How to Survive a Disaster

Business continuity planning helps ensure that an organization can recover quickly should downtime or disaster strike.

The 2014 hurricane season has been quieter than anticipated, with only one storm impacting the eastern U.S. But with several months left to go before the season officially ends, organizations would be wise to take stock of their disaster preparedness. How much time would it take to recover data and applications in the event of a data center outage? How much would it cost?

Hurricanes aren't the only cause of disaster, but they serve as a stark reminder of the importance of business continuity and disaster recovery planning. Most organizations are unprepared even though unplanned downtime is virtually inevitable. Research from the Ponemon Institute found that 95 percent of companies experienced a data outage within the past 12 months. Another study

How to Survive a Disaster

from Gartner revealed that about one in four organizations have experienced a full data disaster.

"Statistics show a steady increase in the number of climate-related disasters since the 1970s," said Krystal Triumph, IT & Telecom Advisor, Atlantic-IT.net. "Malicious cyber-attacks are also on the rise, as well as other types of man-made and technical disruptions. Experts warn that organizations should consider disruptions to be regular events and plan accordingly."

Without a documented and tested business continuity and disaster recovery strategy, the financial impact of such disruptions can be staggering. According to Gartner, downtime costs $70,000 per hour for midsize companies — and those organizations experience 16 to 20 hours of network, system or application downtime per year. The cost to repair damaged relationships and a tarnished reputation could be even more expensive. In fact, PwC found that seven in 10 organizations that suffer a major data loss shut their doors permanently within a year.

What's the Difference?

Many organizations confuse the concepts of business continuity and disaster recovery. While definitions may not seem important on the surface, understanding the distinction between the two can help organizations plan more effectively and minimize the risk and impact of downtime.

Disaster recovery is the process of storing data at a secondary site so this data can be quickly recovered and accessed when a disaster occurs. The speed of this process is critical. If disaster recovery isn't well-planned, or if the organization has no plan at all, it could take days or weeks to recover and access data. Some data may need to be re-created, which could cost thousands of dollars, and other data may be permanently lost. If the organization is subject to regulatory compliance requirements, the failure to produce data could result in severe penalties.

Disaster recovery is just one component of business continuity. Gartner states that, in addition to a disaster recovery plan, business continuity should include a business resumption plan that identifies how critical services are maintained at a crisis site, a business recovery plan that identifies how business functions will be recovered at a secondary site, and a contingency plan that identifies how events that affect the organization will be managed.

"Downtime measured in minutes is tolerable. Downtime measured in hours can be crippling, while downtime measured in days or more can devastate a business."

"While disaster recovery focuses on data, a business continuity plan includes the processes and procedures that enable an organization to operate during and after a disaster with little or no downtime," Triumph said. "Business continuity planning also prioritizes what data and applications need to be recovered based upon the needs of the organization as well as customers, business partners and vendors."

Minimizing Risk

Data protection is still a key component of business continuity. Data should be stored in at least two locations simultaneously, with a failover mechanism that makes it possible for users to access data and applications from a secondary source when the primary source goes down.

Clearly defined processes and effective internal and external communication are also critical. Organizations may be able to recover data quickly but find that the data is difficult to access because passwords and other essential information are lost.

Business continuity plans must be regularly tested and updated through mock exercises and drills so organizations can carefully analyze any number of "what if" scenarios. Weaknesses, errors, omissions, discrepancies and threats need to be identified and addressed. For example, will the plan allow the organization to live up to contracts with customers and business partners?

"The 24x7 nature of today's business environment underscores the need for effective business continuity planning," said Triumph. "Zero downtime is the goal. Downtime measured in minutes is tolerable. Downtime measured in hours can be crippling, while downtime measured in days or more can devastate a business. We live in a world in which people expect fast access to data, fast answers to questions and fast decisions. Only through proper planning and preparation can organizations meet these expectations."

Given the complexity of today's IT environments and the sheer volume of users, devices and data that networks must support, organizations should operate under the assumption that disruptions will occur. The key is to have an effective business continuity plan in place to ensure that normal business operations can continue with little or no downtime when something does go wrong.

Software Bloat Straining Infrastructure

A tangled web of applications within international organizations is getting more and more complex, putting strain on the IT department and stunting digital transformation, according to a new study from consulting firm Capgemini.

Some 48 percent of 1,116 CIOs and senior IT executives said their companies have more applications than required to run the business. Nearly three-quarters (73 percent) believe that at least one-fifth of their current applications share similar functionality and should be consolidated, and 57 percent believe that at least one-fifth of their applications should be retired or replaced.

This isn't just an IT problem, it's a business problem. As organizations implement new cloud, mobility and big data solutions, they often lack the bandwidth to gain full competitive advantage from these technologies because of the bloated applications landscape.

Study: Fraud on Upswing in U.S.

Due to the continuing upward trend in the occurrence and detection of economic crime, companies are beginning to change how they think about cybersecurity — viewing it as a business issue, not just an IT issue.

Forty-five percent of organizations in the U.S. suffered from some type of fraud in the past two years, more than the global average of 37 percent, according to PwC's Global Economic Crime Survey 2014. U.S. companies are growing their international operations, and the expanding role of the internet and mobile technology in business can bring risk from beyond their geographic footprint. The survey revealed that 54 percent of U.S. respondents reported their companies experienced fraud in excess of $100,000 with 8 percent reporting fraud in excess of $5 million.

In the Mail

Growing complexity is straining the framework, but on-premises email remains the standard for business communication.

E mail is perhaps the original "killer app," an application so effective and easy to use that it sparked the rise of the personal computer and the spread of the Internet. Today it is de facto standard for business communication, supplanting the phone and even personal meetings in most organizations.

"Email has become critical to businesses of all sizes," said Suaad Sait, executive vice president of software maker SolarWinds. "Just try shutting it down for 10 minutes and observe the outcry. In fact, in the business hierarchy of need, only Internet connectivity trumps email, with everything else in tow."

Email is such a part of the basic fabric of business communications that it has become easy to take for granted. However, relentless growth combined with disruptive technologies such as mobility and "Bring Your Own Everything" (BYOx) are challenging administrators' ability to keep this oft-neglected application up and running.

According to a recent study by the Radicati Group, there are approximately 4 billion active email accounts worldwide, with one-quarter of those identified as business accounts that generate 100 billion emails per day. Email Analytics reports that more of that email is now read on mobile devices than on desktop clients.

"Contrary to logic, as email matures it's getting harder to manage," said Sait. "The industry as a whole has not given email management the attention it deserves."

Not So Easy

Because email has been around so long and is so easy to use, there is a tendency to think of it as an uncomplicated technology. In truth, it has always been a fairly complex service to deliver because it requires the integration of so many components — servers, storage, operating systems, the platform software itself, as well as other supporting elements such as directories, filters, security, backup, e-discovery and archiving solutions. According to one survey of IT professionals, a typical email architecture might involve roughly 19 platform servers, eight servers for archiving, six for antivirus and another six for mobile device management.

In a survey conducted in February and March, SolarWinds found that IT managers and directors believe the increasing adoption of BYOx and mobile technologies is making email management even more complex. Eighty-seven percent of respondents said the mass adoption of smartphones and tablets has increased the amount of email sent and received. Fifty-three percent say they now use three or more tools to manage the email environment.

This fractured management creates significant risk for organizations in light of the fact that email accounts have become increasingly important data sources. By some accounts, about 45 percent of an enterprise's business-critical information is stored in its email system. Workers routinely rely on email as the repository for messages containing important information such as negotiation details, agreements and customer commitments. Mimecast found in a recent study that 86 percent of workers rely on email as a search tool to find documents or information from within their inbox or archive.

"The research shows that the way the average employee uses email at work has changed," said Peter Bauer, CEO and co-founder, Mimecast. "For many people, email is no longer just a messaging system. It has become the primary tool for storing, sharing and searching for information. This is why we are seeing information workers increasingly becoming 'inbox workers' — they rely on email for all aspects of their job and spend, on average, 50 percent of their working day using email."

> "For many people, email is no longer just a messaging system. It has become the primary tool for storing, sharing and searching for information."

Cloud Reluctance

Some organizations have begun to explore cloud-based hosted email platforms in order to relieve some of the management burdens. However, most IT decision-makers remain reluctant to move the responsibility for email outside the organization. In the SolarWinds survey, 74 percent reported that they maintain on-premises email systems.

There are a number of advantages to maintaining in-house email, including the ability to support a large number of operating systems and virtualized environments, greater control over targeted email broadcasts, and the ability to reuse existing servers and storage to improve TCO.

Security and regulatory compliance remain the chief reasons for maintaining in-house email. On-premises email ensures complete control over the custody of data, which is not entirely possible with a cloud provider. Cloud-based solutions don't always include data loss prevention or encryption, which are critical for organizations with regulatory requirements.
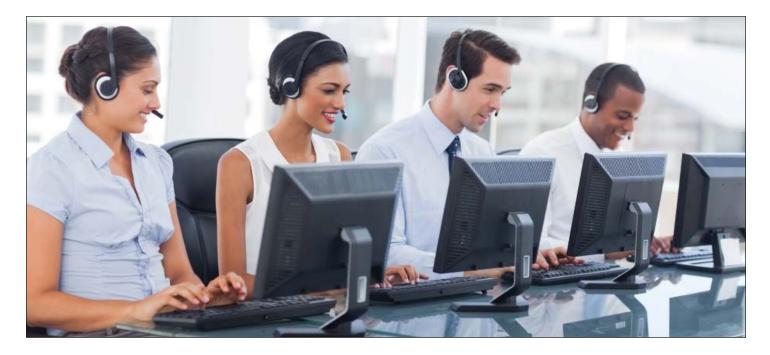
Showing Some Backbone

Industry experts expect "next-generation" email systems will soon relieve IT staff of much of the management burden and give organizations even more compelling reasons to keep these critical systems in house. Some vendors are attacking complexity issues by adding intelligence to the email backbone, the middleware layer of an email infrastructure that handles message routing and policy management. An intelligent email backbone control point reduces complexity by managing authorizations, permissions, alerts and notifications for compliance, while also offloading much of the policy enforcement and message processing overhead from the email platform.

Some industry analysts expect on-premises solutions will eventually morph into overarching portals that allow employees to use social media, instant messaging and other communication channels from within the email client. This "frictionless" communication will better serve the "anywhere, any device" needs of the modern workforce.

Email has been a great business tool for many years because it is easy to use and it gets the job done. Even though new demands are straining the basic framework, most industry experts predict that next-generation advances will allow email to hold its title as the champion of business communications for some time to come.

At Your Service

Today's IP-enabled, multichannel contact centers help organizations maintain strong customer relationships.

For many organizations, the contact center is where the rubber meets the road. It often represents the first interaction customers have with the company, and the success or failure of that initial experience can set the stage for all subsequent interactions.

The nature of that experience has changed dramatically in recent years. While the telephone remains a primary means of contacting a company, customers in growing numbers want to do business by email, chat, texting, and mobile and social applications. Indeed, the growth of these consumer channels has led to the death of the "call center" and the rise of the "contact center," which does much more than handle voice calls.

Voice over IP (VoIP) technology, has made this transformation possible. Thanks to VoIP, contact centers have come a long way from simply routing calls to the agent group with the right skill sets and maybe adding a "screen pop" with data about the customer. With a fully integrated IP contact center, organizations can provide a consistent, high-quality customer experience regardless of how the customer chooses to interact.

Customers utilizing the web to research a product can "click to talk" and be connected to an agent who is familiar with that product and looking at the same screen. Supervisors can not only monitor calls but can initiate online chat sessions with agents to offer advice while the agents are on the phone with customers. Many organizations are also looking to add new contact center services such as video and mobile solutions.

From 'Interaction' to 'Experience'

VoIP makes this possible by converging voice and video onto the data network. As such, any application can theoretically be integrated into the voice infrastructure, providing a platform to support sophisticated, multi-channel communications.

The 21st –century contact center is more than a collection of communications channels, however. The technology is evolving toward a contextual understanding of customer interactions. Instead of handling individual transactions, organizations can create the ability to manage the overall customer experience.

In the past, a financial institution might simply route loan-related calls to a certain type of agent. Today, that

financial institution can understand that the customer has three types of loans and called twice last week, and route the call to a particular agent who can best handle the call based upon those attributes. An organization can also know that a customer started on a web site and then called in and manage the customer's experience accordingly.

Getting to this nirvana is not as simple as plugging in a contact center solution. There's not one technology that can transform a traditional contact center into a full-blown customer experience management solution — it takes a whole set of tools. Organizations should begin by defining the experience that they want their customers to have as they interact with the contact center and how the contact center is going to create and manage that experience. Once that's defined, it's essential to choose the right contact center solution to lay the foundation and then add the necessary building blocks on top of it.

Many Benefits

The converged voice, data and video network underlying VoIP technology offers a number of other compelling benefits in the contact center. It minimizes the total cost of telephone services, reduces network management costs and creates the ability to build geographically dispersed contact centers that satisfy "follow-the-sun" business-hour coverage and assure business continuity.

VoIP also enables the development of the virtual contact center model, in which calls are routed to agents working at home or to their counterparts working in the traditional contact center environment. The technology is absolutely transparent to the customer. Leveraging a home-based workforce not only drives down the real-estate costs of brick-and-mortar operations, but allows organizations to break down the geographical boundaries of their labor pools and opens the door to an untapped pool of highly skilled candidates. It also provides for business continuity in the event of disaster or weather-related travel restrictions.

A contact center has a number of layers, from the core customer interaction management to the agent experience, the supervisor experience and the manager's experience. These interfaces must be easy to use in order for the customer interaction to be successful. Reporting and analytics are also critical decision-making tools that help managers optimize the customer experience, maximize agent efficiency and keep costs low.

Building a multichannel contact center requires analysis, planning and significant expertise. But by facilitating multimedia communications, providing customers with a better experience and improving information flow, IP-based contact centers provide organizations with a powerful edge in their quest to provide better customer service and cement customer satisfaction.

all your technology needs under one umbrella

Keeping up with the multitude of new developments in hardware, software and infrastructure can be overwhelming for IT staffs that are already stretched thin. Atlantic-IT.net can help.

Atlantic-IT.net is a full-service IT solutions provider that designs, implements and supports integrated voice and data communication solutions for businesses and government agencies.

Gain the advantages of "one-stop shopping" plus our 15+ years of experience. Call Atlantic-IT.net for all your voice and data needs, including:

◆ IP Phone Systems
◆ Mobility and Wireless
◆ Contact Centers
◆ Backup and Disaster Recovery
◆ Networking and Security
◆ Cloud Computing

atlantic-IT.net

Aligning Information Technology With Business Strategy

Contact us at 877-936-3328 or go to www.atlantic-IT.net to learn how we can help with technology initiatives that can push your business to new heights.