SPECIAL REPORT :: OCTOBER 2012

NetworkWorld

THE CONNECTED ENTERPRISE

INSIDER

➔ Outages

HOW IS YOUR DISASTER PLAN?

Hurricane Sandy latest test by Mother Nature

INSIDE

Dealing with outages -- are we ready?

BY RANDY CLARK, CMO OF UC4 SOFTWARE, SPECIAL TO NETWORK WORLD

This vendor-written opinion has been edited by Network World to eliminate product promotion, but readers should note it will likely favor the submitter's approach.

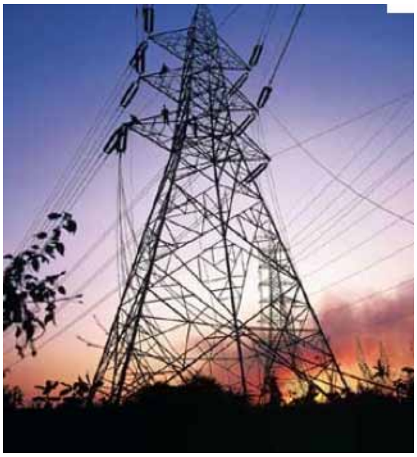
The powerful storms that recently hit the mid-Atlantic region caused electrical outages that in turn disrupted Amazon's EC2 services. The impact to the consumers and businesses that depend on the Amazon cloud have been well chronicled.

Amazon is a leader in reliability and, if it happens to them, it can and will happen to any service provider. The point is that in order to maintain business continuity, enterprises need to take responsibility for planning their outage contingencies.

The problem is that business processes, applications and computing infrastructure are too intertwined and dependent on each other. If the infrastructure isn't configured just right or is unavailable, the business process stops. The industry has made great strides in abstracting the physical computing infrastructure from the applications it supports. Amazon and VMware have created tremendous value and built businesses by abstracting (or insulating) applications and users from hardware diversity and failures.

However, the industry has only started to abstract the business process from the applications and infrastructure that supports it. To work around an Amazon EC2 outage, organizations really need to utilize more than one provider to avoid a single point of failure. Yet in order for the business to be successful at this there needs to be the ability to reroute and rerun the process in their own data center or an alternative service provider. This is where higher-level process automation comes in.

The recent outages at Royal Bank of Scotland, BATS Global Markets and others demonstrate the inability not only to abstract the process from the infrastructure but to see the interdependencies and the failures that plague complex IT systems as well. In those particular outages, it took minutes to fix the problem but days to find it.



Process automation that keeps track of the complex interdependencies between applications, infrastructure and business workflows can help identify, or even predict problems. Then in the case of an unavoidable outage, the business workflows would be rerouted to an available data center.

Most process automation done today is low level IT administrative tasks for provisioning servers, handling backup or startup routines, and generally doing infrastructure tasks that require little decision making that could affect the line of business. This is necessary and important, but not sufficient to preserve the user experience or business process integrity in the face of increasingly complex IT environments where, statistically, something is always failing.

Enterprises must step up their IT process automation to the point that they can manage business workflows not just servers or IT tasks.

If the businesses dependent on Amazon had these capabilities, they would drastically reduce the outages they experienced. Orchestrating business workflows and associated data across applications and infrastructure is easier said than done. However, it can, and is, being done by many enterprises to assure service levels.

Being able to "roll-back" failed system updates to previous working versions, spotting process failures before they create an unrecoverable backlog, and the ability to run a workflow on newly provisioned environments is the type of higher-level process automation that abstracts inevitable outages from the user or business experience.

As enterprises get more serious about higher-level process automation, they will spend more time abstracting their processes from specific infrastructures and application environments. This abstraction is not only key to quickly managing an outage, it's also key to efficiently dealing with the growing IT complexity created by today's hyper-competitive business environment.

Whether IT is ready or not, the business is doing whatever it takes to respond to changing market and customer demands by pushing IT to develop new applications at a faster pace and deploy them quickly (on highly virtualized infrastructure). Add that up and you get a lack of organization, infrastructure sprawl, and more fluidity as to where applications actually run, resulting in IT complexity and skyrocketing application-to-infrastructure dependencies.

It's at this point where the need for process abstraction and automation becomes acute. Because these interdependencies, which represent potential breakage points, are beyond human ability alone to manage. IT organizations are now forced to deal with these new realities while Cloud, Big Data, DevOps and ITaaS pressures get added to the mix in the name of providing more business agility. With all these moving parts, something needs to be stable and act as the IT backbone. It's increasingly obvious that it's the process and process control.

The days of designing the process to accommodate the shortcomings of infrastructure are over. Enterprises must abstract, insulate and protect their business processes from the applications and infrastructures that support them. The need for improved IT process automation is rising as the services and brand impact of on-line outages grows. ■

UC4 Software is the world's largest independent IT Process Automation software company. UC4 automates tens of millions of operations a day for over 2,000 customers worldwide. Rethink IT automation at www.UC4.com.

NY, NJ financial sector well prepared for Hurricane Sandy

BY LUCAS MEARIAN, COMPUTERWORLD

The financial services sector in New York City and New Jersey are dusting off disaster recovery plans and bracing for a storm that could bring 80 m.p.h.-plus winds and major flooding.

Hurricane Sandy could not have been hyped more by weather tracking services. Some are predicting "the storm of the century." Others, such as Henry Margusity, a senior meteorologist with AccuWeather, said the storm could bring a "disaster of biblical proportions."

But analysts and industry experts agree, New York and New Jersey aren't pushovers when it comes to potential disasters -- particularly their financial services business sectors. The lessons from the terrorist attacks on 9/11 were not lost on them, according to Kevin Knox, a research director with Gartner.

"After 9/11 there was notice taken to how close a lot of the data centers were. Since 9/11, we've seen a lot of work to separate the data centers to ensure a regional disaster wouldn't take out multiple data centers," Knox said.

The New York Stock Exchange is currently working with New York City officials to assess the readiness of safety, power, water and transportations systems.

"All U.S.-based NYSE Euronext Exchnages plan to operate on a normal business schedule on Monday, Oct. 29 and on the days following," said NYSE spokesman Eric Ryan.

IT systems over the past decade have become more hardened in terms of recovery time and recovery point objectives (RTOs and RPOs), or the time it takes to get systems back on line and minimizing the amount of data lost during that time. Over the past decade, RTOs have dropped from 48 hours to four or five hours in many cases, he said.

"The finance guys are probably some of the most aggressive as far as having disaster recovery capabilities, both in how quickly they can recover as well as ensuring they're mitigating risk," he added.

In many case, banks and brokerages will have two data centers in relatively close proximity -- 20 or 30 miles apart -- for business continuity where they replicate data in real time between the two to ensure if one goes down, the other can still operate. Then, they'll have a third disaster recovery site to ensure a regional disaster will still not cripple their operations, Knox said.

Knox said virtualization has had a lot to do with better RPOs and RTOs with regard to x86 server infrastructures in larger companies, and for SMBs, SaaS cloud services have allowed for better disaster recovery planning than at any time in history.

Billions of dollars in damage

Forecasters across the Northeast have said the storm could cause billions of dollars of damage to public infrastructure, businesses and private residences.

Walter Dearing , vice president of recovery services and customer resources support at SunGard, said customers are already executing portions of disaster recovery plans.

SunGard, which provides remote business continuity and hosting services, operates two types of facilities on the East Coast: one houses data center equipment that can be turned on and accessed by user companies; the others are "mega centers" where employees can go to work where desks and computers are readily available and pre-configured to go.

Hurricanes, Dearing said, actually offer better preparation time than other natural or man-made disasters that come without warning. Dearning compared forecasts of hurricane Sandy to Irene in 2011, which is the fifth costliest storm in U.S. history and 1991's Hurricane Bob, which at the time was among the ten costliest hurricanes in the U.S.

Hurricane Irene struck in Aug., 2011, brushing along the Mid-Atlantic until making its final landfall Brooklyn. Irene caused massive flooding and widespread wind damage, causing 56 deaths and leaving millions without power. It was estimated to have cause around $15.6 billon in damage.

In July 1991, after brushing past North Carolina's Outer Banks, Long Island in New York, Hurricane Bob made landfall on Rhode Island, and eventually caused $1.5 billion in damage to the upper Northeast including 17 deaths.

SunGard has hosting centers in Orlando; Atlanta; Herndon, Va.; Philadelphia; Carlstadt, N.J.; Queens; and Boston.

According to Marc DeCastro, an analyst with IDC Financial Insights, the impact of a hurricane is always two-fold: The impact to IT systems and business infrastructure; and the human element. What employees should be preparing to work from home or getting hotel rooms near a disaster recovery site, and who should be manning data centers during the storm.

"All those plans are being dusted off and reviewed by executives already and they're being communicated to employees," DeCastro said.

Advancements in mobile technologies will no doubt also play a key role, as they have in the recent past, in keeping communications up during and after the storm, DeCastro said.

"Especially in banking, there are so many electronic channels available. Maybe we don't have electricity, but maybe I can still communicate with my mobile phone," he said. "I can charge off car battery, and if I need to transfer money or make a payment, I can still do it with my mobile device."

"From a systems standpoint, we've had lots of practice," he added. "I think employees will be more involved in personal cleanup initiatives. You're talking 60 million people who are in the path of this storm. There could be a lot of turmoil as far as people thinking 'I need to protect my own property and family.' ■

Seven steps to DR planning

BY BRUCE BEAMAN AND BECKY ALBIN,
SPECIAL TO NETWORK WORLD

This vendor-written tech primer has been edited by Network World to eliminate product promotion, but readers should note it will likely favor the submitter's approach.

Unpredictability is a fact of life. Whether terrorist attacks, cataclysmic weather or simply a backhoe severing a power cable, enterprises never know when their operations may be threatened.

But mitigating the consequences of disasters need not be a matter of worry and guesswork. Here are seven steps to effective business-continuity/disaster-recovery (BCDR) planning:

Step 1 – Admit the possibility of disaster

The first step in BCDR planning is to admit the organization faces tangible threats that could jeopardize its prosperity – or its survival. Until this first step is taken at a senior leadership level, go no further.

Step 2 – List and categorize likely threats to the organization

The nature of the business and its physical and social environment will influence the types of threats an organization might face. Once the threats are listed, they should be categorized according to their likely impact on various systems. The cost of the response should be balanced against the tolerance for system downtime -- the less downtime that can be tolerated, the more it will cost to create an appropriate response. Some systems must be functioning again within minutes or seconds, while others can be down a few hours, and still others can be down for a few days.

Step 3 – Outline the organization's BCDR technology infrastructure

The key technology elements of a BCDR infrastructure consist of a main data center, a remote site that duplicates the resources in that primary location, and high-bandwidth network connections. The best BCDR strategies follow a "redundant everything" philosophy throughout the data center. Multiple mainframes and servers should run in the production and backup data facilities. Then if a component in the production system encounters problems, it immediately fails over to the local backup as a first line of defense.

Power supplies are one of the most critical components in a BCDR strategy. Power outages rank among the leaders in most common and preventable disruptions.

And no matter how fat the network pipe may be, it's of little use if a careless construction crew accidentally severs a fiber. Network connections must not only be redundant, they also need to follow different paths within a wider WAN topology to keep a single threat from bringing businesses to a standstill.

Step 4 – Inventory the organization's IT assets

Once organizations have sketched out the topology of their BCDR infrastructure, the next step is to develop an accurate inventory of IT assets. This enables the organization to understand the resources and business processes that need to be protected. A range of enterprise management tools are available to help organizations develop and maintain accurate inventories of IT resources. Vendors of these tools offer modules that use software agents to scour the IT infrastructure, storing details about hardware and software assets and their configuration parameters in configuration management databases (CMDB).

Step 5 – Set service-level expectations and define contingency policies

CMDBs store not only the details about the organization's software and hardware assets but also information about service-level agreements that define the uptime and recovery parameters for those assets. Recalling Step 2, it is important that senior management buy into service-level expectations, because these will determine (among other things) whether a particular asset must be up and running within 5 minutes or 5 hours of an outage. This determination directly influences BCDR expenditures that senior management will later be asked to support.

Based on a knowledge of assets, configurations and service-level agreements, an organization can define contingency policies. These policies must have executive-level support, and will therefore need to link IT asset performance directly to business requirements. In order to form this important linkage, the organization will need to perform a business impact analysis to flesh out details about system requirements, processes and systems inter-relationships. Executives must understand the consequences of system disruptions in order to support (and fund) contingency policies.

Step 6 – Develop a BCDR contingency plan

Flowing directly out of contingency policies, the contingency plan details the roles and responsibilities of departments and individuals in keeping technology systems available, as well as the procedures for restoring IT systems during an emergency. Key elements of contingency planning also include resource requirements, training needs, the frequency of training exercises and testing, maintenance schedules, and data-backup schedules.

The phases of a contingency plan include the initial notification/activation when the emergency strikes, restoration/recovery once emergency teams have been mobilized, and finally a return to normal operation (or a decision to remain on backup resources in the case that primary resources must be replaced or rebuilt over a significant period of time).

Step 7 – Test the BCDR contingency plan

Disaster-recovery experts say one of the most important yet frequently overlooked aspects of disaster-recovery planning comes after the formal policies and procedures are delineated. Plans must be tested initially for their completeness and effectiveness, and then retested on an ongoing basis to make sure that any subsequent changes to the IT infrastructure and business processes haven't created a need for policy modifications.

In addition, organizations should create test beds that accurately reflect day-to-day business conditions, so that drills simulate real-world conditions.

The world may be too complex for organizations to protect against every disaster contingency, but with the right technologies, clear service-level expectations, practical recovery policies, thorough contingency plans and rigorous testing methodologies, organizations can minimize the business consequences when the unexpected happens. ■

Prepare your business for digital disaster

BY CHRISTOPHER NULL, PC WORLD

You don't have to look hard to find tales of technological disaster. The Gauss virus infiltrated thousands of Middle Eastern PCs, where it could intercept online banking credentials. Apple iPhones were revealed to be vulnerable to spoofed SMS messages. Floods all but demolished Western Digital's hard drive production facilities in Thailand.

Closer to home, writer Mat Honan saw his digital life all but erased when a hacker used a couple of phone calls to order a remote wipe of his MacBook Air. Honan says that he lost more than a year's worth of photos after the breach--photos that, of course, he hadn't backed up.

These incidents--and to some degree, anything that goes wrong with your tech universe--have one thing in common: With careful planning, the victims could have rendered the problems much easier to recover from.

Sure, enduring a flood that wipes out your production facility is worse than losing some stored baby pictures, but disaster planning is essential for individuals and businesses of all shapes and sizes. The only real variable is the complexity of the necessary planning. For a small businesses, it's essential to plan for disasters so that you won't be completely crushed if catastrophe does strike. Here's how to start.

Backups: You can sharply reduce the bad effects of most technology problems by adopting a single surprisingly simple precaution: Back up your data.

You've undoubtedly heard this advice before, but even computer users who have suffered crashes, malware infestations, and other data-killing disasters often find it hard to get started, fearing that regularly scheduled backups are too tedious to perform or too complicated to set up.

None of this is true today. Myriad solutions and systems have simplified the task of backing up, whether you're dealing with one computer or a dozen. Here are some strategies you can start with.

Local USB backup: This is the simplest way to perform backups, but it's suitable for people with just one or two PCs. Plug a high-capacity USB hard drive into your computer, and set up a backup program. Windows 7 has one included--Windows 8 will add File History capabilities to the mix--and copious options exist online. If you arrange for automatic backups, so much the better.

Synchronization: Another strategy is to keep two computers in sync so that if one goes down, the other is available so you can pick up where you left off. Again, this option is effective only for very small businesses or in environments where everyone uses the same machine. One big advantage of a sync strategy is that you can set up computers in different rooms or different parts of the building so that if something happens in one part of the workplace (or if a thief steals equipment from there), the other side of the building may still be safe. Check out GoodSync for a solid sync arrangement.

NAS backup: When multiple computers need backing up, a network-attached storage (NAS) system makes excellent sense. A NAS device attaches to your router. You then use included software or your own backup program to back up to the NAS periodically. One drawback: Often, the backup software included with these drives is limited, and backup traffic can be so heavy that it floods your network. Check out the WD MyBook Live series for a great small-office NAS.

Online backup: If you have plenty of Internet bandwidth available, backing up online can be the most secure way to protect your data against disasters such as a house fire that destroys everything on the premises. Online backup sends your files (usually automatically) to a far-off location, removing any risk of loss from physical theft, fire, or flood at your business. On the other hand, some online, cloud-based services have been victimized by security breaches. That risk is probably tolerable for most of us, but if you work with highly sensitive information such as customer credit-card data, you might be best served by backing up this information locally and securing at an offsite location, such as a safe deposit box.

Antimalware and data security: Another common--and oft-ignored--tip is to install antimalware software on all of your business's PCs and keep it up to date.

This measure isn't terribly onerous if you're dealing with a single PC, but things can get complicated and expensive if you're trying to safeguard a small-business network. Any number of paid and free single-computer security solutions are available. If you have more than a few computers, you can save money by opting for a small-business security suite package. Some of these packages are no more than a bundle of licenses for the individual suite, each of which must be installed and maintained separately. Others offer a central management console for pushing updates out to users' PCs and receiving notifications about threats found on the network. Shop around to determine the approach that works better for you.

Physical security: Software safeguards aside, a thug with a crowbar can inflict massive damage on your business. That's why physical security should be a major consideration, whether you're a one-person shop or a company with a hundred employees. Every business owner knows to lock the doors and install an alarm system if there are valuable assets on the premises. But you should also take specific actions to protect your computer equipment, in addition to securing your building proper.

Cable locks: Cable locks are a simple way to increase any computer's security at very low cost. Almost all laptops have a special Kensington lock port, and most desktops have a metal loop that extends from the back and through which you can run a security cable. (Computers that don't have a lock port can instead use a "universal" lock system that attaches directly to the chassis.) Connect the computer to a desk with the cable, and you've added sufficient security to thwart most smash-and-grab operators. Be sure to store the keys to the cable locks in a secure location. You should also use a cable lock whenever you take a laptop out of the office.

LoJack systems: LoJack for Laptops is software that runs unnoticed in the background but lets your laptop broadcast its location when you report it as lost. This helps law enforcement locate the computer more easily and enables you to wipe its hard drive remotely if recovery seems unlikely. Tools like Find My iPhone offer similar features to smartphone and tablet users. Install them before your device goes missing.

Video surveillance systems: The all-seeing eye of a camera won't prevent determined thieves from breaking into your office, but remote surveillance systems may help you catch them red-handed. Video surveillance with motion detection will show the scene of a crime in real-time and record footage to help you pursue the bad guys later.

Fire, floods, and acts of God: We've dealt with thieves, but what about interventions of overwhelming magnitude? The general preparedness tips outlined above--especially the use of offsite backups--will help mitigate damage due to natural disasters, but a few devices can do even more, if you're concerned that a fire or flood might whisk away your life's work.

For digital storage, ioSafe makes a range of external hard drives designed to resist both fire (at up to 1550 degrees Fahrenheit) and water (a water column of up to 10 feet for 3 days). Keep analog essentials such as paper documents (and printouts of essential data) either offsite in a safe deposit box or in a sturdy fire safe on the premises. These inexpensive safeguards are well worth the investment.

And of course, you should include high-quality surge protectors or UPSs on all high-tech equipment for protection against power surges and lightning strikes.

Insurance: You can replace computer equipment, but that costs money. And if your business is out of commission for a month or two while you rebuild from a fire, you won't be earning anything along the way. That problem can destroy a company that might withstand the physical damage caused by a disaster.

Generally, insurance is the best safeguard against financial ruin. Standard property insurance will cover the loss of hardware, but business interruption insurance is essential if you want a safety net to preserve your company against lost sales.

Succession planning: One other component of your small business needs to be protected: you. Do you want your business continue to operate after you've shuffled off this mortal coil? If the plan is to shut it down, how will that happen? How will ongoing ownership issues be determined? Who's going to run the show?

These are complicated issues that any small-business owner should discuss with a qualified estate planner to resolve, and any protA(c)gA(c)s being groomed to take over when you're gone need to be aware of the plans well in advance. Software such as Quicken WillMaker steps an individual through basic estate planning. It's a serious subject, but tackling the creation of a will and a succession plan while you're young and healthy is far better than waiting until you're lying in a hospital bed. Make it a priority to create a continuity plan (or a dissolution plan, if you aren't going to pass the business along to an heir), and revisit it annually to ensure that it's up to snuff. ■

Is your disaster recovery plan ready for cloud?

BY PATRICK SWEENEY, DELL SONICWALL, SPECIAL TO NETWORK WORLD

This vendor-written tech primer has been edited by Network World to eliminate product promotion, but readers should note it will likely favor the submitter's approach.

Having successfully piloted cloud usage with SaaS applications such as CRM and ERP, many businesses are now looking to replace traditional on-site backup and disaster recovery (DR) solutions with cloud-based DR. Gartner predicts that more than 30% of mid-size companies will have adopted DR in the cloud or recovery-as-a-service by 2014. That begs the question: Is your business ready to make the leap?

Implementing traditional DR solutions typically involves overcoming a number of hurdles. First, they can be difficult for overburdened IT staff to deploy, configure and administer. Moreover, some require the complex integration, coordination and scheduling of disparate systems at multiple backup sites.

Traditional solutions can also be difficult to budget. They often require significant upfront capital expenditures for hardware, software and network infrastructure, duplicated across multiple sites. And, once established, they can be costly to scale incrementally. Additionally, these multiple infrastructures must be managed and maintained, adding to administrative overhead costs.

Yet another traditional concern with DR is uncertainty. Many DR administrators simply do not know if they can rely on being able to recover the data they back up.

All else considered, the worst DR is no DR. Yet the awful truth is that most companies have found it difficult to get any DR plan or solution off the ground.

Cloud-based DR services have the potential to address many of these concerns. First of all, they are inherently easy to use and manage, as they are typically deployed as turnkey solutions, with the back end hosted and managed by the provider.

Because they operate in virtualized environments, they are generally easier to scale as needed, providing more deployment flexibility, and future-proofing against unanticipated growth. This scalability also provides broader DR options (such as supplementing or enhancing VMware, NAS or bare-metal recovery solutions), thus enabling a best-fit deployment.

Perhaps most importantly, by making the process easier, they can enable overburdened IT organizations to actually get a DR solution deployed in the first place.

Using cloud services can also be more

budget-friendly. By eliminating significant hardware costs, they cut out large upfront capital expenses. Instead, DR becomes a flexible, pay-as-you-go operating expense, where companies only pay for the capacity they consume, and can fine-tune or terminate services altogether on demand.

Recovery-as-a-service can also help assure reliability. With no upfront investment, it is easier to test a solution before adoption. Moreover, cloud-based DR technology has matured to the point of providing reliable quality of service and uptime levels, as well as cloud-based validation of backed-up data.

Not all silver linings

Still, there are many challenges that businesses must consider that are unique to cloud-based DR. For example, placing your backups in the cloud may create greater dependency on network availability and, subsequently, in the service levels of your providers.

Likewise, with cloud-based DR, companies can have less control over throughput, and any degraded performance can potentially generate transactional lag time. While this might not significantly affect recovery of static files or email, it can make cloud-based DR inappropriate in other scenarios, such as in recovering dynamically replicated databases. Increased demand for additional bandwidth might also result in unanticipated cost overruns.

Compliance can be another serious concern for many businesses looking at cloud-based DR. While cloud-based security and encryption technology has matured, there may still be grey areas when it comes to meeting regulatory standards, such as with healthcare or financial data.

Ultimately, DR is about shifting the uncertain to the certain. We cannot be certain when a disaster event may occur, but we should -- and must -- be certain of the systems and procedures we put in place to recover when they do. To determine whether your business is ready to bring DR to the cloud, you need to consider factors pertaining both to your organization and to your service provider. The viability of implementing recovery-as-a-service in your organization hinges on both business and technology criteria.

On the business side, you should calculate return on investment by contrasting the projected costs of cloud-based DR against the costs of traditional on-site DR (including equipment and staffing) -- as well as against the projected business costs of enduring a catastrophic system failure while having no DR solution in place at all.

As with any DR planning, you should determine your recovery time objective (RTO) within which your core systems must be restored so as not to create a revenue-impacting break in business continuity. You should also identify any system elements which would be negatively affected by potential transactional lag times. Specify what is required to meet compliance with your particular industry's regulatory mandates (such as end-to-end encryption of data in-flight and at-rest, or granular recovery of transactional data).

You will also want to consider what options you need to meet the specific recovery needs of your business. Potential data recovery capabilities your organization might require include file-based backup, multi-platform device and OS support, and archiving. Potential system recovery capabilities might include block-based backups, and being able to rapidly restart applications in the cloud with a subsequent phased recovery on-premise.

On the cloud service provider side, you need to verify that the service level agreement (SLA) meets your defined business requirements, particularly in the areas of reliability, performance and compliance. Closely examine the fine print on costs associated with scaling up capacity or bandwidth.

Be sure you are willing to house your data on your provider's cloud. Confirm your provider's cloud data center security and availability features, such as AES 256-bit encryption for data-in-flight, uninterruptible power (UPS) and seismic rating, as well as physical security measures such as biometric identification and motion-sensitive CCTV monitoring.

The underlying technology used by your service provider can also provide insight into the viability of your solution. Look to providers with a comprehensive, full-featured offering on a mature, established platform, with central management of data and policy, as well as granular reporting.

By closely evaluating all of these criteria, you can determine with certainty whether cloud-based DR will work for your organization.

Implementing a DR solution is never simple. But for some companies, the emergence of cloud-based DR services can make it much easier, affordable and reliable. Whether your business can take advantage of these benefits will depend on taking a hard look at your unique DR needs and matching them to a service that fits. An uninformed decision will only add more uncertainty, rather than alleviate it. ■

Cloud-based backup and disaster recovery services yield peace of mind

Conducting regular data backups and planning for business continuity in the event of a disaster are two of those mundane tasks that are under-appreciated until critical data or applications need to be restored. The tasks are made tougher in the face of exponential data growth, which Gartner estimates to be about 45% annually. It can be a challenge to find backup and disaster recovery (DR) solutions that are both efficient and cost-effective as the amount of data to protect continues to grow.

Small companies might find it sufficient to use a "prosumer" online solution like Carbonite or Cbeyond for data backup, and this is often the DR plan as well. Large enterprises have the SunGards of the world for contracted DR. The organizations that are too big for Carbonite but too small for SunGard often piece together their own solutions or go without a cohesive disaster recovery program. Although these are essential IT capabilities, many companies don't consider them to be strategic and thus they go unnoticed -- and often under-funded -- until the day these services are needed.

Data backup and disaster recovery are two IT services that are ripe for cloud computing. Cloud service providers already have the data center infrastructure

Amazon failure brings down sites

BY BRANDON BUTLER, NETWORK WORLD

Amazon Web Services has confirmed that its Elastic Block Storage (EBS) service is experiencing degraded service, leading sites across the Internet to experience downtime, including Reddit, Imgur and many others.

AWS confirmed on its status page at 2:11 p.m. ET that it is experiencing "degraded performance for a small number of EBS volumes." It says the issue is restricted to a single Availability Zone within the US-East-1 Region, which is in Northern Virginia. It warns that instances using EBS volumes will also experience degraded performance.

As of mid-afternoon, popular social media site Reddit displayed an error message noting it was down. Photo-sharing site Imgur is also being impacted, along with vacation rental service AirBNB, payment service Payvment and others.

AWS EBS is a cloud-based block storage service that allows users to store large amounts of data; it's typically used in conjunction with AWS's Elastic Compute Cloud (EC2) services. AWS breaks each of its data centers up into multiple Availability Zones and recommends that customers run their workloads across multiple zones to prevent downtime.

AWS has periodic performance issues this year, including its last major outage in late June, which it blamed on powerful storms that ripped through the mid-Atlantic region causing power outages. Last year, AWS was down for as many as four days for some customers, including Reddit, Foursquare, Quora and HootSuite.

Update: Shortly after confirming the EBS outages, AWS reported that its Relational Database Service, Elastic Beanstalk, which is an application deployment service and ElastiCache were also impacted by the outage. AWS says it is working to repair the downed instances and has already made some progress.

Reports on Twitter indicated that other sites, including Pinterest, GitHub and Gamespot, also experienced service disruptions. ■

and the accompanying management practices to back up, protect and restore their clients' critical data and application assets. Client organizations just pay a monthly or annual fee for this little slice of heaven and rest easier knowing their data or entire business operations can be restored if and when the need arises.

There are cloud service providers that recognize this need and tailor their business toward the specific demands of backup and DR. One such company is nScaled Inc., a cloud service provider that offers a hybrid cloud infrastructure as a service (IaaS) for companies under 10,000 employees. nScaled offers multiple cloud solutions, including primary application hosting and Test/Dev environments, but the solution offerings that are attracting the most customers today are disaster recovery and backup. nScaled's hybrid architecture allows customers to recover data quickly from a local appliance if needed.

nScaled places a Local Cloud Appliance within a customer's network which acts as a multi-functional gateway to the nScaled Hybrid Cloud. This appliance connects directly to the nScaled cloud, replicating workloads, de-duplicating data, providing local recovery capability and, according to the company, reducing application response times by up to 98%.

The customer installs nScaled Host Agents on the Microsoft Windows and Linux physical and virtual servers to be protected. The Host Agent replicates block-level data, either by partition or by entire disk, and sends it to the Local Cloud Appliance. The Host Agent delivers real-time data protection for either NAS or SAN storage, providing end-to-end data protection, remote disaster recovery and backup. Once the data is on the local appliance, it is de-duplicated at 90% efficiency and then replicated over secured VPN or MPLS links to one of the subscribed nScaled Cloud data centers.

nScaled says it provides broad-based cloud backup for all servers and workloads in a company's data center. Unlike tape backup, the nScaled solution makes use of snapshot technology which leverages incremental differencing to provide a near continuous backup. Recovery time is said to be in minutes and is easy to perform from any snapshot recovery point on the nScaled appliance. These recovery points, which can be taken every 15 minutes if desired, provide comprehensive historical protection.

Backups can include individual email messages, files, databases or entire volumes. Data is encrypted during transmission to the cloud and is also immediately available for recovery from this location. At least three copies of all data exist in two separate geographic locations: locally on the customer's production servers, on the nScaled Local Cloud appliance, and remotely in the nScaled data centers.

A Cloud Console allows system administrators to manage infrastructure services both in the cloud and within the confines of their data center. Complex tasks like disaster recovery can be executed with push button operations within the Cloud Console.

nScaled certifies its backup services and disaster recovery services. For backups, any physical or virtual production server can be certified that it will mount as a drive, that it is available in the Cloud Console interface and that a recovery of data can be initiated from it. For disaster recovery continuity servers, the backups are certified to spin up automatically when needed. This certification provides organizations the assurance that these crucial tasks are taken care of by experts in the field and allows their IT staff to refocus their attentions on more strategic initiatives.

Data backup and disaster recovery are best practices for every business, regardless of size. Cloud services are making it easier to attain professional-level services at a reasonable cost with little effort or expertise on the customer's part.

— Brian Musthaler, Network World