

Business continuity and disaster recovery planning

Can the cloud help?

ARTICLE

It is not pleasant to think about, but disasters happen, and no business is immune. They can manifest themselves in many different ways, potentially bringing your business to a halt and causing significant financial, operational and reputational harm. Every organization must maintain a thorough business continuity and disaster recovery plan, and cloud technology is emerging as an effective tool to help companies protect their environments.

Disasters are typically thought of as natural events such as a flood or tornado, but they are actually categorized as anything that can disrupt your business for a period of time. Power outages and server failures are also considered disasters in many instances, as well as an Internet disruption or a key IT person leaving the business. While you can't predict when disasters will happen, you can be prepared for when they occur.

Before you know where your disaster recovery plan needs to be, you need to know what your technology capabilities currently are. To evaluate your current posture, you should first go through a discovery phase, connecting business units, and their needs, to technology.

The initial step is to understand your current IT environment, including hardware and software such as network infrastructure (servers, routers, switches, operating systems, wireless access points, etc.) and all business applications. The discovery phase also includes assessing the recoverability of your current systems. Determine if anything needs improvement before looking at the disaster recovery plan, including the usability and accessibility of systems, remote accessibility, performance, and planned and unplanned downtime.

It helps to have someone from IT involved in the discovery process to provide input from a high level about how systems are related to the business. Often, organizations will bring in a third party for this step, including it in an overall technology assessment. The third party can help evaluate what is being done well, what needs to improve and how to leverage technology in the future.

Connectivity is a key element of discovery that is often overlooked; you must understand your current bandwidth, as well as alternative options for access. This can dictate the design of your disaster recovery plan, and whether the cloud can be leveraged in your strategy.

The final phase of discovery is business continuity planning. Begin with the high-level strategy of the business and determine what applications, systems and data are most critical to those goals. Having that organizational plan front and center during the process helps ensure that an effective plan is implemented.

The key part of business continuity is a financial impact analysis; you need to know what the impact to your business is if a system or data set is not available. This discussion should include people that use specific applications to understand dependencies and how applications are used to perform tasks. This process includes questionnaires and focus groups to understand the financial and operational impact that could occur following a disaster.

Once the business continuity plan is approved, IT can use that information as the basis for disaster recovery system development. In many cases, companies upgrade production systems and relocate older systems to the disaster recovery location. This lowers costs at the disaster recovery site, and ensures the best equipment is used at the production site.

The explosion of third-party cloud services and an increase in bandwidth has given businesses more options for implementing better disaster recovery systems in a more cost-effective manner. Some organizations take their first step into the cloud with a co-location strategy. It involves housing storage and servers to run the disaster recovery site in a third-party data center. The monthly costs for co-location are typically more manageable than major upgrades to an on-premises facility. A third-party data center also includes redundant power, connectivity and additional protections that middle-market companies cannot provide on their own at a reasonable cost. Most cloud service providers also have recovery or backup-as-a-service options to back up an organization's environment to their cloud data center.

These solutions can be very cost-effective and a valuable solution because organizations do not have to purchase additional hardware or software to protect their environment from the effects of a disaster. They can also provide an entire backup and recovery solution, not only managing disaster recovery, but also everyday situations when files must be restored.

Some companies are concerned about potential risks when transitioning their production environment to the cloud. However, a business typically achieves better uptime and availability in the cloud, as it takes many of the risks of physical servers out of the equation. The design of a cloud services data center is built for high availability and disaster recovery. Although, as with any

application, you must perform due diligence to ensure the environment that you move your information to meets the requirements for your business.

The two main cloud platforms that can help improve disaster recovery and business continuity for an organization are software-as-a-service (SaaS) and infrastructure-as-a-service (IaaS). SaaS is the typical cloud services platform where data is stored in the cloud, and users access that application through a Web browser or application. For example, many companies are moving to Microsoft's Office 365 cloud platform to provide enhanced disaster recovery capabilities for communications. Email is critical for today's businesses, and you need to make sure it is always functional and available.

Vendors are introducing cloud options for other key business applications to keep up with demand. Anything that is moved from an on-premises environment to the cloud makes disaster recovery easier to plan and account for. When considering your disaster recovery strategy, it is a good idea to look at your vendors and see what cloud options are available and how they can benefit your business.

With IaaS, the cloud provider takes responsibility for virtualization, servers, storage and networking, but your IT department still has the flexibility to activate servers when needed, upgrade applications and move data. IT still performs its typical tasks, without worrying about the availability of hardware.

Regardless of your disaster recovery strategy, testing must be a critical component. Documentation is essential for future testing; any issues can help develop a stronger foundation for your business continuity plan. In addition, proper documentation provides the steps that must be followed to get applications back up and running if a disaster occurs.

An annual tabletop test is also a valuable exercise. The test involves discussing specific disaster scenarios as a group and walking through the process should those situations occur. Your users should evaluate necessary communication, what coordination is required with third parties or other organizations, and other items needed to run the business.

Technology changes at a rapid pace, and as it evolves, you must ensure you are utilizing it to make your disaster recovery plan more effective. Understanding how your technology investments align with business needs and determining which of your applications can be moved to the cloud can help immediately improve your environment. By leveraging the cloud, you can simplify and enhance your disaster recovery strategy, and cost-effectively scale without making significant capital investments.

AUTHORS

Scott German

Director

IN THIS ISSUE

[Can you benefit from the next generation of managed IT services?](#)

[Business continuity and disaster recovery planning](#)

[Transforming the budgeting and forecasting process](#)

THE POWER OF BEING UNDERSTOOD

AUDIT | TAX | CONSULTING

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

© 2019 RSM US LLP. All rights reserved.