
MorningstarAdvisor

When Disaster Strikes

by Bill Winterberg | 09-09-10

In May of this year, Rick Kahler, CFP, president and founder of Kahler Financial Group in Rapid City, S.D., experienced an interruption to his business that every advisor fears. His primary server for nearly all of the firm's services failed, taking out all server-based programs and applications, e-mail, and Internet access. The phone system and the photocopier were the only functional pieces of equipment in the firm for four days.

Through daily updates to Kahler's blog, [Financial Awakenings](#), he chronicled the firm's progress to restore business operations to normal, a process that took nearly 10 days. At the time of the failure, Kahler Financial Group was already testing a migration of its local server to a virtual server supported by an outside IT provider and noted the irony on his blog, writing, "One of the main reasons for going to a virtual server is to prevent what has just happened to us from happening!"

Business-Continuity-Plan Elements

September marks National Preparedness Month supported by the [Federal Emergency Management Agency](#), which makes disaster preparedness resources available at the [Ready.gov](#) website. The [Ready Business](#) page highlights the following three steps in planning for business continuity and crisis management in the event of a disaster:

- * Plan to Stay In Business
- * Talk to Your People
- * Protect Your Investment

Catastrophic system failures, such as Kahler Financial Group's server crash, and disasters, either man-made or natural, present real risks to the business continuity of wealth-management practices. At a minimum, the SEC requires that all registered investment advisors address business-continuity plans in their written policies and procedures. FINRA rules require member firms to maintain a written business-continuity plan and to conduct an assessment of the plan at least annually.

While regulations don't provide specific elements that need to be included in a business-continuity plan, they do require that plans account for the timely resumption of critical hardware and software systems, backup and recovery of electronic and paper-based information, and alternate arrangements to contact employees and clients of the firm.

Christopher Winn, Managing Principal of Advisor Assist, a Marshfield, Mass.-based compliance consulting firm, advises clients to avoid using template plans sold by third parties that contain boilerplate language. Such plans, he says, are an open invitation for negative comments or even deficiency notices from regulators.

Instead, Winn recommends that advisors think through all of the processes and technology required to run the business in the event of a disruption. He poses the following questions to assess the adequacy of a business continuity plan:

- * Do advisors need to sit in the primary office and be present in order to work, or has the firm embraced Internet-based cloud services that can be accessed from anywhere?
- * What happens when the firm's hardware systems are inaccessible? How is client data accessed if a server is offline? How is security trading conducted? How are phone calls from clients answered if the phone system is down?
- * How is the privacy and security of client data addressed when operating from an alternate location?

Winn also suggests that firms separate continuity plans into two functional sections. The most important section is what he calls "day one" functions, which include all processes that must be restored no later than the end of the first day of a business interruption. According to Winn, day one functions include restoring essential hardware and software systems, executing securities trading and

journal requests, and establishing communication with clients and employees.

The other plan section is "day 10" functions, which Winn defines as "important and necessary functions that must be performed regularly, but if not performed for several days during a business interruption, will not have a significant effect on the organization." He includes accounts-payable and accounts-receivable activities and the creation of management or ad hoc reports in day 10 functions.

"There isn't one right way to structure business-continuity plans," Winn adds, "but the collective policies of access to records, data security, and proper retention practices need to work in any business-disruption scenario."

Adopt Cloud Computing

At the center of nearly all advisory firms' technology infrastructure is a server. But in the wake of a natural disaster or hardware failure, access to the company server and all the data stored on it may be impossible, just as in Kahler Financial Group's case.

Instead of storing programs and data on a local server, advisors are increasingly adopting cloud and software-as-a-service applications for programs critical to business operations. SaaS applications are deployed exclusively over the Internet rather than requiring installation on a local computer or server. Such applications improve a firm's business continuity by removing dependence on a local server and providing access to essential business services from any location with an Internet connection.

But despite the growth and popularity of SaaS offerings, advisors are often unable to find suitable applications that meet their specific needs for CRM, portfolio management, or electronic document management functionality. For some firms, SaaS applications simply don't offer the equivalent performance or ease of use compared with their server-based counterparts. So what should advisors do if they are compelled to maintain a local server for just such a purpose?

Avoid Server Interruptions

To identify best business continuity practices when maintaining a local server, I spoke with Steven Ryder, president of True North Networks, a Keene, N.H.-based IT infrastructure provider to the finance and banking industry. He recommends the first thing advisors do is use imaging software on their local server.

Popular imaging software includes ShadowProtect from StorageCraft Technology Corporation, Acronis True Image from Acronis, Inc., Ghost from Symantec Corporation, and vSphere from VMware, Inc. Ryder estimates advisors that should spend about \$1,000 for suitable imaging software and support from the vendor.

"Backing up data on its own is useless," Ryder says. "You need to back up the entire image of the server for proper business continuity. Imaging allows you to recover the entire server intact without reinstalling programs one-by-one from CD-ROMs or tracking down software license keys."

Imaging software works by taking a snapshot of the entire contents and structure of a server and saving it to one large file. When the primary server fails, the image file can be loaded onto another hardware device and then used to restore all of the programs, application data, and files that existed on the original server. Ryder says that several years ago, image files had to be loaded onto a server with the identical hardware configuration as the failed server in order for the restore to succeed. But today, image files can be used for recovery on completely different physical hardware or even a virtual server operating in a virtual environment.

One caveat of using imaging software, according to Ryder, is that a backup server must be available to step in when the primary server fails. With the flexibility to use a server with any hardware configuration, Ryder recommends purchasing a discounted server from one of the large server retail outlets such as Dell or IBM. Advisors should expect to spend around \$2,000 to \$3,000 for a properly-equipped device. Ryder also says that advisors who receive support from an external IT provider should check to see if their engagement includes access to spare servers in the event one is needed.

Lastly, Ryder insists the image file should never be saved anywhere on the primary server. Rather, he recommends image files be saved to an external storage device, such as an external USB hard drive,

and stored offsite in a secure location.

Hosted Virtual Servers

For advisors interested in the benefits of a local server without having to manage imaging software or a server restoration, Ryder suggests the adoption of a hosted virtual server. All essential software programs and files are accessed from a virtual server as if they were in an advisor's local office, but the physical hardware is managed by a third party vendor in a separate, secure location.

Most of the installations performed by True North Networks in 2010 have been virtual servers. "A virtual server has the potential to save advisors a fortune in hardware, power, and licensing costs," Ryder says. Advisors using virtual servers do not need to purchase any hardware of their own. Instead, hosting providers like True North Networks use virtualization software from VMware, Microsoft, or Citrix to configure as many virtual servers as needed using one piece of hardware.

"If a client wants to add two or three more servers to their environment," Ryder continues, "We can configure and boot up those new instances within hours with no additional hardware cost."

Fees for hosted virtual servers can vary significantly depending on the size, speed, and software requirements needed to support an advisor's business. Ryder estimates that the cost for a typical single-server installation for a midsize financial advisory practice with five or more employees is \$200 per month per user. "The cost estimate is not just for hardware alone," he says. "It also includes all of the licenses for the operating system, Microsoft Office software, virus protection, backup software, and all IT support costs to keep the server online and up to date."

Abundant Continuity Options

Rarely is there an ideal time for advisors to stop running their businesses and perform a comprehensive test of the firm's business-continuity plan. But in observance of National Preparedness Month, advisors should re-examine their plans in light of new, cost-effective technologies available for their business infrastructure.

Local servers can be restored quickly via imaging software, critical business applications can be transferred to cloud services, or the entire server hardware and software complex can be hosted off-site in a virtual environment. Implementing these measures as a part of a comprehensive business continuity plan should please even the most critical of regulatory examiners while ensuring the business can operate with little disruption when a future disaster strikes.

Get practice-building tips and information from our team of experts delivered to your e-mail inbox every Thursday. [Sign up for our free Practice Builder e-newsletter.](#)

Bill Winterberg, CFP, is a technology and operations consultant to independent financial advisors. His comments on technology have been featured in a variety of financial industry publications. You can view more information about Bill and see his schedule of upcoming speaking engagements at his Web site, FPPad.com.

Reader Comments (1)

September 15, 2010 10:48 am

Bill, great column... Having been through disasters (hurricanes) before that have impacted the way your business operates, its very important to have a plan in place. For example, I always figured that having a land (phone) line as a backup in the event of a disaster would be paramount. However, when Hurricane Wilma struck South Florida a few years back the landlines were out within 8 hours of the storm--it was the cell phones that became the primary method of communication--until you run out of charge, and then it was utilize the car charger if you had one or piggyback off a generator!

- Mike, Dallas

