DOWNTIME COSTS HOW MUCH?

Calculating the business value of disaster recovery

Quest®

Introduction

As an IT professional, you will experience a system failure, outage or complete site disaster at some point. It's inevitable, and your organization probably already has some sort of disaster recovery (DR) plan in place.

> An ineffective DR plan can mean the difference between being seen as a hero to the C-suite and finding yourself in a job interview.

Most days, you probably don't even think about DR. You focus on projects that streamline processes, decrease costs and give you some good visibility. DR is rarely considered strategic to the business. But when that disaster happens and you need to quickly restore your company's data and IT services, an ineffective DR plan can pose a serious threat to the company as a whole. And for you, it can mean the difference between being seen as a hero to the C-suite and finding yourself in a job interview somewhere else.

Take, for instance, the Orleans Parish in New Orleans. As you can probably imagine given the location in an area prone to natural disasters, the parish has a DR plan rightfully in place. However, when two servers that held the area's conveyance and mortgage records dating back to the 1980s crashed simultaneously, their DR plan came up short.

The Times-Picayune newspaper reported on the incident, saying, “Without a complete and verified database of both conveyance and mortgage records, title companies can’t be sure that a person trying to sell a property truly owns it free and clear. And the mortgage record database, which is separate from the one for conveyance records, is still missing about 100,000 documents.”

A bout of finger-pointing ensued. The parish’s IT staff had thought it was backing up the parish’s data using a cloud backup and disaster-recovery-as-a-service (DRaaS) provider. But neither the IT staff nor the service provider was aware that the data hadn’t been backed up for months. What data had been backed up had passed its 30-day retention policy and was deleted.

In baseball, it’s like two outfielders giving up on a fly ball because each player thinks the other will make the catch. The ball just drops to the ground with a thud and rests at both players’ feet.

No doubt personnel at both the Orleans Parish IT department and the service provider found themselves scrambling to update their resumes.

What happened in Orleans Parish illustrates a situation that is all too common and yet completely avoidable. Effective disaster planning ensures that your business is adequately prepared to continue functioning in the wake of events that would otherwise be catastrophic. The purpose of this e-book is to put you on the path to developing an effective disaster recovery plan that will be seen as a strategic tool to your company’s success.

Expectations vs. reality

As an IT professional, you already know that companies rely on technology more than ever before. With this increasing reliance on technology comes the expectation that it will always work. And, increasingly — as shown by the 80 percent increase in the number of days per week that people telecommute — it needs to work from any location.

End users have come to see IT as a basic service, just like water or electricity. They expect that their company's data and applications will be available at all times, from any device. Most people don't even think about it until it's suddenly not available.

Your customers' expectations have grown as well. For example, a customer trying to make a purchase through a company's website expects the transaction to go smoothly — exactly when they're ready to buy and from whatever device they happen to be using.

Again, this is hardly news to a seasoned IT pro. But what is surprising is the gap that exists between these expectations and the reality most companies face. While IT professionals are doing all they can to meet these growing business needs, an integral component of their mission — backup and disaster recovery — often fails to receive the strategic focus and support it deserves from the business side of things. Companies that do have DR plans in place often fall short in developing and executing the right DR plan.

Your mission, should you choose to accept it ...

This misalignment between IT and business strategies gives rise to a tremendous opportunity for you as an IT professional. You are already a jack of all trades — an expert in multiple domains. You are uniquely positioned to recognize the gaps and identify solutions. You are equipped to apply the tools and techniques needed to mitigate risks and position the company to thrive. In today's world, IT professionals who can apply their knowledge in technology and also think like business leaders will be more likely to advance and realize success in their careers.

> IT professionals who can apply their knowledge in technology and also think like business leaders will advance and realize success in their careers.

Use your know-how to bridge the gap and make yourself really stand out. This e-book offers information to help you organize your thoughts, ask the right questions and develop the right strategy to begin building a business-centric DR plan.

Calculating the value of DR

DR is often neglected because it doesn't generate revenue or reduce costs. To take a more business-centric approach, you'll need to step outside your comfort zone and demonstrate the value that DR brings to the business. The No. 1 way of doing this is to calculate how much a disaster would cost the company if one were to occur.

This calculation can get complicated quickly, with the potential for many variables. But simple arithmetic often does the trick, as long as the variables you use are realistic and the calculations stand up to scrutiny.

Cost of downtime	
Average yearly compensation per employee (salary + benefits)	$65,000
Total hours that F/T employees work per year	2,080 hours
Hourly compensation	$31 per hour
Number of employees unable to work because of the disaster	100 employees
Number of hours of downtime	8 hours
Total cost of downtime	**$24,800**

Table 1: *This example demonstrates the cost of a disaster that caused eight hours of downtime during normal business hours.*

Lost revenue	
Company's total yearly revenue	$10,000,000
Hours of operation	2,600 hours
Average revenue generated every hour	$3,846
Number of hours of downtime	8 hours
Total revenue lost	**$30,768**

Table 2: *You also would need to calculate your company's lost revenue.*

Nonrecurring costs (per disaster)	
Employee overtime/contractor pay to restore operations	$2,000
Vendor charges	N/A
Hardware repairs	$5,000
Total cost of downtime	**$7,000**

Table 3: *Be sure to add nonrecurring costs associated with restoring operations, such as hardware repairs, vendor charges (some less scrupulous vendors charge for the amount of data recovered), contractor pay and employee overtime.*

The total cost of eight hours of downtime in this particular example is **$62,568.** And if the downtime affects a customer-facing website or application, these numbers don't even begin to calculate the cost of customer frustration, the flood of calls to your customer support teams or giving your customers an opportunity to consider alternatives (read: your competitors). The outcome of your calculation will be different, but the key principles of how to calculate the value of DR are the same.

Common terminology

You probably use certain terms casually with your IT colleagues, but confusion reigns outside that inner circle when it comes to exact meanings. It's just a best practice to always clearly define what you are talking about to make sure everyone is on the same page. So here goes.

Backup is a vital component of data recovery. It is the creation of point-in-time copies of your data. That data could be unstructured or structured; it could be file-, block- or image-based. Each type of backup has its own pros and cons.

Business continuity (BC), also called "business resiliency," refers to an expansive form of data protection. It includes the restoration of data and IT services, just like in what we call "disaster recovery," but it also includes the processes and procedures taken to maintain business operations during a disaster.

Continuous data protection (CDP), also called "continuous backup" or "real-time backup," refers to data backup performed by automatically saving a copy of every change made to that data, enabling IT admins to restore data to virtually any point in time.

Disaster recovery (DR) is the series of steps taken to recover IT services after a disruptive event using the tools and techniques at your disposal. For the purpose of this e-book, we are referring specifically to the recovery of applications, data, network, IP telephone systems and all other technology necessary to conduct business.

High availability (HA) is a characteristic of technologies that can help your business continue to operate during a disaster. HA technologies provide redundancy of production systems so that if one fails, another can quickly "fail over" and take its place. It does not protect against corruption. High availability is intended to fulfill an entirely different need and, therefore, should not be considered a substitute for a robust DR strategy.

> To make business stakeholders aware of the urgency of disaster recovery requires a combination of technological prowess and business-leader thinking.

Replication is the process of copying data from one location to another, enabling IT admins to restore up-to-date data in the event of a disaster. Synchronous replication solutions write data to primary storage and to a replica site at the same time so that the primary copy and the replica are always in synch. Asynchronous replication solutions, on the other hand, write data first to primary storage and then copy that data to a replica site. Replication in this case often happens on a scheduled basis. Asynchronous replication costs less, requires less bandwidth and can happen over long distances. Synchronous replication, however, provides high availability of critical applications. Failover from the primary storage to the replica is nearly instantaneous, ensuring near-zero downtime to users.

BLURRY LINES

It's important to note that virtualization and modern backup solutions are blurring the lines between DR and business continuity. For example, many organizations are leveraging the two technologies to create "virtual standby" systems. Ideal for your most mission-critical application servers, this method minimizes downtime and data loss by keeping standby virtual machines (VMs) at the ready. The standby VMs are continually updated, and in the event of a disaster, they can be rolled back to any point in time and temporarily assume the role of the production server. When the primary machine is restored, users are then able to fail back with all the changes that were sent to the standby VM.

Conclusion

When you consider the stakes involved, it's clear that, despite not increasing top-line revenue or reducing cost, disaster recovery is absolutely essential to the business. To make other stakeholders aware of the urgency of DR requires the perfect combination of technological prowess and business-leader thinking. That's where you come in.

ABOUT QUEST

At Quest, our purpose is to solve complex problems with simple solutions. We accomplish this with a philosophy focused on great products, great service and an overall goal of being simple to do business with. Our vision is to deliver technology that eliminates the need to choose between efficiency and effectiveness, which means you and your organization can spend less time on IT administration and more time on business innovation.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (www.quest.com) for regional and international office information.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at www.quest.com/legal

Trademarks

Quest and the Quest logo are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit www.quest.com/legal/trademark-information.aspx. All other trademarks are property of their respective owners.