Is Your Right-Hand Talking to Your Left-Hand?

January 8, 2019

Arguably two of the most important and interrelated business practices for any RIA are those firms that support compliance and technology. However, often, you find firms taking a silo service approach, resulting in the RIA not effectively managing either of these critical functions.

System intrusions and data breaches have plagued the financial services industry in recent years and this will only continue. As regulatory scrutiny of RIAs increases, advisors need more than off-the-shelf infrastructure offerings to ensure they are protecting firm and client data to the best of their ability. Aligning compliance and technology partners to make sure these efforts complement each other is a critical step in this process.

The internet and electronic communications are integral to how RIAs do business and interact with clients, making the cybersecurity policy a necessary defense against bad actors. Most cyber events are caused by carelessness, ill-will or lack of training, but malicious attacks can come from anywhere. This includes cybercriminal and hactivists, competitors, vendors, and even firm insiders or employees. Having an established and well documented cybersecurity policy is the first step in this process.

Unfortunately, most RIAs lack an enforceable and manageable cybersecurity policy within their overall compliance manual because most compliance firms are not experts in technology. Even when a compliance team is very knowledgeable in the technology space, they have no way of enforcing the policy. As found in the OCIE's 2017 summary of observations, firms did not enforce their own policies and procedures, or the policies and procedures did not reflect the RIAs actual practices. This makes them easy targets in an age where cybercriminals are running highly sophisticated and highly lucrative operations. Without a multi-faceted program in place, cybersecurity becomes a game of Whac-A-Mole, with reactive responses rather than proactive solutions.

With the right technology partner, RIAs can better understand their unique risks and implement policies procedures, training, assessment and the best tools to mitigate cybersecurity risks. By weaving cybersecurity protocols into the fabric of daily operations, the policy protects and monitors access, data storage and transmission from the RIA perspective.

The bottom line: By having both compliance and technology firm's efforts in sync and working together, ultimately everyone benefits—RIA owners, staff, and clients, and allows advisors to focus on doing what they do best.

Read our most recent whitepaper The Cybersecurity Policy Upgrade Imperative for RIAsThe

Cybersecurity Policy Upgrade Imperative for RIAs to learn how you can best align compliance and technology.