RIGHTSIZE
SOLUTIONS

Making Smart Technology Decisions

Six Steps for a Secure and Efficient IT Infrastructure

Whether you're starting a new Registered Investment Advisor (RIA) or looking to improve the way you manage technology at your existing firm, deciding how to manage technology can be one of the most important decisions you make. The good news is that technology choices now available to smaller independent models have not only caught up with but have surpassed those at larger institutions and offer greater flexibility to better serve consumers.

With greater technological capabilities comes greater responsibility. While technology has allowed smaller firms to offer online transfers, digital portals and other technological features once previously reserved for larger firms, it has also incurred a greater responsibility on smaller firms to protect their businesses and their clients' information. Regulatory boards that monitor the financial services industry are taking note and quickly shifting accountability to financial advisors. Not being proactive in this area is risking your firm's technology, client data and reputation.

In this whitepaper, we'll provide useful insight and best practices on some of the issues related to the technology component of an RIA, including:

- Evaluating short terms needs vs long term goals
- Establishing vendor and project timelines to stay on schedule
- Lining up the right resources to guide you through the process
- Developing policies and procedures that are practical and enforceable
- Preparing for the unexpected by getting it right the first time
- Planning for the 'What If?' scenarios that can and will occur

Introduction

Properly managing technology is essential to your firm's business health and keeping your clients' personal information safe. It can also help you to gain a competitive advantage and do better business. To better understand the growing importance technology plays you need only look at recent news headlines:

- Advisers plan to spend more for compliance and tech in 2017
  InvestmentNews, November 29, 2016

- Asset Managers Plan to Embrace Technology In 2017
  WeathManagement.com, November 15, 2016

- Most FAs Aren't Ready for Cybersecurity Attacks
  Financial Advisor IQ, September 20, 2016

- Is Technology a Cost or an Investment?
  Financial Planning, September 7, 2016

More than ever, Elite RIAs view technology as a critical component of their business. As noted, 57% of Elite RIAs now consider the effective use of technology as a key driver of success, up from 38% last year. Technology now stands alone as the top driver of success among top RIA firms, just ahead of client growth and retention (51%). They see it as central to improving workflows and productivity, as well as a way to manage client data more effectively and efficiently. In fact, 74% of Elite RIAs stated that technology is strengthening their effectiveness as financial advisers, allowing them to deliver even more customized services to their clients.

Source: InvestmentNews 2016 Elite RIA Study

#1 Decide on the right environment for your firm; decentralized or centralized

While there are many considerations that go into determining the appropriate technology solution, the number of employees and office locations will play an oversized role in determining where to invest. This will help you decide if you're better off with a decentralized or centralized environment. When it comes to managing your information technology, there are essentially two ends of a spectrum:

- Decentralized requires each function and application to be managed independently and directly with each vendors.
- Centralized enables all aspects of the firm's servers, computers and networks to be managed by a single service provider.

While a decentralized approach can be more cost efficient and adequate for a two to three-person firm where everyone has a trusted employee standpoint, it poses certain risks and extra effort for a larger firm. Centralized systems can help make supervision of both routine and complex tasks more streamlined. Managing new software installations, updates, user control, and security patches across the organization is much less painful from a centralized system.

62% of cyber-breach victims are small to mid-size businesses, which are at the greatest risk for an attack. Their level of preparation is low, and the costs of customer notification alone can be enough to do a small company irreparable financial harm.

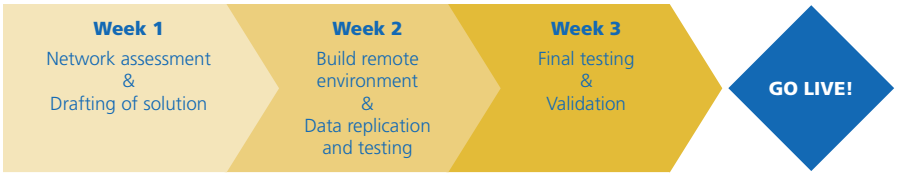
PropertyCaualty360; Small, mid-sized businesses hit by 62% of all cyber attacks, May 2016

#2 Understand vendor timelines; they can differ vastly from a start-up to established office

Timing is critical when building out your technology infrastructure. For example, if you are setting up a new office, versus an office that already has internet and networking, you should expect a lead-time of up to 60 to 90 days just to get internet circuits put in. Make sure you get timelines from all the vendors that you work with. You also may want to consider assigning a staff member or bring in an outside operation consultant to help you manage this process.

Instead of managing your infrastructure in-house, consider a cloud based solution. Not only is housing your own server complicated, expensive, and time-consuming, it can become a hindrance as your advisory practice grows. A cloud based solution provides a secure, scalable, and upgradeable cloud server that houses your entire business network and mission critical technology applications, while providing you access from anywhere.

Lastly, take the time to clearly understand how the implementation and migration process work. By moving your data files over a weekend will minimize disruption to your day to day operations. The final synchronization of your files should also be done during non-business hours.



Phases of what to expect in a typical implementation and migration process.

In the case of a merger, an early focus on and plan for consolidation issues such as integration of multiple systems and offices, ensuring data protection, training of staff, and managing end user devices is essential. When addressed properly, you will mitigate disruption, address security and compliance issues and reduce expenses with fewer headaches sooner rather than later.

> When building an RIA, each decision impacts the next—the custodian you choose will affect access to investments and technology integrations; the reporting provider you choose will be affected by which CRM best integrates with it; certain third-party trading systems work better with certain custodians and/or reporting systems, etc. You can't make these decisions linearly—you have to think of them in a 3-D matrix. This makes sticking to your proposed timeline/ deadlines so critical.
>
> Matt Sonnen, Founder and CEO, PFI Advisors

#3 Review all contracts and agreements carefully: a Service Licensing Agreement (SLA) may not be in your best interest

Financial Advisors benefit the most from spending more time client facing, not working through the complexities of managing IT infrastructure. Working with a partner that understands the industry and will help you towards success. When choosing the technology firms to assist you, one factor to consider is how willing and able they are to support you throughout the process; pre, during, and post launch. In the early stages, will the service provider be flexible on offering guidance and education without charging you or will they make you sign a Service Licensing Agreement (SLA) before starting? There will always be unforeseen situations that can delay your start date. A SLA may impact your bottom line by demanding you pay for services you may not need right away.

Your clients have entrusted you to manage their money and wealth. You should expect that same level of commitment from your technology partners. Conduct a thorough due diligence with each vendor to confirm they are keeping your information technology and data safe and secure. Make certain they take a proactive approach with layered protection and safeguards to shield communication and data. Built-in multifactor authentication and an encrypted connection can reduce potential risks and safeguard personal information across all devices and platforms. Real-time alerts are required in detecting vulnerabilites such as an Email containing a virus like Ransomeware or a link in a phishing Email. Immediate responses to issues will minimize your risk when the issues arise. If you're still not sure if the firms the right one for you, ask for a few client references.

> Choosing resource partners with deep knowledge and commitment to the RIA model drives the best outcome. The right providers can quickly link their functional specialty to other critical processes in the RIA. The outcome will be a powerful combination of partners that perform well in isolation, but are also additive to their counterparts.
>
> Brandon Kawal, Consultant, Advisor Growth Strategies

#4 Defining and adhering to clear policies and procedures are critical for technology ROI

Your policies and procedures may be the most important and complex phase of the process. This initial investment in time will save both money and headaches in the long run. For example, does the employee handbook establish a clear contingency plan for dealing with cybersecurity incidents? Make sure your plan has both preventative and reactive action items that are clearly communicated and understood by all employees. To ensure this, create actionable steps for dealing with employees, clients, partners, members of the press, and police & government. Think about all of the levels of security at your company. Clearly lay out who has access to what and control administrative privileges accordingly (both with internal staff and outsourced vendors). Limiting the ability to install drivers and execute applications can help control what gets onto your systems and prevent attacks like ransomware.

Recognize the impact of social media and create a policy specific to it. Not only does it distract employees, social media is a direct portal to cyberincidents. RIAs are prime targets for advanced phishing campaigns because much of their personal and business information is available online. Social Media should be monitored for both public and employee comments. Policies should restrict what employees can and/or should be saying on Social Media accounts. Lastly, be sure to include any company social media accounts in your archive process for auditing purposes.

#5 Define clear employee policies and procedure: social media is a direct portal to cyberincidents

Auditor examinations are a fact of life for both new and established RIAs. Whether it is a week, month or year down the road, you want to be prepared.

Based on The Office of Compliance Inspections and Examinations (OCIE) cybersecurity preparedness examination, the focus should include:

- How is your firm periodically evaluating cybersecurity risks and whether their controls and risk assessment processes are tailored to your business?
- How is your firm controlling access to various systems and data via management of user credentials, authentication, and authorization methods?
- How is your firm monitoring the volume of content transferred outside of the firm by its employees or through third parties, such as by email attachments or upload?
- How is your firm focusing on practices and controls related to vendor management, such as due diligence with regard to vendor selection, monitoring and oversight of vendors, and contract terms?
- How is your firm's training tailored to specific job functions and how is training designed to encourage responsible employee and vendor behavior?
- How does your firm establish policies, assign roles, assess system vulnerabilities, and develop plans to address possible future events?

While these may seem daunting at first glance, the better you plan to address these issues the more prepared you will be for an audit, and equally important, how you'll respond to an unforeseen incident.

#6 Conducting employee disaster recovery and continuity planning drills will drastically mitigate risk for when the "real thing" happens

Effectively managing your information technology is an ongoing process that requires constant participation at all levels of the firm. Invest in training to make sure employees realize the critical role they play and that they are equally capable of causing huge issues. Consider conducting a mock disaster recovery in order to test their knowledge of what they should be doing in such an event and how they would handle clients. Train them to recognize red flags such as emails that ask for personal or credit card information, requests for immediate action regarding unfamiliar situations, or emails that include suspicious attachments. Include employees in the process and preach the culture of security. Managers are not exempt. Make sure they are included in awareness training. Managers have more responsibility for company information and administrative privileges, which makes them more vulnerable.

Lead by example; regularly discuss your firm's technology in staff meetings and with other internal communication. Employees need to be empowered with knowledge and a shared commitment that goes far beyond the annual 'check the box' that you have read and understand the company IT policies. If an incident does occur, let your employees know about it. Not only will it help deter the impact of the incident, it will help your employees develop a team approach. When employees alert management to mistakes early in the process, they are giving management the opportunity to prevent huge losses of time, data, and money. Specific ways that you can educate employees are by conducting mock cybersecurity drills, scheduling periodic 'test' phishing emails or phone calls. Discussions regarding recent and specific documented cases should be had in staff meetings. Question employees directly on how they would individually handle such situations.

Many firms develop a plan or ideas to add value to their current business model, and then think about technology later in the process. Define upfront how technology should be used to support your ideas. This enables you to see how several areas can benefit from the same technology, find conflicts that need resolving, and better assess which areas need immediate attention.

Sue Glover, President,
Susan Glover & Associates

For this paper we partnered with a few industry experts who contributed their thoughts on the subject. Learn more about them here:

- **PFI Advisors:** http://pfiadvisors.com/
- **Advisor Growth Strategies:** http://advisorgrowthllc.com/
- **Susan Glover and Associates:** http://susangloverassociates.com/

The Takeaways

Apply these 6 steps for making smart technology decisions that ensure a secure and efficient technology environment:

1. **Plan ahead:** Evaluate and identifying the needs and goals will help you to determine the proper environment, such as decentralized or centralized, which it turn will have determine how efficient and productive your technology is.
2. **Set deadlines:** Acquire timelines when building out your technology infrastructure. Get it in writing and hold vendors accountable while at the same time be an active partner is the process by being responsive to requests and information that they require.
3. **Choose wisely:** Conduct a thorough due diligence of the vendors who safeguard your information technology. Work with service providers who are willing to make the investment in time are dedicated to your specific needs and goals. And, always ask for client references that you can interview for their experience.
4. **Be flexible:** Getting locked into a long term Service Licensing Agreement (SLA) may impact your bottom line by demanding you to pay for services you may not need right away. Protect yourself by understanding all aspects of a contract before you sign on the dotted line.
5. **Engage employees:** Technology is only as good as the people using it. Your policies and procedures must be clear and accountable at every level of your firm. By empowering employees to understand their role and responsibility in the process you can often times significant reduce the damage that occurs from an incident.
6. **Stay proactive:** Firms that have the strongest infrastructures are those who continue to stay current and use best practices and technology. Regular review and updates to your policies and procedures will ensure you're prepared for when an auditor knocks on your door, and equally important, how you'll respond to an unforeseen incident.

Conclusion

Your ability to manage your clients' money relies heavily on technology—more so than other businesses. Privacy, security and compliance are essential. Determining the right solution, partnering with the right vendors, and establishing effective policies and procedures are all critical components to building a successful and sustainable infrastructure. While this whitepaper may not address every issue you will face along the way, and there will be many, we hope it will provide better awareness into making the right technology decisions to meet the exact needs of your new RIA firm.

11011 King Street, Suite 280
Overland Park, KS 66210

(913) 396-4600

info@rightsize-solutions.com

RIGHTSIZE SOLUTIONS