15 Cost-Efficient Cyber Best Practices for your RIA

February 26, 2018

15 Cost-Efficient Cyber Best Practices for your RIA

It’s no longer an option to view cybersecurity as just a component of your overall technology plan. RIAs need to use proper cybersecurity as an overarching framework to plan, manage and budget all IT initiatives…however, implementing and enforcing cybersecurity measures properly doesn’t have to break the bank. Many fraud-preventing measures can be supported by implementing best practices.

In our latest whitepaper, Changing the Cybersecurity Conversation, we share specific controls and best practices that can help protect your firm and your clients’ data, including:

- Use secure passwords. Remind associates to use secure passwords and multi factor authentication. These days, passwords are quickly becoming just a part of confirming identity. Having a combination of a password and a personal identifier (something you know, and something you have) is quickly becoming the norm.
- Use a password manager. Password managers provide access across multiple devices, programs, and apps. Opt for the premium or enterprise version to receive extra features, such as alerts when one of your sites or services has been breached and priority customer service.
- Encrypt your devices. Encryption technology can be cumbersome and relatively time consuming compared to typical online interaction but has a very real and important business purpose. Recognize when it’s appropriate and don’t overuse encryption. Sending encrypted emails for basic email communication will quickly become tiresome for your employees and clients, but when used properly can help PII and PFI from leaking.

Get 12 more best practices that your RIA should implement when you download our latest whitepaper, Changing the Cybersecurity Conversation.Changing the Cybersecurity Conversation.

Need a cybersecurity partner who cares about your firm’s growth and success? Let’s talk.