9 Ways to Create a Culture of Cybersecurity

June 7, 2016

The biggest stumbling block for registered investment advisors when it comes to guarding against cybersecurity breaches is not technology-based, it's a people problem. The right technology is critical, but RIA leaders can face a bigger challenge in fostering a cybersecurity-sensitive culture in a way that resonates throughout all levels of their firms.

RIA technology policies should be non-negotiable, but the reality is, today's work force tends to need convincing about how these protocols benefit and protect them, their employers and their clients from cyberattacks. Generation X and millennials in particular place a higher premium on convenience versus privacy.
With rare exception, no advisor or RIA employee intends to put client data or firm assets at risk by not adhering to firm policies on cybersecurity. But cyberthieves are increasing in their sophistication, making compliance with these policies a necessity. There was a new identity fraud victim every two seconds in 2014 — that's $16 billion stolen from 12.7 million U.S. customers — according to Javelin Strategy & Research's 2015 Identity Fraud Study.
Firms are best served when the senior leadership explains why their cybersecurity policies exist and deliberately models appropriate behavior. When the top levels of the RIA lead by example, cybersecure behavior and attitudes become "normalized" and compliance is much easier to come by.

RIA owners wondering how to start building a cybersecure culture can lead by example with the following:

1. Formally review the firm's technology policies regularly. Most RIAs insist that those new to the firm read, review and sign the firm's documented policies on technology usage and security. Requiring everyone to revisit and re-sign technology policy documents at least annually is a reminder to advisors and staffers about the importance of compliance.
2. Circulate outside news about cyberattacks. Share the latest headline news on cybersecurity breaches with your colleagues and include a short note with key takeaways and reminders for the firm.
3. Update the firm on its own cybersecurity successes. Make it clear that cyberattacks happen extremely close to home by sharing your firm's data internally. How many phishing emails were quarantined? How many did not get through firm firewalls? Which staff members should be applauded for calling attention to suspicious activity? At weekly team debriefings or monthly staff meetings, share the statistics that will make a meaningful impression.
4. Share key learnings from industry events. At the next advisor conference or other

networking event, attend at least one session on cybersecurity. Take copious notes and report back on the main takeaways for keeping the firm protected from thieves.

5. Weave cybersecurity into client conversations and new business pitches. Clients may not choose a RIA because of its cybersecurity protocols, but they will certainly leave one if there has been a breach or if they feel their assets and information have been compromised. Take time to explain the firm's cybersecurity investments and policies and why they are a benefit to clients, and periodically update clients on the firm's efforts.
6. Show clients that cybersecurity matters to the firm. Whether clients visit the office, call in, or advisors meet them offsite, let them experience the team doing extra logins for security, and taking extra steps for identification over the telephone.
7. Insist on dumbed-down devices. It is possible to use one mobile device for work and personal matters, and in so doing keep firm and client data secure. Doing so means relinquishing the concept of a "smart phone" and instead giving users mobile devices that only have one work application — the one that gets the user to the firm's protected smart platform through a multi-factor authentication. Once on the platform, the user can get to any application they need through a centrally managed password vault.
8. Consider bringing in outside experts for education. RIA leaders do not have to become experts on cybersecurity in order to guide their firms. Invite the firm's technology partners to speak at the next offsite or planning meeting, or sign the firm up to attend a webinar.
9. Be regulator ready. Industry regulators are paying increasing attention to cybersecurity policies and enforcement, and want to see that firms are taking a more active stance against potential breaches. Set the standard for RIA security by instituting a systematic and replicable ongoing awareness-training program for all advisors and staffers.

Clients entrust RIAs with an awesome and serious task: Their advisors are managing hard-earned assets to achieve very personal life goals. The magnitude of this responsibility should give advisors pause and consider: As part of my mandate, is my firm taking the necessary preventative measures to ensure that our clients are protected from cyberthieves?