The DynaSis Educational Series for C-Level Executives

Cloud Backup & Disaster Recovery

"The Towering Inferno"

"Earthquake"

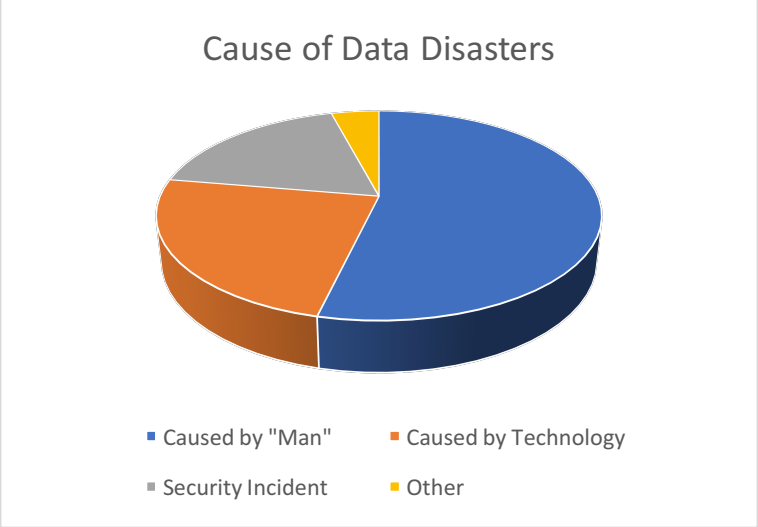
"San Andreas"

"Volcano"

We all love a good disaster. As long as it's not real. And especially if it doesn't happen to us. These movies show some pretty spectacular imagery that really gets your blood rushing. But as you probably guessed by now, today we are going to talk about an entirely different type of disaster…the kind that happens when your company's files disappear, or are rendered useless, or are stolen. In some cases, this business disaster may be the result of one of the above "natural" disasters, but recent history shows us that the vast majority of data disasters, whether intentional or accidental, are man-made and/or man-preventable. But regardless of how it happens, data disasters are real and must be dealt with quickly, completely and accurately. How do they happen? Here is a breakdown (chart on next page.):

65% Human Error
29% Technology Incident
22% Security Incident
5% Other

Let's start with a look at some of the worst data loss disasters in recent memory. We say "some" of the worst, because there have been far more than we could possibly mention here, and people will disagree about how bad is bad.



The Government of the United Kingdom Loses Its Data on EVERY Criminal in the Country.

The key word here is "loses". In this context, it doesn't mean that the data disappeared from the British government. No, it means that all these records were transferred by an employee onto a memory stick (aka flash drive), and then the employee literally lost it. This happened in 2009 and included all the records of more than 40,000 bad guys convicted for serious felonies, but also included the home addresses and personal information of everyone in the prison system.

Remember Ma.Gnolia? Here is why it's not around anymore.

If you don't remember Ma.Gnolia, it was a quickly growing bookmarking site that gave it's users the ability to bookmark favorite sites and share their bookmarks with other users. It was truly a pioneer with unique technology and was expected to become a major player. Until disaster struck. In a complete outage, their servers lost 100% of their data, including their on-site backup, which was corrupted, as well. The site was effectively dead and not too long after, so was the company. Afterwards, their CEO admitted that offsite backup with proper backup software would have saved the company.

US Government Loses Data on 26 Million Veterans.

Here's one for those of you who work for (or own) companies that allow BYOD (bring your own device). With people working from the office, from home, and on the road, employees who use their own laptops, smartphone and tablets have become more and more common. It's easier for the employee than having two of everything – two phones, two laptops, etc. – and cheaper for the employer. While this one happened a few years ago (2006), the lesson rings true today. A data analyst working for the Department of Veterans Affairs had his laptop stolen from his house. Unfortunate in itself, but he just happened to have the records of 26,500,000 military veterans on the device. The laptop was recovered (after paying a $50,000 reward) but follow-up lawsuits cost the government more than $20,000,000.

A couple more quickies:

When the database of the **US consulate** crashed in 2014, more than 200,000 visas for people from

around the world were put on hold. The data had been backed up, but the system that crashed was not. Issuance of visas ground to a halt. This disaster was caused by a simple patch that didn't work properly.

In 2015, a computer security researcher found a **database containing the personal information on 191,000,000 voters** from all 50 states. Included were their party affiliations, phone numbers, email addresses, and birth dates. This information was "out there" due to a database that was incorrectly configured.

And finally, here is one that could have been a disaster but was saved because one person **didn't** follow the rules. The entire almost complete film **Toy Story 2** was almost lost when one of Pixar's employees entered "remove all" and went click. An accident? We don't know. We do know that the only reason the film was not lost was because the film's technical director, who wanted to work from home, had transferred a copy of the entire film to her home computer, which, by the way, she was not supposed to do. Dilemma: does she get fired or is she a hero?

If you think these are isolated incidents, think again. Within the past year, almost half of IT pros at small to mid-sized companies have lost data and used backups to recover it, which is great when the backup data is intact and retrievable. To ensure that it is, a little more than half of those surveyed stated that they are using a hybrid approach to backing up – on premise and off (we will get to exactly what that means in a little while.) But what about the other half? Our opinion: they are opening themselves up to potential disaster. (Please note: just because you are backing up off-premises doesn't automatically mean you are doing it right. It still needs to be performed correctly.)

Like most things in the IT world, backup and disaster recovery are changing at a rapid pace, and most modern companies are at least taking a hard look at off-site cloud backup. (Another note: files can be backed up offsite without the cloud. Some organizations routinely backup their files to tape or disks, then transport these to an offsite secure storage facility for safekeeping.) Obviously, this becomes expensive and cumbersome when files need to be restored. We should also note that this method of file backup is shrinking in popularity, for obvious reasons, but an analysis of off-site storage wouldn't be complete without mentioning it.

Why has "off-site" more and more come to mean the cloud? There are several reasons:

- First, the cost of moving massive amounts of data has gone down quite dramatically.
- The speed of broadband has increased to the point where it is much more feasible to move large amounts of data on a daily basis.
- Storage costs for this data has also decreased.
- Storage is now highly scalable so as the amount of the data you want to store in the cloud increases, your storage capacity increases, although there is some cost for this.

You should also note that these days, hybrid backup is gaining momentum, meaning you store one backup copy on premises and one copy in the cloud (you should always have at least two backups, each stored a different location.) This makes perfect sense. It is more cost effective to have one backup copy

on-site, right at your fingertips, but keeping that second copy at a highly secure facility provides your company with a level of protection that couldn't be achieved (not cost effectively, anyway) by a small to mid-sized company on its own.

Cloud Security

Cloud security is a concern many people have. Perhaps it is natural to feel safer knowing that your data is stored on your own premises, right down the hall. And we agree that cloud security should not be taken for granted. Modern data facilities are highly secure, with temperature and humidity control, access control systems, power backups, multiple Internet providers, etc., etc. These are considerations you should be looking for if you are going to interview a cloud service on your own, as well as the functionality that will be available to your in-house IT if rapid recovery is ever needed.

Which brings up another point: this may be a great time to look into retaining the services of a managed IT support company that will be there 24 x 7 x 365 to make sure that your backups are running according to plan and, most importantly, to jump right in in the event of a needed recovery. Many mid-sized companies that have their own internal IT teams also engage an outsourced IT support company to run their backups and the monitoring of them. A first-class IT service company will monitor and maintain the system around the clock and will usually spot and fix "issues" before they become "problems". They also free up your people from mundane daily tasks, allowing them to focus on long-range planning and higher level projects.

If you have your own in-house IT team, they will certainly be heavily involved in the process of selecting the managed IT service provider and/or the data facility, and your service provider will usually report to them.

Disaster Recovery as a Service (DRaaS)

Disaster Recovery as a Service is a relatively new service that's appropriate to this discussion.

For some organizations, having off-site backup of files is only one part of an overall solution. Another important part is an off-site "disaster recovery site." Simply put, this means a second physical location where back-up servers are fully up-to-date and which, if and when a site disaster occurs, can be used to fully run the company's IT infrastructure. We are speaking about a disaster that not only makes files unusable, but also cripples your server(s). A second physical site, with all the costs associated with such a site, can be expensive to maintain, but the ability to quickly come back online can be critical to a company's survival. The question you have to ask yourself is, what would be the cost, in dollars and cents, in reputation, in lost customer base, in employee morale and loyalty, if your company's IT network was shut down even for a relatively short period of time. Without going into a lot of statistics, suffice it to say that the cost for many companies can be in the hundreds of thousands of dollars a day

and many never fully recover.

But another option is **Disaster Recovery as a Service**, a functionality under which your data would **not** be recovered to another server(s) at your disaster recovery site, but rather to a server(s) in the cloud, where all of the company's workloads could still function until normal operations were re-established. This is a great methodology for a company, particularly smaller ones, that need to be able to get up and running quickly in the event of a data disaster, but want to avoid the cost of maintaining a second office site. With DRaaS, the disaster recovery infrastructure and company workloads will exist in the cloud only for as long as they are needed. As soon as the permanent infrastructure and files are available, the temporary structures are removed and charges stop being incurred. Again, this is a functionality that may be best served through an outsourced managed IT support provider that has experience in this type of service.

Finally…

Backup and recovery in the cloud offers many advantages over traditional methods, such as keeping a second server in your office or physically moving backed up files onto tape or disk. As this statement implies, we believe that at least one off-site back-up copy of your data, along with an on-site backup, is an imperative. (That's 2 backups plus 1 original = 3 complete copies). On an even higher level, and important for certain companies that cannot withstand long downtimes, is Disaster Recover as a Service, especially as the software involved continues to improve making the functionality easier to implement.

We also believe that in today's world, with cyber-attacks on the rise, especially in terms of ransomware (see our white paper: Cyber Security 2017), the ability to rapidly lock out encrypted files so as to keep infections from spreading, and the ability to quickly recover lost, stolen or damaged files is paramount. (See our Case Study: A Tale of Two Cyber-Attacks.) The key to successfully implementing such a program for most small to mid-sized businesses is finding the right IT partner, a managed services company that can provide an un-biased risk assessment, and then work within your security requirements, budget and level of comfort.

One final anecdote: this may be shocking to millennials, but at one time, data was actually stored in these paper things called "books", and before that on scrolls. In Alexandria, Egypt, there were about 500,000 irreplaceable scrolls containing advanced works of mathematics, physics, astronomy, poetry and more, all stored in the library of Alexandria. In 300 BC, the library burned down, taking all 500,000 scrolls with it. This was history's first recorded data loss, and with no backups, all this knowledge was lost. Had there been a second set of scrolls stored elsewhere, we might not even remember the event.

Since 1992, DynaSis has been at the forefront of managed IT service, taking the lead in developing IT security measures now used across the nation. We provide complimentary IT Assessments that include Risk Assessment. If you believe that your company might benefit from such an analysis, please give us a call, or fill out the form. We'd love to chat!