DISASTER RECOVERY and the CLOUD

A Primer to What You Need to Know About Protecting Your Business Data with the Cloud

ARE YOU READY?
Before we dive in, answer this question first, “What would happen to your business in the event of a natural disaster, or a cyber attack, or if a human or mechanical error wiped out ALL your company data?” There was a time when we laid awake nights worrying about these scenarios. Thanks to hurricane Sandy our fears became reality for thousands of businesses (some of our customers and friends)!

In today’s world of 24x7 business requirements, few companies (large or small) can afford downtime. Business technology availability and productivity are constantly growing priorities, yet most businesses are not allocating proper time, attention, and resources to prevent potentially catastrophic downtime. Some businesses that understand this risk have taken steps to protect themselves but are using traditional models for recovery that are proving too expensive, too time-consuming, or to antiquated to meet today’s more aggressive recovery objectives.
THE DILEMMA

Data disasters come in all shapes and sizes. You always hear about the biggies like hurricane Katrina, hurricane Sandy, Midwest tornadoes, southwest wildfires, west coast earthquakes, etc…. But what about the common everyday threats like hardware and software failure, infrastructure failure, human error(s), and the newest threats; hacking and cyber attacks.

It’s said, “your list is your gold” and we agree but equally if not more important is the gold found in your business data. Your business data is the asset that drives your business decisions that grows your business. Think about it, what would you do if your contact info (names, address, emails, phone numbers, billing info, etc…) was lost? What would you do if all your vendor or product information was wiped out? Most business don’t recover from this type of loss unless they’ve taken the right steps to protect themselves.
WHAT IS BUSINESS CONTINUITY


Wikipedia defines Business Continuity as encompassing a loosely defined set of planning, preparatory and related activities which are intended to ensure that an organization’s critical business functions will either continue to operate despite serious incidents or disasters that might otherwise
have interrupted them, or will be recovered to an operational state within a reasonably short period.

We believe Business Continuity (BC) is also defined as the capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident. This guide specifically addresses Disaster Recovery and Business Continuity in relation to the data used to run your business through interruptions of any kind including human errors, hardware failures, IT system crashes, natural disasters, supply chain problems and more.

You might say, “I have insurance for those things.” In reality, Insurance helps you financially and Business Continuity helps you operationally. Insurance covers your financial loss in the event of a disruption but may take months before you receive your compensation. What happens to your business in the meantime? What happens to your suppliers and customers? What happens to your employees?

Business insurance will recover your expenses for your tangible assets (like computers, servers, desks etc…) but it will not recover your intangible assets like business data, vendor data, product data, customer data, etc… data that you have gathered over years etc. Those assets are more
important for sustaining your business than the tangible assets like hardware.

Business continuity (on the other hand) allows you to continue stakeholder expectations long after the disruption has taken place. Business continuity protects your revenue, your reputation, and your market share (things that insurance can’t protect). Insurance may help financially but Business Continuity acts as your operational safety net.
WHAT ARE THE RISKS OF DOWNTIME

Not all downtime is the same. The cost to the company and the value of lost data varies depending on a multitude of factors. Something as simple (yet troublesome) as the loss of customer history takes time to recover but can be reentered (as long as copies exist) by lower skilled and lower paid personnel. At the other end of the data loss spectrum, the loss of custom code could be significant. Numerous studies and reports cite that companies experiencing data loss of just 10-days never fully recover and usually end up shutting their doors within 5 years! We ask again, “what would happen if you lost access to your data?”
According to headline news, natural disasters account for most of IT and business downtime while in reality most IT and business downtime come from accidents, sabotage, and technical failures. Additionally, most data-loss events and outages are due to the failure of single hard-disk drives, machines, or servers. Simply put, mechanical things break over time.

IT and business outages like these reinforce the critical importance of having a thorough disaster recovery (DR) and business continuity (BC) plan in place so your organization can rapidly recover from data-loss events and resume business operations as quickly as possible. Since the survival of a business depends on rapid BC, failure to develop a business continuity and disaster recovery plan can result in lost productivity, customers, and revenue as well as decreases in customer satisfaction, sales, reputation, stock price and in worst case scenarios your business!
WHY DATA BACKUP AND DISASTER RECOVERY IS IMPORTANT

Data growth is a growing necessity for most businesses. Think about it, do the systems you depend on demand larger hard drive space each year? Are you collecting more data on existing clients? Is your client base growing? What about the data you collect and use as a resource pertaining to your products and vendors? These questions and more speak to data growth and its increasing size demand.
With the unpredictableness of natural disasters and the increasing manmade threats, proper data protection, backup and disaster recovery are critical for any business (from small one person shops to large enterprises), most folks however are unaware of their susceptibility. Those that have taken steps to protect themselves from data loss disasters are still using traditional (antiquated) devices such as external hard drives and tape backups.

Data loss is an inevitable reality for businesses and their IT departments. According to well-regarded published research about real-world data-loss events and their consequences on businesses, here are some hard facts:

- 25 percent of personal computers are forecasted to fail each year.
- 24 percent of all companies will experience a complete data loss each calendar year.
- Among those companies that experience a complete data loss, 70 percent will go out of business within the first year of that data-loss event.
- Companies that experience a significant data loss will need an average of 30 hours to recover.

The estimated cost of downtime for a small to mid-sized company is tens of thousands of dollars per hour. And, the average cost of data loss to a small- and medium-sized
business can run into the millions for each data-loss event. Remember the intangible costs, which can be even greater, come from lost productivity, lost customers, impact on reputation, falling stock price, etc. These numbers further support how critical BC planning is for rapid recovery from a data-loss event.
FIVE REASONS WHY TRADITIONAL BACKUP DOESN’T WORK ANYMORE

1. **Costs** – data growth is a reality at most companies. The more data employees create, the more data you have to backup. Other reasons companies see rising backup costs are annual maintenance fees, having to add protection
for remote offices, and more time the IT staff has to spend maintaining and verifying backups.

2. **Capability** – traditional backup does not provide sufficient protection. With IT environments becoming increasingly complex – with virtualization, different operating systems, and applications – traditional backup is lacking in functionality and in protection options. For example, companies are realizing that in the case of a disaster, the restore does not happen quickly enough and it cannot protect all of your data types or locations.

3. **Complexity** – traditional backup vendors have been trying to fill gaps in protection by adding new features or integrating with other products, which adds complexity. Just look at most user interfaces and also at how much time most IT professionals have to spend monitoring and verifying backups. Does your solution take too much effort, man power and expertise to get up and running? People are looking for increasingly simple, yet powerful tools to help them keep their business running.

4. **Completeness** – more and more companies today are realizing that legacy systems and players can’t innovate and are looking for those who can keep up with their IT systems. If your backup vendor has a product created more than just ten years ago and is simply adding on top
of that layer of obsolete code, how can you rely on them to keep up with advances in technology?

5. **Customer Support** – the very nature of traditional backup points toward problems in the support side as well. Companies are increasingly frustrated with long on-hold wait times, multiple escalations, and unresolved issues when it comes to their backup products. Having to deal with multiple vendors also adds to the problem as finger-pointing becomes rampant.
WHAT IS THE CLOUD?

Our friends at Wikipedia define “the Cloud” internet-based computing in which large groups of remote servers are networked to allow centralized data storage, and online access to computer services or resources.

An easier and simpler way to think of the cloud is software and services that run on the internet instead of on your computers. If you have used Apple iCloud, Amazon Cloud Drive, Amazon Prime, Box, Dropbox, Google Drive, Netflix, etc… you have already experienced the cloud! Businesses of
all shapes, sizes and industries are increasingly ditching their internal servers and software in favor of cloud-based ones.

Cloud computing offers businesses many benefits. It allows you to set up what is essentially a virtual office to give you the flexibility of connecting to your business anywhere, anytime providing the data recovery component to your overall business continuity plan. With the growing number of web-enabled devices used in today’s business environment (e.g. smartphones, tablets), access to your data is even easier. There are many benefits to moving your business to the cloud:

- Reduced IT Costs
- Deployment Time Decreased from Years to Months
- Improved Information Security
- Scalability
- Business Continuity
- Collaboration Efficiency
- Flexibility of Work Practices
- Access to Automatic Updates

Over the past few years, Disaster Recovery as a Service (DRaaS) has received a lot of media attention and experienced significant growth. More and more Infrastructure and Operations professionals are looking for ways to improve their recovery objectives without increasing costs. Using
DRaaS means the organization doesn’t have to invest in -- and maintain -- their own off-site DR environment. An additional benefit is that DRaaS contracts can be flexible as the business’ needs change. But keep in mind, one size DRaaS does not fit all.

During the past several years, a slew of DRaaS offerings have come to market with the promise of faster recovery in the cloud at the same or lower price points and more flexible contract terms compared with traditional recovery methods. While this may sound too good to be true, many who have taken the plunge report that these claims are not as far-fetched as they seemed at first glance. But just like downtime, not all services and providers are the same.
DATA BACKUP IS NOT DISASTER RECOVERY

We’re often asked “do I really need disaster recovery if I have a data backup system.” The answer is, “it depends but most of the time yes.” Data backup and disaster recovery are not the same. Backup software and hardware can and does fail. Sometimes, the person responsible for backing up can fail. Also, backing up without recovery in mind is practically the same as not backing up at all especially if you don’t take the time to identify the right people, processes, and tools necessary to recover your data and put it back online successfully.

With today’s technologies, Disaster Recovery can practically recover your systems to the state before the disaster occurs.
SO, WHY THE CLOUD

At NSA Computer Exchange, we’ve been helping wholesale distributors and businesses manage their data for over 30 years. We’ve seen and fixed lots of failed software and hardware implementation exercises. At the same time, we are constantly looking for better strategies, tactics, tools and services to bring to our clients.

As technology becomes an increasingly important of business, many companies are looking for solutions that will provide the most advantages for the least amount of money, time and complexity. In conjunction, we know and
understand the critical importance Data Disaster Recovery has on Business Continuity. A cloud based monitoring and disaster recovery service should provide the following benefits (at a minimum):

- **Cost-Effectiveness**

  The costs of traditional disaster recovery solutions can force you to make tradeoffs on what you can afford to protect versus what you need to protect. This can leave your organization vulnerable to having inadequate protection. Disaster Recovery addresses variable capacity requirements needed to support common DR use cases, such as replication, failover, and recovery, at a significantly reduced price point over traditional in-house disaster recovery solutions or managed service alternatives. You have the scalability to accommodate shifting requirements, you pay only for what you need, and you have flexible subscription options.

  In addition, backing up data can be extremely expensive, especially when considering the necessary equipment and hardware. Labor costs become an issue too, as manual backups are time-consuming and complicated. Cloud storage solves these problems by leaving the maintenance and equipment costs to a third party provider. Cloud storage solutions are easily scaled, allowing businesses to only pay for the amount of
storage necessary for their business and making it simple to increase or reduce space as customer needs change.

**Ease of Getting Started**
Deploying and managing a traditional disaster recovery plan can be complex and require time, budget, and staff that you may not have. Disaster Recovery provides an easy way to get started with an effective disaster recovery plan—without hiring and training new specialists, and without having to invest in a secondary site. The service provides a simple, secure, automated process for monitoring, replicating and recovering applications and data in the case of a local disaster or disruptive event.

**Security**
Storing information in the cloud is much more secure than keeping paper documents or using physical devices for file storage. Hard drives and USBs can be stolen or lost, while information in the cloud will always stay put. At the same time, security is not a core competency for many companies, but it is for cloud service providers. Because of this, providers who are mainly focused on data security are much more adept at keeping information protected than a business with an IT team focused on dozens of projects and problems at once. Cloud storage also creates an extra layer of security between privileged data and cybercriminals. Backup files are kept separate from
originals so hackers cannot steal everything at once.

- **Protect files, folders, applications or entire systems**
  Your disaster recovery solution should protect not only your critical data, but also your applications and all systems in your IT environment. A strong backup and disaster recovery solution creates a fully-deduplicated mirror of your business locally and in the cloud so that you can easily access and recover files, folders, applications, servers and even your entire office with a click.

Since 1984 NSA Computer Exchange is a professional service organization that’s in the business of helping businesses. In our 30+ year history we’ve seen a lot and done a lot. We believe our consultants and programmers can do anything. We pride ourselves on our commitment to professionalism and personal service, availability, truth, cohesive partnerships, and keeping our promises. We believe this is confirmed by the volume of service requests we receive by companies preferring to partner with us versus their primary service providers. With our vast business experience, we bring more than technical ability and know to the table.

If you or your company are considering implementing or upgrading your business continuity plan with an emphasis on backup and data recovery add our team of consultants and programmers to your research and due diligence.
Contact us for a no commitment, no obligation demonstration of the NSA Axcient Solution.

Pat VanPutte, President
NSA Computer Exchange Corp.
270H Duffy Avenue
Hicksville, NY 11801
Phone: 516.240.6020
Email: pvanputte@nsacom.com

Office Locations (U.S.):
Ashville, NC
Binghamton, NY
Buffalo, NY
Colorado Springs, CO
Hudson Valley, NY
Parkland, FL