Empower Staff to Recognize Red Flags

February 16, 2018

Empower staff to recognize red flags

While media coverage of cyber incidents (such as data breaches, ransomware attacks, malware and viruses) has built well-deserved awareness of the need for cybersecurity, it has also generated fear while doing little to provide answers.

As an RIA, you are responsible for the security of your own firm, and the personal data of your clients—but this responsibility shouldn't be a fear-based burden. In our latest whitepaper, Changing the Cybersecurity Conversation, we demonstrate how to deal with cybersecurity in a proactive and positive way that can significantly contribute to the growth of your firm.

Here's an excerpt:

Knowledge is Power
Ways to empower staff to enhance the client experience

Policies and Procedures are only as good as your weakest link. Learn how to empower employees to recognize red flags and confidently respond to potential incidents. Basic education can go a long way toward increasing client service efficiency and productivity.

Encourage your employees to report abnormalities, and avoid discouraging false alarms. Building an environment where employees feel comfortable reporting issues without repercussions is paramount to identifying and acting upon breaches or other cyber issues as soon as possible. While first instinct might be to chastise an employee that opened a questionable email attachment, being able to act in the first couple hours can actually save a lot of damage. You will be much worse off if the employee doesn't report it, and the virus/ransomware/malware, is able to run for hours, days, even months without detection.

Download our latest whitepaper, Changing the Cybersecurity Conversation, to learn how your RIA can positively respond to the call of cybersecurity within all aspects of your business: firm culture, client experience, operational management, and business development.

Need a cyber security partner who cares about your firm's growth and success? Let's talk.