# How Much Downtime Can You Really Afford?

## Painting the Picture...

There's no question that data is the lifeline of the modern business, and without access to it for even a minimal amount of time can devastate the bottom line. But how costly is it really?

To really understand the impact, we don't have to look far beyond recent headlines:

- In March of 2015, iTunes and Apple Store outages caused by a configuration mistake made on an internal DNS cost Apple an estimated $25 million in lost revenue in just 12 hours. (Source: Tech Times)
- Google's Cloud Platform services were down for a mere 18 minutes on April 11, 2016, costing the company millions when they offered affected customers service credits for 10% of their monthly Google Compute Engine charges and 25% of their monthly VPN charges. (Source: CRN)
- On May 10, 2016, SaaS giant, Salesforce.com, experienced a huge outage that wiped out 4 hours of customers' data. The outage was linked to a database failure on one of Salesforce's 45 cloud instances, specifically NA14, which promoted a social media storm using the hashtag NA14. Salesforce would not release the number of customers or organizations affected by the outage, but using Twitter as a gauge, it was a significant and incredibly damaging to Salesforce's reputation. (Source: CMS Wire)
- On August 8, 2016, Delta Airlines lost power at its operations center in Atlanta, causing their booking system to go down for almost 5 hours. They had to cancel about 1,000 flights that day, and an additional 1,000 flights over the two days that followed. To appease their angry customers, they gave travel vouchers for future dates, further costing them money. All in all, Delta said the total bill for their downtime was $150 million. (Source: CNNTech)

It's not a matter of if something will happen, it's a matter of when. To be truly effective, disaster planning needs to be looked at closely as a key part of IT strategy, not just an afterthought.

These are just a few examples of what happens when mission-critical IT infrastructure fails and backup systems don't kick in quickly enough, resulting in huge impact on the business' bottom line, not to mention the impact on customer satisfaction and reputation.

These incidents also bring to light the often aging infrastructure that power many businesses, leading to what could be preventable failures. Outdated technology and inadequate disaster recovery (DR) planning will lead to more failures if the proper steps aren't taken.

## What is your plan?

Obviously, avoiding an outage should be high on the list of priorities; however in case of an outage, DR and business continuity (BC) plans can save the business tremendous heartburn. Upfront planning and investment in infrastructure can help organizations avoid, or at least more quickly recover from downtime.

OneNeck® IT SOLUTIONS
a TDS® Company

To prevent avoidable failures, it is key to thoroughly evaluate disaster recovery plans and build redundancy into the infrastructure supporting the business. Taking time to walk through potential failure scenarios and auditing the effectiveness of existing systems can also help avoid disaster.

So, what should you consider when developing your plan?

- Adopt a No-blame Culture: Blogger, Greg Ferro recently tweeted, "Reward firefighting and you will create a culture of arsonists." What does this mean? Gartner puts it this way, "Organizations should reward people based on the problems they prevent, not the problem they fix." This is a culture shift for traditional IT, but by taking this approach, IT is motivated to proactively identify vulnerabilities and automate processes that remove higher potential for human error.
- Off-site Backup and Storage: Any disaster that threatens a business is likely to make access to on-site data impossible. From the onset, security during the backup and accessibility following a crisis must be considered. There's no point to creating a backup if the data is not transferred via a secure method and stored in an offsite data center with concurrently-maintainable design. In addition, when developing a backup plan, it is key to determine a recovery point objective (RPO), which is the time between the last available backup and when a disruption could potentially occur. The RPO is based on tolerance for loss of data and helps determine how often a backup should be made.
- Develop a DR Plan: Developing a DR plan can be overwhelming, so it's important to remember not to attempt to boil the ocean. Start small with the basics, then add on over time. To begin, define what is important to keep the business running and the recovery time objective (i.e., how quickly the company needs to be up and running after a disaster). Additional considerations are designating who declares a disaster, the process to inform employees that a disaster has occurred, and how customers will be informed and reassured.
- Develop a BC Plan: To give your organization the best shot at success during a disaster, you need to put a current, tested plan in the hands of every person responsible for carrying out any part of that plan. The BC plan outlines procedures and instructions an organization must follow in the face of a disaster, such as business processes, assets, human resources, business partners and more. It's also important to remember that a DR plan is a part of the BC plan; so alignment with IT is crucial.

## An Ounce of Prevention...

Obviously, preventing an outage is the number one way to avoid the costly impact of one. The sure solution is to partner with somebody whose primary responsibility is monitoring and protecting your critical data and applications. Rather than adding these responsibilities to your already-overworked IT staff, consider contracting with someone who can actually prevent outages, not just fix them, a partner who will help manage, monitor and maintain your infrastructure.

If you're looking for that partner who will take the time to become intimately acquainted with your IT infrastructure and house it in a top-tier data center, we'd love to show you how we can help. Our concurrently-maintainable facilities provide colocation and customizable data and cloud storage options — all with no down time.

With OneNeck's managed services, you get a turnkey, full-service IT solution that includes the highly-certified experts, live 24/7 US-based support, SSAE 16 compliant, tested and proven ITIL best practices in IT managed hosting and world-class technology. All of this is wrapped in a high availability service level agreement (SLA) that financially guarantees your satisfaction.

So, take the worry about the costly impact of downtime out of the equation, and start preparing now.

OneNeck® IT SOLUTIONS
*a TDS® Company*

Part #01.1.3_ARDR_0207_v1