. Define team expectations in relation to those goals. Be clear and concise in communicating your expectations.
3. Gather input from the team. What questions or concerns do your team members have when it comes to cybersecurity?
4. Conduct an anonymous internal assessment. Find out what your team knows and understands regarding OCIE requirements and cybersecurity.
5. Identify the gaps. Focus your training on closing these gaps.
6. Create a training process. Determine how often to conduct training, whether it’s mandatory, and how you will deliver that training, among other things.
7. Summarize the training process. Summarize the process on a single page so you can tell your clients what you are doing.

For a sample assessment recommended in step No. 4, download the full white paper at OneFPA.org/cybersecurity.

“The debate about whether robos or human advisers will win is moot. The future of financial advice is bionic—a powerful combination of both.”

—David Siegel, CEO of Investopedia, Investopedia
9 Cybersecurity Tips to Keep Your Firm Safe

If somebody walked up to you and asked for your house keys, you wouldn’t give them away. But when somebody asks for our key identifying information on the Internet, most of the time we willingly hand it over.

That’s what representatives from SeeGee Technologies Inc., a next-generation technology solution provider, told FPA staff at a recent cybersecurity training.

You may think that just because you have a small firm, cyber criminals don’t have any interest in you, but that’s not true. In fact, you are their portal into bigger pools of information. And your employees could unknowingly be putting you and your clients at risk each time they access sensitive information over unsecure connections.

“Any individual or business is safe,” said Daniel Lakier, chief technology officer for SeeGee.

Always exercise common sense and responsibility when using the Internet and apps—don’t click on pop-ups, don’t click on links to track packages you aren’t expecting, and don’t provide personal information to hackers posing as your bank.

Here are some tips to keep your personal information and your firm’s information safe:

- Establish strong passwords and update them every 90 days.
- Don’t download email attachments you aren’t expecting and beware of emails telling you to download software to fix problems.
- Install anti-virus and anti-spyware programs on all devices before connecting to the Internet.
- Install and use a firewall on every device.
- Have physical access controls for all your devices.
- Backup all important data daily.
- Keep your software updates for browsers and operating systems current.
- Limit access to sensitive and confidential data and don’t ever access it on unsecure connections.
- Get technical expertise when needed.

For more information, visit seegee.com.

---

STAT BANK

18...Percentage of investors surveyed who have searched for an automated investing platform.

7...Percentage of investors currently using an automated investing platform.

73...Percentage of investors who are satisfied or very satisfied with the primary automated investing platform they are using.

53...Percentage of advisers who said that spending on compliance and technology is a priority for 2017.

$5.4 billion...Investment in fintech in the first quarter of 2016, a 67 percent increase over the same period last year.

75 percent...Overall growth of global fintech investment in 2015.

$150 billion...Estimated cumulative investment in fintech globally over the next three to five years.

$61 billion...Estimated assets under management of robo-advisers in June 2016 in the U.S., up from $11.5 billion in 2014.

81...Percentage of advisers who say that addressing cybersecurity is high or very high on their priority list.

2.9...Percentage of advisers who admitted that a successful attack had been launched against them or their firm.

44...Percentage of firms with more than one team member that provide mandatory cybersecurity training to employees.

> 169 million...Number of personal records exposed in 2015 from 781 breaches across the financial, business, education, government, and health care sectors.

38...Percentage more security incidents in 2015 than there were in 2014.

$2.1 trillion...Projected costs of cybercrime by the year 2019.