Are you an informed investor?

CYBERSECURITY:

IS YOUR INVESTMENT PROFESSIONAL TAKING STEPS TO SAFEGUARD YOUR FINANCIAL INFORMATION?

. . . If not, it's time to have "The Talk!"

The list of financial institutions targeted by organized cyber attacks continues to grow with ever-increasing frequency. Since investors are encouraged to take steps to ensure their own personal systems are updated with the latest anti-virus and anti-malware software, and to follow proper account password safety protocol, they generally trust their investment professionals to do the same on their behalf.

But do they?

In September 2014, the North American Securities Administrators Association (NASAA), the longest-serving international investor protection organization, released results of a pilot survey designed to better understand the cybersecurity practices of state-registered investment advisers. These advisers account for more than half of the registered investment advisers conducting business in the United States.

The survey, conducted in early summer 2014 in nine states, found that 62 percent of firms have undergone a cybersecurity risk assessment, and 77 percent have established policies and procedures related to technology or cybersecurity. The pilot survey also found that very few state-registered investment advisers reported experiencing a cybersecurity issue.

While the relatively low rate of cybersecurity incidents identified in the pilot survey is encouraging, investors should think about the safety of their financial information, and talk with their investment professionals about what steps firms are taking to safeguard client information.

(over)

Issued: January 2015

Contact NASAA
Phone: 202-737-0900 | Fax: 202-783-3571 | Web: www.nasaa.org

Here are some questions that investors should ask their investment professionals:

- ***Cyber preparedness:***
  Has the firm addressed which cybersecurity threats and vulnerabilities may impact its business?

- ***Cybersecurity compliance program:***
  Does the firm have written policies, procedures, or training programs in place regarding safeguarding client information?

- ***Cyber insurance:***
  Does the firm maintain insurance coverage for cybersecurity?

- ***Cyber expertise:***
  Has the firm engaged an outside consultant to provide cybersecurity services for your firm?

- ***Cyber confidentiality:***
  Does the firm have confidentiality agreements with any third-party service providers with access to the firm's information technology systems?

- ***Cyber incident:***
  Has the firm ever experienced a cybersecurity incident where, directly or indirectly, theft, loss, unauthorized exposure, use of, or access to customer information occurred? If so, has the firm taken steps to close any gaps in its cybersecurity infrastructure?

- ***Cybersecurity safeguards:***
  Does the firm use safeguards such as encryption, antivirus and anti-malware programs? Does the firm contact clients via email or other electronic messaging, and if so, does the firm use secure email and/or any procedures to authenticate client instructions received via email or electronic messaging, to work against the possibility of a client being impersonated?

√ *The Bottom Line*

As a customer, you have the right to ask these questions and get answers you can understand in writing. This is all part of the process of doing your due diligence and becoming … an Informed Investor!

If you have any questions, contact your state or provincial securities regulator. Contact information is available on the website of the North American Securities Administrators

NASAA Informed Investor Alert

This information was prepared by the Alerts & Advisories Project Group of NASAA's Investor Education Section. For more investor alerts and advisories, visit www.nasaa.org