CNBC

Is your advisor prepared to handle cyberattacks?

Deborah Nason, special to CNBC.com

Friday, 16 Oct 2015 | 7:00 AM ETCNBC.com

http://www.cnbc.com/2015/10/15/is-your-advisor-prepared-to-handle-cyberattacks.html

We're being watched ... by cybercriminals. And if we don't stay vigilant, the costs can be overwhelming.

Data breaches cost an organization an average of $6.5 million, according to a 2015 study from the Ponemon Institute and IBM, which examined the costs incurred by 62 U.S. companies, across 16 industry sectors, that experienced the loss or theft of personal data. About half of the incidents were caused by cyberattacks, while the rest were caused by system glitches or human error

Cybersecurity is also a hot topic in the financial advisory space.

To that point, last month an investment advisory firm agreed to settle charges by the Securities and Exchange Commission that it failed to establish required cybersecurity policies in advance of a security breach that compromised customer data. The firm was fined $75,000 by the SEC, which explained that the breach compromised the personally identifiable information of about 100,000 individuals, including thousands of the firm's clients.

Widespread ignorance

Most of us are in over our heads.

"It needs to be recognized that neither clients nor advisors have the necessary technical knowledge to understand common risks and how to counteract them," said Peter Palion, a certified financial planner and a registered principal with United Planners Financial Services.

Palion gives some examples of common cybersecurity risks:

- Downloading PDF files without realizing there is still a temporary copy in the computer, and not knowing how to clean out the cache.
- Using one computer for the whole family — and the kids downloading malware.
- Not realizing the traces of their activities on their mobile devices.

"On top of all that, most of the stuff we need to keep track of is on the Internet itself, such as password managers," Palion said. "Look at account aggregation — everything is in the cloud. Neither service providers nor broker-dealers are providing guidance to advisors or clients."

It's clear, however, that savvy financial advisory firms are changing their systems and procedures to protect clients and their own firms from the rising cases of cybersecurity attacks and breaches.

Fighting back

Jorge Padilla, CFP and client advisor with Lubitz Financial Group, said his firm is taking a variety of measures, such as hosting a recent public webinar on cybersecurity for clients and friends.

"We implemented a written information security program that has been incorporated into our policies and procedures to create more clear guidelines on measures we take internally to protect confidential information," he said.

"We also have implemented an online secure vault for sharing confidential information to clients," he added. "This vault is part of our online My Money Life client portal, where clients can see their accounts as well."

In addition, his firm relies on its custodians to provide support and advice on how to best handle any ID theft or breaches on their accounts and websites.

Barriers to breaches

Linda Lubitz Boone, CFP and president of Lubitz Financial Group, shares some of the measures her firm has undertaken to safeguard against data breaches:

- Detecting unauthorized access.
- Reviewing and ensuring business risk is addressed in business compliance procedure.
- Compiling a list of vulnerable vendors (those with access to confidential client data) and verifying that they have information security programs.

- Obtaining cybersecurity insurance in conjunction with E&O insurance.
- Addressing screen-sharing protocols.
- Including lost phones or laptops as potential breaches in attestation and policy.

Cybersecurity is front and center for Steven J. Stanganelli, CFP and principal at Clear View Wealth Advisors.

"When I talk with [clients and prospects], I disclose how I deal with security of client data right up front," he said. "I explain to them that I will provide them with a dedicated and secure client folder accessible through Citrix ShareFile, where sensitive information can be shared."

As part of the planning process, Stanganelli also uses MoneyGuidePro software and encourages clients to link their accounts using the Yodlee integration tool, which, he noted, boasts the same level of security used at banks.

"Both clients and prospects appreciate it when I mention this," he said. "Many will comment on their concerns about ID theft, especially highlighted during tax season, when there were security breaches reported by the IRS."

Stanganelli's firm also uses encrypted and password-protected hard drives and keeps sensitive equipment in locked offices.

Karl F. Frank, CFP and president of A&I Financial Services, said his firm uses a program called Security Snapshot to monitor all the other software and make sure it is always up to date. The program issues an alert to take action if, within the first 24 hours, a software has not been automatically updated.

In addition, "we have different team members perform the audits of each other to make sure we are in compliance with our processes," Frank said.

For her part, Juli Erhart-Graves, CFP and president of Worley Erhart-Graves Financial Advisors, takes cybersecurity "very seriously."

"We have a page on our website devoted to cybersecurity that encourages freezing credit files and talks about [our custodian] and their two-step verification," she said. "We are so concerned about security, we even clean our own offices." *—By Deborah Nason, special to CNBC.com*