Post Merger Tech Intergration Doesn’t Have to Be Painful

July 6, 2015

The pace of mergers and acquisitions proves that many of today’s RIAs believe there are competitive advantages to growth. For instance, working as a larger, single entity affords firms the opportunity to realize economies of scale in many areas, including technology. Technology-related expenses are one of the largest controllable operational expenses for every RIA, second only to staffing, so there are bottom line benefits to consolidating and getting the integration right.

Before tying the knot, merger-minded advisors would be wise to understand how to commingle disparate technologies without putting the client experience or firm data at risk. By focusing on and planning for the following consolidation issues early on, RIAs will mitigate disruption, address security and compliance issues and reduce expenses with fewer headaches sooner rather than later.

- Many platforms, multiple offices. Firm combinations involve bringing at least two — and typically four or more — different operations together, across multiple offices and remote work sites. It is not uncommon for merging firms to be on two different clouds, or to have end users with no desire to change tried-and-true core applications. Even if firms use the same programs, they may be using different versions, or there may be levels of customization that will not easily merge without at least one party undertaking an expensive upgrade prior to consolidation. Moving to cloud applications is an option that may solve some integration issues, but it may also require operational changes that set off a cascading series of policy and compliance issues.
- Data protection. Whenever there is a shift in organizational structure — due to mergers, lateral hires or turnover — the potential for data leakage becomes a serious concern. To avoid these growing pains, firms need control over who has access to data. RIAs also need to take steps that will lower their risk in the event of a potential cybersecurity breach. For example, a stolen laptop containing a spreadsheet with client Social Security numbers and account information becomes less of a risk when it is encrypted.
- Managing a larger staff. As assets under management grow, so too do staffs, particularly when multiple firms come together. According to the Cerulli report RIA Marketplace 2014: Growth Drivers in an Accelerating Industry Segment, RIAs with $500 million in assets employ approximately 17 people full time, on average. When two RIAs of this size combine, the risk controls and data security measures needed magnify beyond what was previously in place at either firm. For instance, staff turnover and onboarding can be a natural

consequence of many mergers, requiring that access to firm data and systems to be controlled accordingly. This can challenge the most senior technology person, particularly when they are also charged with supporting multiple systems that do not share data. As the complexity of access issues increases in conjunction with the size of the firm, many RIAs are best served by calling in outside experts for help in managing the transition.

- Proliferation of end user devices. There are many opinions about which mobile devices are best for particular needs, and it is not uncommon for firms to accommodate their end users' devices of choice. This approach can be a technology and security management nightmare for fast-growing firms, which may not fully appreciate the risks or how to mitigate them. Big RIAs are well-served by mandating a consistent BYOD (bring your own device) usage policy based on a unilateral compliance policy across the firm. For example, users who want to use their personal devices to access work emails must have them encrypted and password protected. This allows employees to use a variety of mobile devices to access the firm's platform, without regard to whether they are corporate or personal devices.

  Firms can take a huge step toward integration and reduce costs by using a centralized management platform that can support multiple applications, which will reduce technology and operational costs. This will allow all users to run off of a common email. The centralized platform can support multiple office systems, files and operations as well, without the costs of managing two or more platforms. By immediately centralizing user access, files and applications into one main environment, growing firms will address security concerns and avoid having to and support parallel platforms and can plan a more thoughtful transition for everyone to a single application.

Technology should not make or break a potential merger between firms, but integration, compliance and liability issues should certainly be part of the discussions to help avoid a post-merger hangover. Whether wealth managers have their sights set on the $1 billion asset mark, or are multi-office regional players intent on forming a multibillion-dollar national brand, typically RIAs will find common ground in some areas. Rapidly growing firms that can integrate even some portions of their technology early on to a centralized platform will see huge cost savings right away and can worry about merging disparate systems over time, when all sides are ready.