TOP 7 Best Practices for Business Continuity

Business continuity undoubtedly is at or near the very top of every IT organization's list of strategic initiatives, considering the dramatic costs and implications of downtime. Here are some best practices organizations should keep in mind when designing and implementing a business continuity strategy.

Nearly every organization needs to ensure seamless and reliable business continuity in the event of an unplanned outage. The economic, legal and reputational risks of failing to do so are far too frightening to imagine. Forrester Research, for instance, points out that the average cost per hour of service disruption is $110,000, and a typical business interruption event costs more than $1.5 million.

Of course, when safeguarding applications, data and business services against a wide range of threats, there are pragmatic issues for IT organizations to consider, including budget limitations, staff resource constraints, business stakeholders' hesitancy to change how they work and many others. But the looming threats of malicious cyber attacks, natural disasters and simple user errors mean that organizations must be more vigilant than ever in making their infrastructure, applications and essential data more resilient and always available.

The good news is that most midsize and enterprise-class organizations at least have a business continuity plan in place in the event of a disaster or threat. AT&T's 2012 Business Continuity Study found that 86% of companies with annual revenues exceeding $25 million have a business continuity plan in place — an increase of 8% over the past five years. But having a plan is simply the first step. Here are some best practices to consider when designing and implementing your own business continuity plan.

TechTarget Custom Media

Symantec

1. Automate every aspect of your BC plan.

It's amazing to think that many organizations still rely upon manual, human-centric processes to recover from outages and restore access to data and applications. The epic Hurricane Sandy storm of 2012 brought home the importance of automated failover and recovery processes, even for organizations that had planned for recovery at remote data centers. In many cases, their business continuity strategy relied upon individuals getting to remote facilities to begin the failover and recovery steps, but many of those data center employees were stranded at home with their own power outages, were unable to access public transportation, navigate blocked roads due to downed trees or couldn't drive their own vehicles because of scarce gasoline supplies. Failover, recovery and restore steps need to be automated.

2. Don't assume that your virtualized infrastructure enjoys full protection from service interruptions.

As important and pervasive as virtualization has become for organizations, a business continuity plan must address the reality of a mixed virtual and physical infrastructure in a cohesive, synergistic approach. While having virtual servers, storage and desktops does help reduce your service interruption exposure, virtual machines do fail. One of the key steps you should consider is ensuring you have a backup strategy for virtual machines, especially if you've increased your use of virtualization for mission-critical applications. A recent study from Symantec found that two-thirds of respondents had not yet deployed a backup solution for their virtual servers. Virtualization is an important part of today's IT architecture planning, but in and of itself, the technology doesn't mitigate the need for end-to-end business continuity planning across virtual and physical infrastructure. For instance, that same study noted that most IT organizations wouldn't immediately know if an application running on a service-interrupted virtual machine was unavailable. Also, be sure to consider application availability tools that tightly integrate with leading virtualization hypervisors like VMware vSphere. Solutions such as Symantec's Veritas Cluster Server are purpose-built for application availability in virtual environments, which is increasingly important as organizations move their more demanding workloads to virtual machines.

3. Planning for business continuity is important, but not nearly as important as testing.

Business continuity testing is a sensitive subject for many IT executives. While few would debate its importance, far from all IT organizations actually take the time to regularly test their plans. Additional research from Symantec indicates that 22% of companies never test their business continuity plan, or do so only after an emergency takes place. Another 22% say they only test once a year. And while frequency of testing is important, it may be even more important to test the full software stack to ensure that you can actually immediately enable availability of mission-critical applications. Don't stop at testing core software components such as the database, operating system or virtualization hypervisor. If essential applications don't immediately and reliably fail over to backup servers, you won't be able to do critical work and the meter will start running on your economic losses.

4. Consider your strategy for data center location.

Lots of companies have more than one data center. In fact, the 2012/2013 IT Spending and Staffing Benchmarks report from Computer Economics says about 60% of North American companies with more than $50 million in revenue have more than one data center. For those companies, it's important to establish a reasonable distance between production and recovery sites in order to steer clear of regional problems such as the 2004 power outage that darkened about 25% of the entire U.S. for several days. But what about the approximately 40% of midsize and large companies that have only a single data center? Prudent planning for business continuity is driving many of those companies to consider partnerships with cloud service providers or managed storage service providers in order to have a secure, reliable failover option. Again, while it's natural to first consider recovery partners in close proximity to your primary data center, you should also think about the option of backing up your data and applications at a partner's remote facility.

5. Prioritize your business continuity functions to avoid overspending.

Depending upon your organization's size, IT complexity and industry, deploying a business continuity solution is far from a trivial expense. So it's important to do an in-depth analysis of your core business processes to prioritize which applications need to be available immediately, which ones can be offline for a few hours, and which ones can wait even

a day or so. For instance, your marketing automation application that includes email list management and production of the company newsletter probably can be restored from secondary tape storage systems well after you've immediately restored your customer-facing applications like customer service and e-commerce. Also, think about recovery point and recovery time objectives for each application. Order entry, fulfillment and compliance-centric applications can't afford to miss a beat, and even a single lost record in the recovery process can have serious implications.

6. Think of disaster recovery and business continuity as a managed service.

Software, infrastructure, security, platforms, customer support — all of these managed services are important elements of any CIO's portfolio. IT leaders select managed service providers that have proven experience and know-how in each area. The same should be true with picking a partner for business continuity and disaster recovery. While it's true that almost any IT services partner will claim it can help you recover from a service interruption, there's a big difference between a partner offering remote backup storage and one that has the essential combination of hardened infrastructure, disaster recovery tools for backup, archiving and restore, multiplatform storage management and proven expertise in failover to any of multiple recovery sites.

7. Be sure to integrate mobility as a core element in your business continuity plan.

There's no doubt that BYOD is more than a buzzword — the bring-your-own-device trend is changing the way all organizations work, and it's changing the way organizations think about business continuity. At one level, pervasive mobility means employees, contractors, vendors and customers all can continue to do business even though a facility has lots its power. But more important, shifts toward virtual workforces, mobile-first applications and IT consumerization mean that business continuity planning must account for new types of devices and business processes that allow people to do business as long as they can find sufficient power and a reliable Internet connection.

TOP 7 Best Practices for Business Continuity

Summary

For many years, organizations thought about business continuity in much the same way they thought about business insurance — yes, it was important, but rarely was it top of mind. But that's all changed. Many organizations have, unfortunately, discovered that even a scant few minutes of service downtime can have deleterious effects on their business operations, resulting in lost revenue, diminished customer confidence and heightened compliance risk.

For those and other reasons, IT executives have raised the bar on business continuity preparedness for their organizations in all ways. New technologies, business processes and partnerships, combined with a raised level of importance for testing and a full appreciation of what virtualization can and can't do for business continuity, are essential to new thinking around avoiding the impact of an unplanned service interruption.

TechTarget® Custom Media

Symantec™