7 Critical Ways to Protect Your Business from Data (and Financial) Loss

RANDGROUP

Disclaimer

The information contained within this whitepaper is the opinion of the author and in no way represents the opinion of The Rand Group, LLC. The information contained within should not be taken as legal or binding, and should be referred to as an opinion piece by a subject-matter expert.

About the Author

Lorenzo Fife is a Director of Infrastructure with over 12 years' experience helping organizations plan and manage their technology platforms to leverage them for success.

Lorenzo has spent several years of mentoring and grooming IT teams focused on working with businesses in the manufacturing, retail and energy sectors. He has helped several organizations grow exponentially through the application of cloud and hybrid cloud solutions, better IT strategies, infrastructure planning, and performance optimization. With a dedication to enabling seamless transitions, Lorenzo has overseen several company mergers and acquisitions, the development and implementation of software solutions and integration of 3rd party applications, as well as consolidation of resources for improved efficiencies. Respected for his ability to understand and identify the real business issues, he has a proven track record of making precise decisions and taking quick action to positively affect business drivers. Over the course of his career, Lorenzo has enabled companies to significantly reduce overall IT expenditures while improving management, end-user, and client side satisfaction.

Lorenzo is a Microsoft Certified Systems Analyst and Systems Engineer, a VMWARE VSphere Certified Professional, an EC-Council Certified Security Analyst, Certified Systems Hacker and Licensed Penetration Tester, and is an ISACA Certified Information Systems Auditor.

Whether you have dedicated staff or contract out your IT requirements, having someone in charge of your technology epicenter can lull executives into a false sense of security. Even in large organizations that have someone available 24/7 to deal with things like email outages or data loss, making an assumption about the safety and security of your data can have nasty consequences. You want your business to run optimally, and you need it to quickly recover from any type of data loss so you don't lose time, money and the confidence of your customers and clients.

It's estimated that in the United States alone, data loss costs organizations $12 billion dollars a year and facilitates the existence of an entire data recovery industry .* Your data is the single biggest asset your company possesses. If you were to lose everything else but retain your data, you would be able to continue operations and recover your business. Conversely, in 60% of the cases, companies that lose all their data face bankruptcy within six months.**

In 78% of cases, complete data loss – including financial records, accounting, order history, inventory, payroll, contacts, vendors, clients and more – is the direct result of a hardware or software failure, which means protecting your data should be a top executive priority.*

In today's data-centric, 24/7 operations, businesses run mission critical applications while simultaneously generating a bounty of user-data. With so much company data to manage, it's important to re-think the way it's being handled. It's not enough to stay the course with your old solution because it "hasn't failed you yet". Today's business environment demands that you contemplate the risks of stagnation and complacency in data protection, and consider how to move your business ahead.

As every IT professional will tell you, it's never a matter of if something will fail, only a matter of when. Assuming that automated back-ups are occurring at regular intervals is not sufficient. Even if your system is working, the set-up itself could be flawed. You need a clear picture of exactly how your data is being handled, with insight into your core infrastructure, and you need to consider all your data sources, and the impact each has on your business.

So ask yourself, do you really know everything you need to know about the security and reliability of your data?

The following will help you identify the Top 7 questions to ask yourself about your data, so you can better protect your business.

* *http://www.datarecoverylabs.com/how-often-should-you-backup-your-files.html*

** *http://beyondtechnology.com.au/drstats*

1 - How many transactions would you lose if you had to recover from your data back-up?

Say you lost everything on a Thursday afternoon, what would that look like for your business? If your back-ups are only being performed on a weekly basis, what impact would that have on you? Do you even know?

Start by considering your volume of transactions. From client interactions and orders through to inventory management and compliance reporting, how many pieces of data are processed through your organization on a daily basis? Further, how many of those transactions are considered critical, versus something like emails exchanged?

Once you've determined the volume, start to imagine what recovery would involve. Could you fulfill orders or meet your service level agreements if you lost an entire week of data?

How many transactions with clients would be lost between scheduled back-ups, and what would the recovery from that look like? Would you even know where to start in terms of fulfilling orders or tracking time and materials to jobs in progress?

You need to know the answer to these questions before you can be certain your current back-up process will meet your company needs. If you can't afford to lose 48+ hours' worth of interactions (and most likely you can't), then what is reasonable for your organization? Determining the level of productivity lost based on your current back-up schedule will help you determine the schedule you should actually be on.

2 – How are your back-ups prioritized?

All data is not created equal, and assuming that everything should be treated with the same level of priority and importance will make contemplating your backup strategy overwhelming. You need to consider the priority of what gets backed up, and when.

A lot of data is exchanged on any given day, and it may not be feasible or imperative that you back up all of the information at the same frequency. Back-ups should be prioritized in the order of maintaining the highest level operations should something go wrong. Figure out the crown jewels of your data exchange and focus more attention on protecting those data sources than other less imperative ones.

To optimize your back-ups, prioritize your business units. This will enable you to develop different levels of back-ups to meet your needs. Critical data, like transactions within your ERP system or across your SQL server, can be backed up with more consistency and stored to meet regulatory requirements, while things like email exchanges and documents can be backed up less frequently with copies kept for a shorter duration.

By prioritizing your data into categories based on how crucial they are to the operations and compliance of your business, you're able to develop an easier to manage, more cost effective data solution. This will enable you to instantly recover mission critical data and applications in the event of a loss, without wasting time sorting through items which hold less overall value. Financial data and pending orders are of a higher priority to a recovering business than last month's accounts payable records.

3 – What is your technology business continuity plan?

Consider your current back-up and recovery situation: are you confident enough in the set-up to put your business on the line for it? If you didn't answer an emphatic yes, it's time to reconsider your plan.

You should have a business continuity plan that lays out how you will resume operations should you suffer an unexpected event which creates widespread loss of your data. The plan should include how to handle the emergency from an operational standpoint, and that includes disaster recovery and continuity.

You may believe you have a plan; it may even exist in your organization, but when was the last time it was audited? Businesses change every day, and with growth and a data-centric environment, the plan you put together last year is unlikely to suffice today. Your business continuity plan should evolve, the same way business planning does – to keep up with your current state organization.

Consider this: ***IDC says that in 2011 we created 1.8 zettabytes (or 1.8 trillion GBs) of information. In 2012 it reached 2.8 zettabytes and IDC now forecasts that we will generate 40 zettabytes (ZB) by 2020.***

Your business plays a role in that, and while it may be a small piece of that pie, it's your whole world.

Even in the event of a disaster, you can't afford to be offline for long periods of time. You owe your staff and customers more than that. Your business continuity plan must include direction on how to get things like payroll up and running, so you can take care of the people who take care of you. Further, it's imperative that this plan be both easy to understand and easy to access. There is no use developing a complex plan that is stored alongside your other on-site data, rendering it useless in the event it's actually needed.

Multiple copies, in multiple locations that can be accessed by a set of people designated to manage disaster recovery is vital.

4 – How well do you know your metrics?

Part of your business continuity plan should include metrics such as the recovery time objective (or RTO) and the recovery point objective (or RPO); if you don't know what those are, you don't know your metrics and recovery plan well enough.

Recovery Time Objective

The RTO is the measure of how long your business can be down following a disaster or data loss, before you must resume a certain level of service. This is the point at which you'll start to experience an unacceptable level of repercussions (usually profit and financial loss) from which your business cannot easily recover. The grace period for your business depends extensively on the type of operation you run and the customer or clients you serve. An RTO is expressed in a measure of seconds, minutes, hours, or days.

Multiple studies have been conducted that try to determine the total cost of downtime for certain applications and enterprises; however it's difficult to quantify on a general scale. This is due to the combination of short and long term consequences, as well as tangible and intangible effects. Your IT team should help define the acceptable RTO for your applications and data, which will in turn help drive decisions on back-up scheduling and storage options.

Recovery Point Objective

This is another critical metric for you to evaluate. The recovery point objective (or RPO) identifies the age of recovery for your retrieved data. In other words, how far back should your recovery reach in order to keep you operable, or what is the maximum amount of data you can stand to lose?

Your RPO is expressed in past tense, from the moment a failure occurs and can be specified in seconds, minutes, hours or days. Your IT team should help define the acceptable RPO for your applications and data, which will in turn help drive decisions on back-up scheduling and storage options.

Recovery Level Objective

The final metric for your business continuity or disaster recovery planning defines the granularity with which you must be able to recover. Do you need to be able to recover the entire server farm, or will only specific servers suffice to keep you operational? Do you need to recover primary and secondary application servers, or will one of the two be enough to serve the application adequately?

Your executive team should work in conjunction with your IT department to finalize your RTO, RPO and RLO and ensure it meets your business needs.

5 – Do you have a 3-2-1 Plan?

If you don't know what that means, the answer is probably not.

The 3-2-1 Backup Rule relates to how and where you store backed up data.

Widely known but painfully underutilized, the 3-2-1 Backup Rule was designed to help people and enterprises effectively secure their most important data. The principal is simple:

- Keep 3 copies of your data
- In 2 different formats
- With at least 1 copy off-site

It seems logical that you don't store your back-up in the same location as your central data but you'd be shocked to learn how often that happens. It's one thing to store a back-up at your desk in the event of a server failure, but what about a flood or fire? Further, just because it leaves your office doesn't mean it's secure. Who takes the backup offsite, and where do they keep it? Is it secured correctly or is all your data at risk of getting lost, or worse, finding its way into the wrong hands?

The premise in all of this is based on redundancy. Too often people believe that the simple act of backing something up is enough to secure it. However, we know that multiple points of failure can occur, especially in the case of disaster when the physical equipment is wiped out. By adhering to the 3-2-1 Rule, you can better secure your data and your business.

Keep 3 Copies:

This means three copies of the same data, in three different places. Creating digital copies is simple, and the more you have the better it is. If you keep three copies in different places, you significantly reduce the chances of losing access to all your files.

In 2 different formats:

Much like keeping 3 copies, you want to keep information in different formats. There are pros and cons to each data format, and by ensuring you're using at least two types, you further reduce the risk of losing access. For example, this means using a combination of disk and hard drive, not simply using 2 different hard drives.

Keep 1 Offsite:

Ideally you use a tape or disk back-up to keep at least one version of your data offsite. This will provide immunity against total data loss should your physical site be affected by some sort of disaster. This will also help protect against data theft, or loss of data should the staff member responsible for your back-ups decide not to return to work one day. This offsite data should be kept somewhere secure and updated with regularity.

Cloud services provide an excellent option for fulfilling a portion of each of these rules. Cloud storage counts as 1 copy, in 1 format and can be your offsite location. However, it's good to be aware that cloud services still have risks of their own, and should not be counted as your single data source. Cloud services do make the process of frequent back-ups simpler, by allowing automation and offsite storage to occur with very little intervention. However, the cloud is not immune to risk, so don't rely exclusively on one cloud location to host all of your data.

6 – How reliable and available is your data?

It is one thing to back-up your data and another thing to access it. If you're storing your data offsite, do you know how long it would take you to retrieve your full data set in the event of a systems failure? Is there a protocol in place for dealing with data recovery? How much time can you afford to spend trying to retrieve your data before you start the process of recovering from a complete or even partial loss of critical information?

Data availability, or data accessibility, is another part of data redundancy. Backing up your files is critical to your business success, but availability is just as important.

Data storage and availability comes in multiple forms, each with its own role to play in your data strategy. There are two primary external data storage methods that offer available data: a SAN system and a NAS system:

- A SAN system, or storage area network, can offer shared storage, and allow for servers to boot directly from the SAN. This means quick and easy replacement if your server fails. Additionally, in the event of a disaster, SANs can be configured to access a distant location where your secondary data is stored, via an IP network.
- A NAS system, or network-attached storage, is a dedicated file storage device the users connect to via a LAN connection. Each device acts as an independent network device and is assigned its own IP address, offering substantially more storage space than the local drive or server could accommodate. NAS offers easy to deploy, multiple file system storage for your back-ups that can be simply accessed in the event of a failure.

There is also a RAID system, which can help you improve your data availability. RAID's, or redundant array of independent disks, while nothing new or extraordinary, offer different levels for performance and accessibility for different environments and cases. To determine your RAID needs, you will have to consider costs, performance and data availability requirements, capacity and your organizational goals.

The RAID system doesn't replace the offsite and scheduled back-ups we've been discussing, but can help you build your arsenal for redundancy. The RAID will help protect and maintain the data on your primary storage system, such as the server or hard drive, and when combines with a reliable back-up strategy can give you end to end accessibility.

7 – When was the last time you actually saw a successfully completed back-up?

Can you answer this question with certainty? If you haven't recently audited the complete back-up, how can you have total faith in its completeness and availability?

The best laid plans can sometimes fail, and it's not enough to believe in your back-up system. You must put the time and effort into verifying that it works. A back-up audit is a crucial part of every IT strategy, and should not be ignored. Your back-up and recovery plan should include periodic back-up audits, which will help you ensure you can recover in the event of disaster.

Back-up audits don't need to be complex, they just need to be conducted. The basic steps in a back-up audit include:

1. **Review:** assess and confirm the files that you want to back-up. As your business progresses and things change, so should your back-up strategy. Confirm the files you're backing up, review the frequency and determine if changes need to be made to further protect your business. Also consider if there are files that no longer need to be backed-up, or no longer need to be backed-up with the same regularity.

2. **Test:** You don't want to find out you cannot restore your files from your back-up when it's too late. Pick a selection of files at random and determine your ability to restore from them. Ensure the time and data set match both your Recovery Point Objective and Recovery Time Objective that was discussed previously.
3. **Inform:** Be sure everyone knows which folders are backed up and which aren't. With the constant evolution of your business and the changes in staff, it's important that everyone realize which files are backed up, and which files aren't. Many companies don't back-up the local drives on everyone's PC and instead choose to back-up only the centralized server. If that's true for your company, ensure everyone knows not to store important information on their local hard drives.

You would be surprised how often this crucial part of the overall IT strategy is neglected. Nothing is fail safe, and if you're not reviewing your protocols and ensuring your data is accessible and recoverable when you need it, you're bound to find out the hard way when it's not.

You're Nothing Without Your Data

All too often, IT departments, companies and professionals are left to their own devices, blindly trusted by the executive charged with ensuring the business is properly protected. Technology can be confusing to even the savviest individual, and managing your IT professionals can seem overwhelming. That said, in order to truly protect data, one of the most valuable and pertinent assets in your organization, you must stay on top of how it's managed and handled. While many IT professionals cover the full gamut of what we've reviewed today, some are missing critical steps in the overall plan. This is not an area in which you want to learn the hard way.

Our team of highly specialized IT professionals is available to help you get a better understanding of your current technology environment and how to best protect yourself from a devastating loss.

Security is only a phone call away: 866-714-8422

RANDGROUP

Test Your Backup Health

You want to avoid data loss, but do you know your current state? Take our 30-second Backup Health Quiz and see — the answer might just surprise you.

And if you're in shock, we're here to help ease the strain by guiding you through an effective back-up and recovery strategy.

You have everything to lose. Protect yourself. And your business.

TEST MY BACKUP NOW

RANDGROUP

About Rand Group

Rand Group is a professional services firm that serves the oil and gas, manufacturing, distribution, and construction segments within the state of Texas. Rand Group combines the business acumen of CPAs and industry specialists with the technology expertise of software developers and process improvement specialists to drive real business results utilizing technology. Consistently the fastest growing application partner in the US domestic market, Rand Group has built a reputation of making systems work for business.

Rand Group. ***Software Delivered as Promised. No Surprises.***

For more information please visit www.randgroup.com.