Are You Ready for a Tech Emergency?

June 11, 2015

Many registered investment advisors (RIAs) are now on the hook for assuring clients that their systems will run at all times, regardless of circumstances.

The North American Securities Administrators Association (NASAA) adopted its Model Rule 203(a)-1A or 2002 Rule 411(c)-1A, requiring state-registered RIAs to develop business continuity and succession plans that detail how operations will "minimiz[e] service disruptions and client harm" in the event of a disruption – such as natural disasters, equipment or system failures and records destruction, terrorist acts, unexpected loss of a market or service provider, unexpected loss of key technology providers, death, or any event that materially impacts the normal functions of the advisor. The Securities Exchange Commission is also expected to pass a similar rule for larger RIAs.

The charge may seem daunting, but advisors can collaborate with their technology service providers to develop plans that account for the myriad of front- and back-office systems running their businesses. Whether going it alone or with the help of outside experts, the end goals are the same for every RIA: compliance with the new rule, and having a Plan B protocol can be executed flawlessly when it matters most.

To get started, RIAs should ensure their business continuity and succession plans address the following five areas of concern:

• Control. Start by documenting who is authorized to have control of, and access to, the firm's information and systems when it is not business-as-usual to ensure that services are not disrupted. RIAs can follow the model of A.L. Rhodes, an advisor in Mukilteo, Washington, which designated by name the individuals who will have access to what files and systems in the event of a disruption.

• Mission-critical instant access. RIAs need to think carefully about the data that are most important in an emergency, and ensure that these files are assembled "to go," up to date, and can be restored quickly in any scenario. This is the firm's survival kit, and the RIA needs to show that there is a plan to get access to it in the event of a crisis. Indeed, the National Archives & Records Administration in Washington, DC, has reported that 93 percent of companies that lose their data center for at least 10 days due to a disaster filed for bankruptcy within one year of that disaster.

Each RIA will have its own definition of what constitutes mission-critical data, but to start consider: client and employee contact details; the business continuity plan; access information for core systems; technology vendor information; as well as custodian and other trade-related information.

• Information sharing and access. With key data identified and ready to go, the plan should include the process for information sharing across all platforms integral to the RIA's business. This could include custody, clearing, trade-execution, CRM, and record-keeping, to name a few. This information should only be made available when necessary, and it should otherwise remain secure in the encrypted folder that is part of the firm's emergency kit.

• Communications. RIAs should map out a communications strategy for reaching clients, employees, vendors, regulators and other key constituents in a crisis. For example, the firm that wants to send out a mass notification email at the time of a disruption will need a plan for communicating with clients when key systems go down and contact information is not readily available.

• Long-term operations. Advisors need to be able to show how they will stabilize the firm for the first hours and days following a disruption, and for keeping it running for the duration. This means addressing data migration, cybersecurity issues, relocation, and other technology-related matters in the business continuity plan.

Advisors should identify possible outage scenarios, examining their potential impact and develop plans accordingly. An office move or overnight snowstorm need not disrupt operations if the advisor has previously made remote work arrangements; however, other circumstances call for a different type of plans. After Hurricane Sandy hit in 2012, RIAs in and around Hartford, CT, and New York, NY, worked securely and without interruption at a local fast food restaurants offering free Wi-Fi. While setting up shop at the nearest McDonald's or Starbucks is not a long-term plan, it can be a stopgap solution for firms with their data securely stored and ready for retrieval.

A business continuity plan no longer just good business sense, it is now required for state-registered RIAs. To do it right, advisors should call on their technology service providers for input and expertise on how to make their firm function anytime, anywhere, under any circumstance. This will not only make the plan development process more palatable, but it will also give the advisor peace of mind knowing that client data and firm operations are protected in the event of an emergency.

Wes Stillman is the founder and president of RightSize Solutions www.rightsize-solutions.com, a provider of intelligent cloud technology and business management solutions for RIAs. He can be reached at wnstillman@rightsize-solutions.com.