This blind spot is putting financial advisors and their clients at risk

July 11, 2019

It’s an email every financial advisor should expect to receive at least once.

Financial advisor Charles Failla recalls receiving an email from a client asking for about $5,000. She was vacationing in the Caribbean and claimed the hotel where she was staying didn’t accept credit cards.

“She needed cash,” said Failla, certified financial planner and principal at Sovereign Financial Group in New York.

“I said, ‘I know you’re on vacation, but call me collect. I need to confirm it’s you before I send money to a Caribbean island.’”

After several emails, the client was able to track down a phone and confirm her identity.

“She understood and appreciated it,” Failla said. “It’s definitely a policy at our firm: You get an email asking for money? Verify it with the client via telephone.”
He was right to be suspicious. Last year, victims lost $2.7 billion to cybercrime, according to the Federal Bureau of Investigation.

The Securities and Exchange Commission, as well as state securities regulators, are paying close attention to financial advisors’ cybersecurity practices.

Whether you directly manage clients' assets or your practice specializes in financial planning, you'll need to protect your customers' data.

Even large companies aren't immune to internet scammers. Last September, New York-based Voya Financial Advisors paid the SEC $1 million to settle charges regarding a data breach that compromised customers' personal information.

Though advisors themselves are under pressure to protect their firms from cyberattacks, they're often unsure where to start.

"We're always getting hackers trying to break into the firewall and go on phishing expeditions, but people don't think about what they will do when they have a breach," said Michelle Jacko, CEO of Core Compliance & Legal Services in San Diego.
The SEC's Office of Compliance Inspections and Examinations highlighted cybersecurity as a 2019 examination priority.

There are two types of audits advisors should expect from the federal regulator, according to Wes Stillman, CEO of RightSize Solutions, a cybersecurity consultancy in Lenexa, Kansas.

"Cybersecurity is part of the normal SEC exam: There might be 13 to 15 questions around information technology and cybersecurity," he said.

"Then there's the big cyber sweep: Forty-plus questions around policy, cybersecurity and all that good stuff."
In either case, regulators want to make sure advisors have written policies and procedures around the rules and methods used to safeguard devices and data.

This manual should include the firm's approach toward mobile computing, virus protection, remote access and more. It needs to be kept current, and staff members must be trained on how to follow it.

"We run into people who say 'Sure, we have a written policy,' and it's referencing SkyTel pagers and 56K modems," said Greg Goldstein, president of Highridge Technology in Ho-Ho-Kus, New Jersey. "That's almost worse than not having a policy at all."

Firms need a written incident response plan, spelling out the necessary steps to address a cybersecurity incident, vulnerability assessments and details on who is responsible for implementing the plan after a data breach.

"Everyone needs to know their role, including legal counsel," said Bryan Baas, managing director of compliance for TD Ameritrade Institutional. "When the roof comes crashing down, you won't have the time or the patience to field questions on what happened and what do we do."
Advisors should be aware of three key risk alerts from the SEC Inspections and Examinations,

said Jacko of Core Compliance.

These alerts highlight vulnerabilities SEC staff has spotted while examining advisory practices.

One recommends establishing rules around electronic communication, including reviewing employees' use of social media and ramping up security around remote access to email.

A second risk alert addresses the use of policies and procedures on customer privacy and establishing safeguards to protect client records.

During its exams, SEC staff "observed registrants' employees who regularly stored and maintained customer information on their personal laptops," according to the risk alert.

Firm policies and procedures didn't address how to safeguard clients' data, the SEC said. Finally, a third risk alert, issued in May, covers client data protection when firms use cloud-based storage.

Indeed, the SEC's exam staff found that some firms didn't properly configure the security settings on their network storage solutions to protect against hackers.

The SEC also uncovered another vulnerability: Some advisory firms failed to make sure their third-party vendors' cybersecurity practices were up to snuff.

"These cybersecurity issues transcend registered investment advisors," said Failla. "A lot of these cracks in security come from the relationships businesses have with third-party vendors."
Cybersecurity consulting advice doesn't come cheap. For instance, Goldstein can charge up to $10,000 a year for staff training and regular onsite meetings with executives.

Nonetheless, all firms need to adopt a formal approach toward cybersecurity. Here's where to begin.

• Draft your policies and procedures: "The two big things regulators want when they walk in the door is 'Who is accountable for the cybersecurity program?' and 'We want to see the documentation for the plan,'" said Baas of TD Ameritrade.

New York State's cybersecurity requirements can act as a good checklist for advisors to follow for best practices, said Failla.

• Enforce your own rules: Auditors want to make sure you're putting your own policies and procedures into action. "Your policy might say that you train the employee on cybersecurity," said Stillman. "How do you do that and how do you track their progress?"

• Run a fire drill: "Vulnerability tests are highly technical and can run from $1,500 to tens of

thousands of dollars, depending on the size of the firm and the depth they go," said Stillman. "Be prepared to fix the problems it shows you."

• Query your vendors: Ask about their cybersecurity plan, their vulnerability testing and how they would proceed amid a data breach.

"Go visit your vendor if you can and understand the physical environment," Baas said.

More from FA Playbook:
Cringeworthy money mistakes clients have made
5 tips for advisors to consider before the stretch IRA is out
New tax rules give real estate investment trusts an advantage