Cybersecurity For Small RIAs

September 8, 2017

Small RIAs are more susceptible to cyberattacks than their owners would like to believe. In fact, with smaller technology budgets and insufficient controls, small firms may be the perfect targets for hackers.

According to a recent report by Symantec on Internet security, personal financial information was the second most common form of data stolen in 2016, behind personally identifiable information.

Implementing and enforcing cybersecurity measures properly should not break the bank. Even without deep pockets to invest in cybersecurity, RIAs should have policies and measures in place to prevent fraud. There are plenty of bells and whistles to choose from, which can make it hard for an advisor to discern what is really necessary. To help, here are six basic elements that should be the foundation for every small RIA's cybersecurity program.

Use Password Vaults

Passcards hold the authentication credentials to access specific applications and automatically log the user into their assigned applications. Password vaults are a secure solution for storing passcards for RIAs of any size. Typically, there is a master password that grants access to all of the passcards in the vault.

A word of caution: when firms allow employees to create their own passcards, they give them the credentials to access the applications without the use of the vault. This means anyone with credentials can log into applications on unprotected or virus-infected devices, such as personal devices, increasing the risk of a breach. This is typically more problematic for smaller RIAs, which are more likely to lack a chief compliance officer and may neglect compliance.

Firm owners can enforce secure access by creating passcards for all employees for all business-based applications. This virtually eliminates the possibility that others have access to core business applications outside of the password vault and secure devices.

Adopt Two-Factor Authentication

Two-factor authentication is quickly becoming the standard for secure logins. Whereas the password is "the thing you know," authentication is "the thing you have." This typically means receiving codes on an authorized device such as a mobile phone or responding to additional prompts to authenticate your login.

Advisors who utilize password vaults and two-factor authentication give their firms quite a bit

of cybersecurity protection, even if they do nothing else to guard against potential fraud.