JUNE 2015 | US$25

FINANCIAL SERVICES: 9 STEPS TO CONTINUITY SUCCESS

Partner Marketing
CHANNEL PARTNERS

Table of Contents

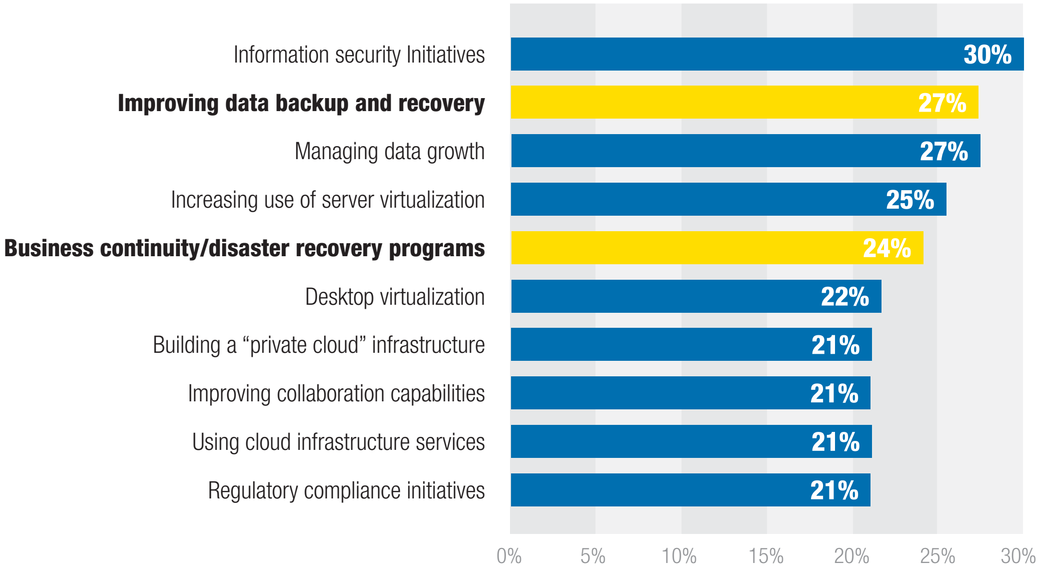
FINANCIAL SERVICES: 9 STEPS TO CONTINUITY SUCCESS

IT'S NO SECRET THAT FINANCIAL SERVICES CUSTOMERS EXPECT ANYWHERE, ANYTIME ACCESS — REGARDLESS OF WHETHER A MAJOR STORM IMPERILS YOUR DATA CENTER OR A BROKEN WATER MAIN PREVENTS YOUR EMPLOYEES FROM getting to work. If delivering on those expectations means taking a fresh look at the "recovery" side of your disaster recovery and business continuity strategy, you're not alone. According to the most recent IT Spending Intentions Survey by the Enterprise Strategy Group (ESG), two of the top five 2015 priorities at middle-market firms involve boosting IT resiliency.

Fortunately, the technologies and tools to help fine-tune recovery strategies have never been more robust or affordable.

Top Ten IT Priorities in 2015 for Midsized Organizations

Top 10 most important IT priorities for midmarket organizations (100 to 99 employees) over the next 12 months. (Percent of respondents, N=233, 10 responses accepted)



Source: The Enterprise Strategy Group Inc.

“It’s an exciting time for durable IT in the financial sector,” says Jason Buffington, senior analyst with ESG. “Enterprise-grade technologies are less complex and more cost-effective, so midsized orgs can finally have the BC/DR that they’ve long wanted but didn’t think attainable.”

However, simply throwing technology at any given challenge has frequently proven foolish. That’s why we’ll discuss nine steps financial services firms, with help from their IT advisers, can take to develop a successful recovery strategy. Along the way, we’ll also spotlight a firm that’s taken an innovative approach.

STEP 1: START YOUR INTERNAL CONTINUITY ASSESSMENTS NOW

Aside from Wall Street traders, where uptime is a firm’s lifeblood, industry insiders say financial services continuity strategies currently range from highly available active-active architectures to still absent from the starting gate.

“For example, in the insurance space we see the entire spectrum among middle-market companies,” says Mike Holmes, a former insurance CIO who is now an IT consultant with Sirius Computer Solutions working with clients in all financial services verticals.

While the industry’s relative continuity immaturity may seem like good news for laggards, experts stress the vulnerability inherent in remaining behind the curve.

“For most small and mid-sized financial services firms, there’s another company down the street that will happily take your business if you are unable to provide a typical customer experience for an extended period,” Buffington says.

In other words, no matter where your firm falls on the continuity spectrum, the time to begin improving is now.

STEP 2: CREATE A DISASTER PROBABILITY MATRIX

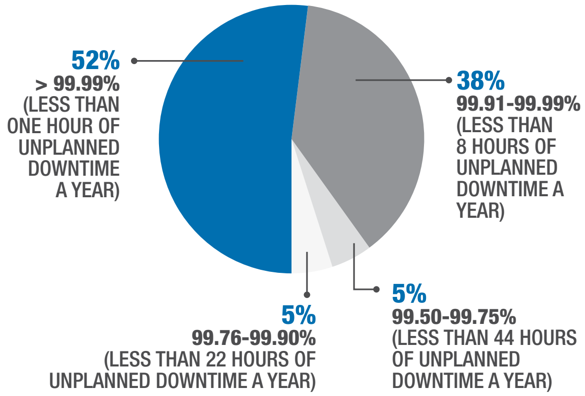
Once you understand where you are, consider creating a disaster probability matrix, as suggested by Sid Herron, director of channel sales for cloud continuity provider VirtualQube. Begin with a physical or digital sheet of paper containing three columns:

- **Column 1:** List every possible DR scenario, from a cascading virtual server outage to a severed fiber-optic line to a multimonth catastrophe.
- **Column 2:** Using a simple 1 to 3 scale, rate each event’s likelihood.
- **Column 3:** On a scale of 1 to 3, rate the impact on your business.

Naturally, events rating a “1” in both the second and third column deserve immediate attention. Conversely, events receiving a “3” in both columns may not be worth the price to address. “For items with mixed results, you’ll need to conduct a further cost/benefit analysis to determine which scenarios make sense to remediate,” Herron says.

Always On

Financial services firms have lofty availability goals for mission-critical systems



Source: Continuity Software, 2014 Service Availability Benchmark Survey

STEP 3: DETERMINE YOUR RTO AND RPO

Next, determine your firm's unique recovery-time objective (RTO) and recovery-point objective (RPO) targets, which will shape every component of your continuity strategy. The catch: The lower the RTO/RPO, the greater the cost and complexity.

As continuity analyst Marc Staimer points out, most firms must balance RTO/RPO and cost. "If you're a Wall Street trader, you may need nanosecond RTO and every transaction RPO," says Staimer, the founder and president of Dragon Slayer Consulting. "But, most firms can tolerate much less, depending upon the individual application."

Granularly determining RTO/RPO for each application in your IT stack is the key. "From an operational and compliance perspective, financial services systems involved with moving money are completely critical," says Buffington. Everything else, including email, should be prioritized appropriately.

STEP 4: DIFFERENTIATE BETWEEN REPLICATION AND RECOVERABILITY

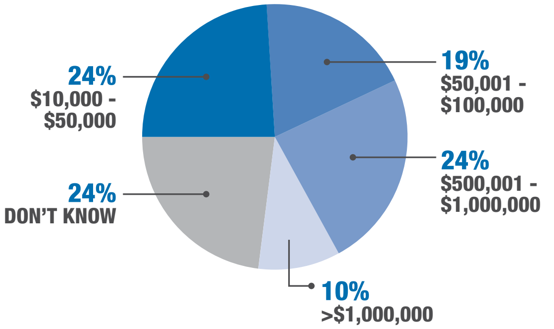
Too often, small and middle-market firms confuse the ability to replicate information to an off-site location with the ability to recover it rapidly enough that customers don't notice a blip. In reality, replication occurs at a trickle over time, while recovery from a crisis must happen fast.

"Even with WAN optimization, bringing terabytes of replicated data back from your distant DR site — whether it's in the cloud or at a physical location — can take many weeks," says Scott Gorcester, CEO at VirtualQube. "In fact, we asked one of the world's best-known DR brand names about the time frame for streaming a single terabyte of data back from the cloud." The response? "They said five months." No wonder companies still regularly ship encrypted hard drives via FedEx.

In short, replication ensures the survival of your data and systems. Recovery requires various technologies, which will be determined by your RTO/RTO.

Downtime Adds Up

For financial services firms, the cost of an hour of downtime varies. This is one metric where "I don't know" is not a good response.



Totals may not equal 100% due to rounding.
Source: Continuity Software, 2014 Service Availability Benchmark Survey

STEP 5: TAKE AN END-TO-END APPROACH

Any modern continuity strategy includes securely linking people, applications and data, from end to end. At the connectivity layer, this frequently means WANs or VPNs. When choosing, ensure you take connection speed into consideration. "While secure, VPNs can be slow," Staimer acknowledges.

On the desktop, VDI can be a cost-effective means to address both continuity and operational objectives. Just don't expect one size to fit all, as financial services VDI often requires multiple desktop patterns based on business units or employee roles. "For example, claims employees frequently need applications that can run offline," says Holmes.

Another desktop consideration is collaboration. As Holmes points out, displaced employees may need to interact effectively for weeks or months before their regular worksites are restored. “Too often, the criticality of collaboration gets completely overlooked,” he says. Electronic collaboration tools, such as such as Cisco’s Jabber or Microsoft Lync, offer integrated solutions to connect employees by voice, instant messaging and Web conferencing.

Still, for some job categories, collaboration tools and VDI won’t fill the bill. For this reason, many organizations take a hybrid approach to temporary workspaces. Consider establishing one, or more, employee sites — either internally within branch locations or externally via rented space — as well as enabling employees to work from home offices.

STEP 6: ADDRESS LEGACY SYSTEM CHALLENGES

If your firm’s greatest continuity obstacle is one or more inflexible legacy core systems, you’re in good company. The workaround: masking recovery weaknesses with the help of an IT adviser who understands your specific requirements. For example, the answer might be to establish an operational data repository that mirrors production systems. “Then, the mirror can be used for inquiry purposes to help meet customer experience expectations,” says Holmes. Another option is providing customers with an online interface that gives immediate feedback but delays data processing until core systems are available. An example is supplying a payment confirmation even though the transaction is awaiting execution.

STEP 7: BUILD COST-EFFECTIVENESS INTO YOUR STRATEGY

Rather than investing in — and then spending to maintain — a single-purpose DR site, consider designing continuity systems to serve multiple functions, thereby creating operational and cost efficiencies. According to Holmes, the most common design technique uses a distant continuity site to double as the primary development and testing center. “Rather than simply establishing a traditional lights-out DR data center, ask yourself what other ways you can use your continuity assets,” he says.

Measure, Then Manage

How frequently financial services companies measure progress toward replication, failover, and RPO and RTO goals.

	REPLICATION SUCCESS	VIRTUALIZATION SUCCESS	LOAD BALANCING SUCCESS	STORAGE FAILOVER SUCCESS	RTO OBJECTIVES MET	RPO OBJECTIVES MET
Real-Time	43%	37%	32%	29%	18%	32%
Daily	25%	15%	14%	29%	11%	14%
Weekly	7%	15%	18%	0%	11%	18%
Monthly	7%	15%	4%	11%	7%	4%
Quarterly	7%	11%	14%	11%	25%	14%
Annually	0%	0%	4%	4%	14%	4%
Never	11%	7%	14%	18%	14%	14%

Totals may not equal 100% due to rounding.
Source: Continuity Software 2015 IT Operations Analytics Survey, 27 financial services respondents

STEP 8: EVALUATE DRAAS

Like all cloud technologies, disaster-recovery-as-a-service (DRaaS) is gaining ground among financial services firms. Still, analysts, technology partners and financial services CIOs are divided on whether the time is right for adoption.

Buffington is bullish on DRaaS as an option for midsized firms that would otherwise shrug their shoulders with the presumption that traditional methods were unattainable due to cost/complexity. As long as the provider can meet regulatory requirements, it's a better bet than crossing your fingers and hoping for the best.

Staimer is more cautious, warning firms to thoroughly investigate and differentiate between vendors that treat DRaaS as data recovery versus those offering true "recovery-as-a-service." The former can mount and run a series of virtual machines that enable financial services firms to recover files or even run applications. "But, they are not set up to actually run their clients' data centers as they tend to lack assets, personnel and robust DR experience," he says. "In addition, they are often unprepared to recover large numbers of clients simultaneously."

Woodforest National Bank CTO Richard Ferrara falls somewhere in between. Although his organization has charted a different course (see the sidebar, "Honing Its Strategy: Woodforest National Bank."), Ferrara says it's a question that must be weighed for each office, or even individual applications. "If your firm is comfortable with running applications in the cloud, and is in compliance, then DRaaS can be a viable option," he says.

Honing Its Strategy: Woodforest National Bank

After Hurricane Ike took aim at Houston in 2008, Woodforest National Bank made a gutsy move. CTO Richard Ferrara developed a twice-yearly distant migration strategy as the centerpiece of the firm's continuity plan — and then did the ultimate real-world test. "In June 2011, we completely failed over to our colocation near the beginning of hurricane season," Ferrara says. "We operated from our distant site until hurricane season ended in mid-October."

The bank, which is based in The Woodlands, Texas, was an early adopter of virtualization technologies. However, Ferrara initially found migration automation tools lacking. Although this meant the biannual migrations required a weekend to complete, Ferrara's team ensured the customer impact was under an hour. In addition, Woodforest developed an employee continuity plan, with units designated to travel to a specific alternate site should their locations be damaged. Plus, all locations were connected to both the primary and the distant site via WAN links, to ensure consistent computing performance.

Still, biannual migrations are no small trick for an institution with more than 750 locations spread across 17 states and a commitment to providing 24/7 access to live representatives, so Woodforest continued to hone its strategy. Migrations were reduced from a weekend to overnight.

Then, in late 2013, Ferrara's team deployed a new hypervisor-enabled replication appliance and immediately reduced the migration window to several hours. Correspondingly, individual systems were unavailable for 15 minutes or less.

Today, Woodforest has added back-office VDI, can administer the primary and secondary sites remotely and has adopted a six-month rotation — migrating to the distant site in July and back in January — which also supplies an effective refresh and maintenance window. Additionally, the institution performs regular exercises to ensure any-event durability.

"We started with a SAN-to-SAN model, moved to an appliance-based model and, currently, we're evolving to software-enabled hypervisor replication," says Ferrara. "The Holy Grail for us is running live-live, but our core banking systems aren't quite there — yet."

STEP 9: TEST, TEST, TEST

Last, but by far not least, if compliance mandates form the basis of your firm's testing blueprint, your company is at risk. Simply put, current regulations specify only bare minimums, and often lead to inadequate spot testing. "Unless you've completely failed over and run your company from your DR site for a reasonable period, you don't know that you can," Herron says.

Indeed, views from the trenches reveal the depth of the testing problem. In banking, Ferrara says, few of his peers have ever attempted a systemic recoverability test, let alone regularly run the system through its paces. And it's much the same for insurance, where Holmes "sees every imaginable approach, including firms that don't test at all."

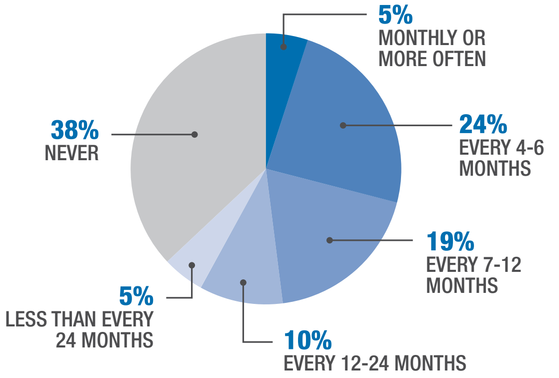
What's more, Holmes frequently witnesses testing that resembles a hyper-controlled laboratory experiment rather than a simulated crisis. "What tornado," he asks, "is going to contact you in well enough in advance to let you know it's time to execute your continuity strategy in an orderly fashion?"

In addition to performing complete recovery drills, consider investigating new types of continuity analysis tools to assist with uncovering potential weaknesses in advance. Such technologies enable IT and partners to predict the outcome of any systems change, whether it's an OS patch or an application update. This, in turn, allows IT staff to make adjustments that improve operational resiliency as well as help with meeting or exceeding continuity goals.

According to recent surveys by Continuity Software, about half of large companies already use such tools, with midsize firms catching up quickly. As costs have dropped and simplicity improved, Continuity's director of marketing Roy Goffer anticipates smaller-firm adoption rates to continue climbing.

Risky Business

How frequently financial services firms test availability of their private clouds. No. 1 answer? Never



Total does not equal 100% due to rounding.
Source: Continuity Software, 2014 Service Availability Benchmark Survey

Regardless of the tools your firm uses or the type of DR site you choose, Buffington sums up the imperatives succinctly. "No one is as vested in your IT resiliency as you are," he says. "So, no matter how good the partner, self-testing your IT durability must be part of your resiliency plan."

If your firm isn't already on an IT durability modernization journey, staying competitive requires getting started now. As you do, remember there's no one right way to proceed. "In fact," says Holmes, "some large, deep-pocketed companies have strategies that are much less robust than some smaller firms have in place." The mistake is to think disaster won't strike, and if it did, that your recovery strategy will go off without a hitch when you've never tested it.