WHITE PAPER

A white paper by Colin Bell, Timico's Director of Cloud and Hosting.

Is your Disaster Recovery plan bullet-proof?

How to spot common vulnerabilities in your DR plan and fix them with little impact on you, your business and your customers.

timico®
connect · host · manage

Is your Disaster Recovery plan bullet-proof?

How to spot common vulnerabilities in your DR plan and fix them with little impact on you, your business and your customers.

A white paper by Colin Bell, Timico's Director of Cloud and Hosting.

Executive summary

As dependency on technology continues to increase across all market sectors, it is essential that IT departments have a bullet-proof plan that minimises the negative repurcussions should downtime occur. However, despite their best intentions, many Disaster Recovery (DR) plans are not up to the job they were created for, leaving the business exposed.

In this white paper we identify where these vulnerabilities are and how to patch them and explore a new type of service that will ensure businesses enjoy the best Disaster Recovery money can buy at a fraction of the cost of traditional solutions.

Contents

01. Introduction

Technology is amazing...when it works

It empowers us to do more than we could ever have imagined, increases the speed at which we can do it and vitally the number of people we can do it for. Unsurprisingly the IT department has become the engine that drives modern business forward.

The problem is as technology becomes more pervasive, we put ourselves more at its mercy. When technology fails, as it is apt to do, the negative effects reverberate across every aspect of the business.

Customers are fickle and users are impatient. Some businesses can afford to be offline for hours or days but for many, any kind of disruption in business as usual will cause frustration from within the company and anger from without.

This is why you have a plan to ensure that when the worst happens you are equipped to meet the challenge head-on and get your business back up and running as soon as possible.

That's the idea anyway. Unfortunately experience shows that many DR plans are not fit for purpose. Far from bullet-proof, they have major vulnerabilities that if left unchecked can have a devastating effect on your ability to meet your Recovery Time Objectives (RTOs).

02. Disaster? What disaster?

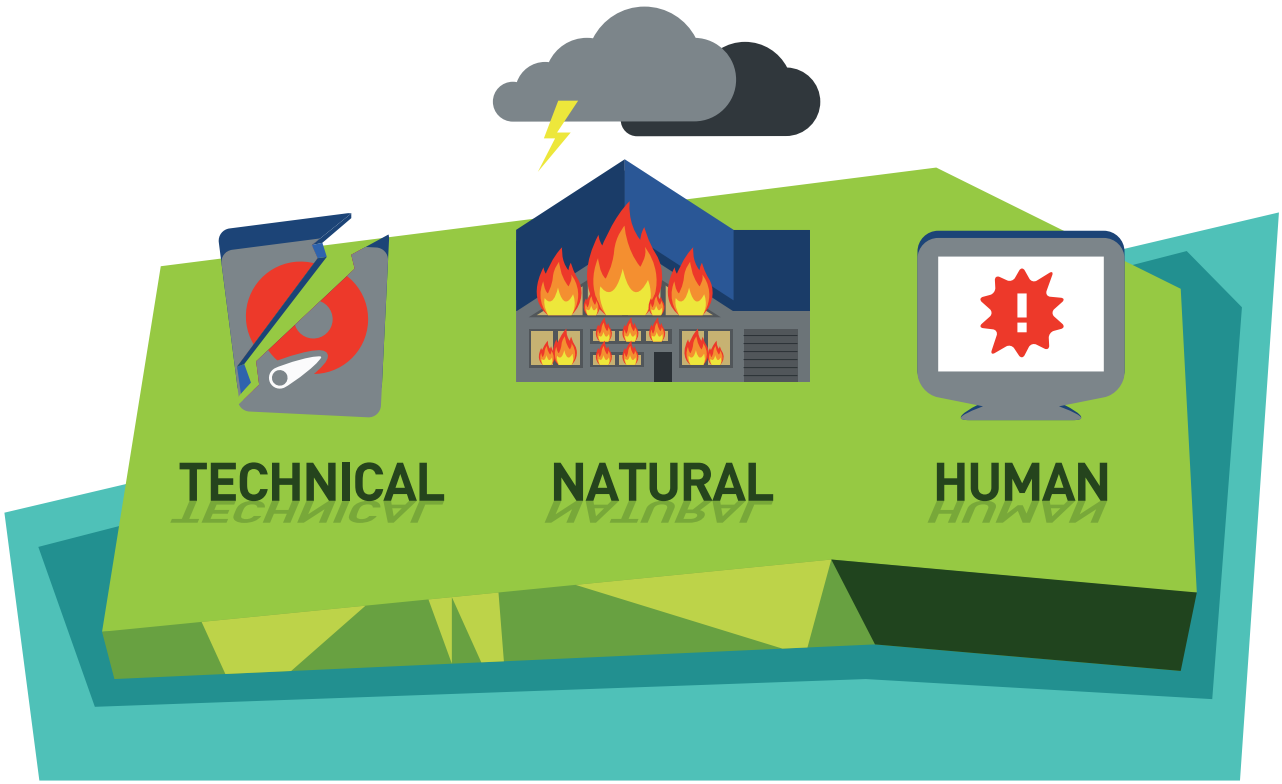
Risk is one of those things that is neither easy to define nor measure. Yet mitigating against it is an important part of all our lives. It's a balancing act. You weigh up a percieved problem against the likelihood of it happening and the consequences should it do so.

You then make a decision on what you are willing to do to ensure you are prepared when disaster strikes.

Even when the likelihood of something happening is remote, if the consequences are bad enough, you will be motivated to take preventative measures. This is the basis of IT Disaster Recovery.

Technology plays such a critical role in the running of so many businesses that ensuring it can continue to function in the face of disaster is essential. Even though the probability of catastrophic failure can feel remote.

However, while it may be preferable to dismiss the potential for disaster, the causes of catastrophic failure are not just a possibility but fast becoming more and more likely.



Natural disasters - extreme weather

While the likelihood of becoming the victims of a devastating tsunami or typhoon like we have seen so recently in Japan (March 2011) and the Philippines (November, 2013) is remote, the UK is far from immune from extreme weather.

Serious flooding is an almost annual occurrence, while fierce storms and high winds are more frequent than ever before. In June 2014 a report from the Institution of Chartered Engineers warned that the UK's infrastructure was woefully underprepared for the increase in extreme weather conditions.

The report concluded that hundreds of billions of pounds of investment is needed to safeguard the UK's energy infrastructure from failure and with it our ability to remain economically competitive. [1]

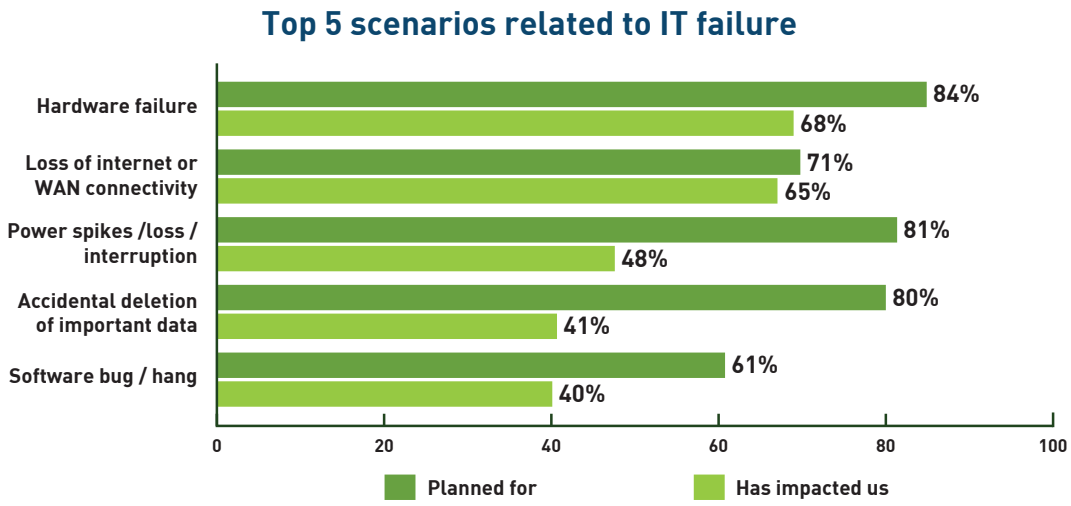
Their warning may feel a bit overblown but a quarter of respondents in research conducted by leading IT trade magazine, Computing, in 2012 said that they had experienced downtime caused by extreme weather. [2]

A quarter of respondents surveyed by Computing magazine in 2012 said they had experienced downtime caused by extreme weather

1 The Guardian, http://bit.ly/TzqzwG
2 Computing, http://bit.ly/1snkUZN

Technical disasters

The more tech you have, the more complex the environment and the greater the probability of some sort of failure. The evidence speaks for itself. The chart, again taken from Computing's research shows that hardware and software failure are two of the top five reasons businesses experience downtime.



New technologies can have teething problems, but it's old or ageing technology that's at the root of so many IT issues. It can be temperamental, it's a pain to integrate with newer tech and it can break down altogether.

All represent a downtime risk, so what happens when the country's 100 year old energy infrastructure is basically one massive legacy system? The answer is power outages.

In November 2013, chaos hit London when a power cut at rush hour trapped people in the Undergound's dark tunnels and stranded many more on their way home. It could not have come at a worse time. What was worse no one was able to predict how long the outage would continue for.

A spokesperson for EDF Energy was quoted in the Daily Mail as saying, "We have lost supplies to large parts of south London in the last few minutes as a result of a National Grid failure supply in the south London area.

"It's difficult to predict how long this is going to take. National Grid has got to get the circuit back." [3]

The reality is that power outages will become more common and they wont be quick or easy to fix.

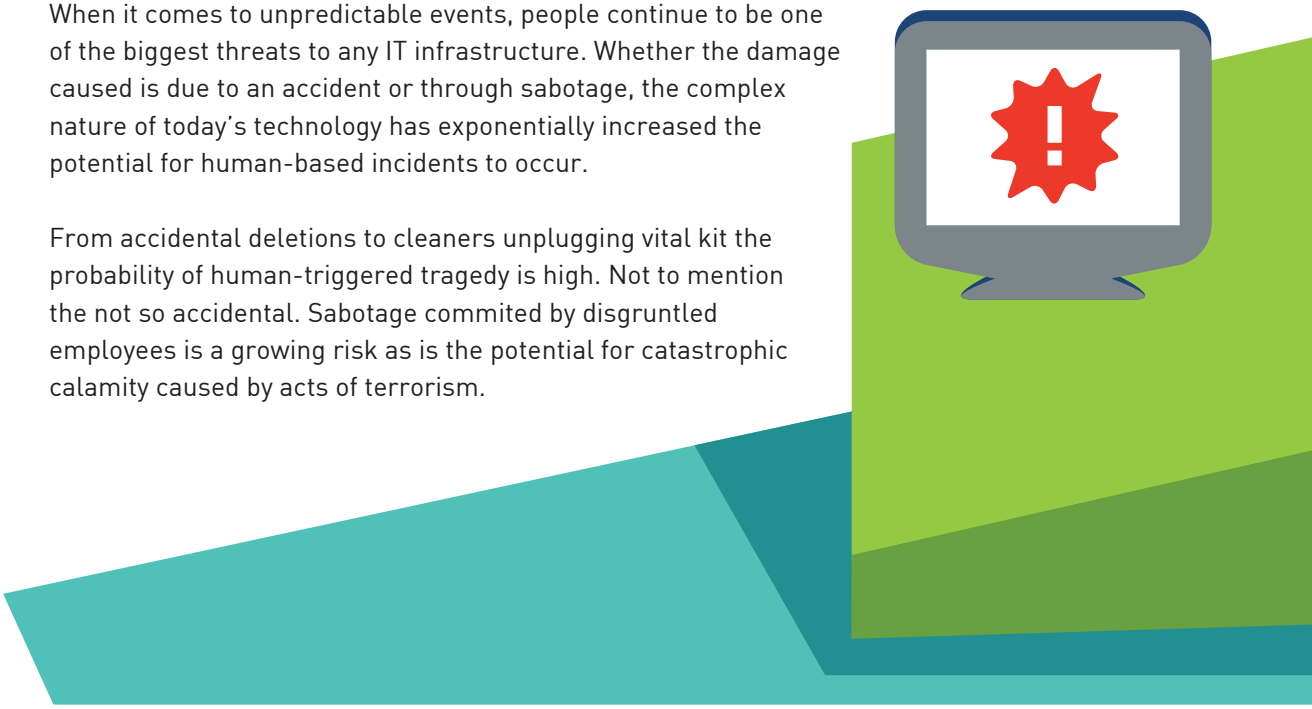
[3] The Daily Mail, http://dailym.ai/1wpYPXW

Human disasters

Disasters are not just acts of God. They can be any isolated, unpredictable event that spells disaster for a business's IT systems.

When it comes to unpredictable events, people continue to be one of the biggest threats to any IT infrastructure. Whether the damage caused is due to an accident or through sabotage, the complex nature of today's technology has exponentially increased the potential for human-based incidents to occur.

From accidental deletions to cleaners unplugging vital kit the probability of human-triggered tragedy is high. Not to mention the not so accidental. Sabotage commited by disgruntled employees is a growing risk as is the potential for catastrophic calamity caused by acts of terrorism.



03. Common vulnerabilities in Disaster Recovery planning

None of the dangers covered above are new, nor are they anything that a seasoned IT Manager or Director will not have considered. It's why the majority of businesses have a well thought out Disaster Recovery plan in place.

The problem is, ensuring your DR is bullet-proof can be expensive, disruptive and risky. This leads to a number of common vulnerabilities that can have a huge impact on your ability to respond to IT failure.

Best value, not best practice

Fundementally, the purpose of a DR plan is to ensure the business can continue to operate as usual in the face of catastrophic failure of its primary IT environment.

This is a tall order no matter how much money you throw at the problem. There will always be a delay between the main system going down and the back-up system coming online. It is, therefore, the DR plan's job to minimise that delay as much as possible.

In theory this is a sound argument but in practice it presents the IT department with numerous problems, the most prominent of which is budget. An optimised DR plan demands that the primary IT environment has a twin. That means twice the technology and of course, twice the cost. You've then got to figure in the day-to-day running and management of that secondary environment and the fact that you may get little ROI on your investment.

Unfortunately it doesn't stop there. With the rate at which technology is refreshed further investment in the secondary environment will be inevitable.

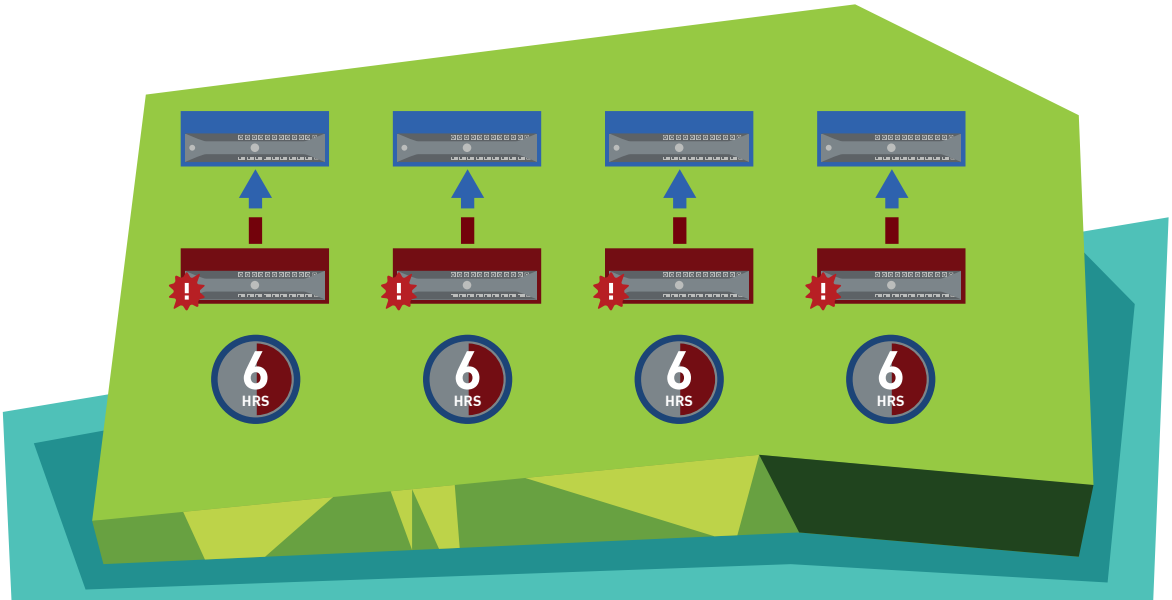
This kind of expense is not just out of reach for many businesses but even if it weren't, coming up with a compelling argument that will secure that budget from a decision maker is close to impossible. No matter how real the risks, in the face of spending that kind of money on what is considered redundant kit, it's no wonder budget holders choose to opt out.

A holiday insurance mentality takes root, where you opt for a backup solution that ensures vital data can be recovered and mission-critical applications brought back online.

Backup solutions make sense. They are a fraction of the cost of building a secondary IT environment and appear to provide a decent level of business continuity in the face of disaster.

The challenge is this solution takes time to failover and time is a luxury that businesses do not have these days.

Connections have to be reset, operating systmes rebooted, permissions restored and data drawn down. Depending on the quality of your internet connectivity and how up-to-date your plan is, this can potentially take hours or days.



4 servers to restore using standard restore and recovery methods. Estimated - 6 hours per server. Estimated total time - 24 hours plus.

- Restore Hypervisor
- Recreate virtual servers
- Confirm and set up all necessary permissions
- Reinstall applications where necessary
- Reconfigure any network and firewall permissions
- Restore data from backup if available

In addition, it's not unusual for companies to back up their data once a day. Therefore when the restore button is pressed, they could potentially be missing up to a day's worth of data. And with the 24/7 nature of business, this could mean the loss of a lot of critical information.

Vulnerability patch

Restoring your backup is a journey and as long as you know all of the directions on the route to your destination, you can ensure your travel time is as quick as possible. There are no shortcuts.

Untested and unproven

In an ideal world a DR plan would be tested on a regular basis. Like the Submarine Captains of numerous war movies you would drill your team to ensure that the plan not only worked but in the event of catastrophic failure you would know the exact time it takes to get the business back on its feet.

Unfortunately we don't live in a perfect world and rather than a regualr occurrence, many DR plans are rarely tested and in some situations they are not tested at all.

This is not surprising. Testing a DR plan is not as simple as flicking a switch. In reality, testing presents significant risk and disruption to the business. You not only have to commit time and resource to the testing process but in order to ensure the plan is sound you have to fail your system over to the backup. And failing over can be an accident waiting to happen. Anything can go wrong and there's no guarantee the problem will resolve once you fail back.

Of course if you don't test it, you won't know if it works, how long it takes to execute or what issues could arise that will inevitably cost you valuable minutes, hours or even days.

Vulnerability patch

There is no simple answer to this challenge. The bottom line is an untested plan is no plan at all. So whether you do it in the middle of the night or at a relatively slow period for the business, it is imperative that you make sure your plan works.

Outdated, not updated

In my experience the vast majority of Disaster Recovery plans are well thought out. They accurately show the cost of running the plan, the amount of human resource needed to execute it and offer a detailed execution process.

While this all may be true at the beginning of the plan's life, problems arise when there isn't a system in place for regularly updating it.

The speed at which modern businesses change is astounding. They expand and contract with joiners and leavers. New technologies and applications swell the IT environment as businesses seek greater productivity and efficiencies. Satellite offices open as the workforce becomes more mobile and remote. All of which have an impact on your plan. If it does not reflect the changes to the primary IT environment, you will not be able to effectively execute it.

Vulnerability patch

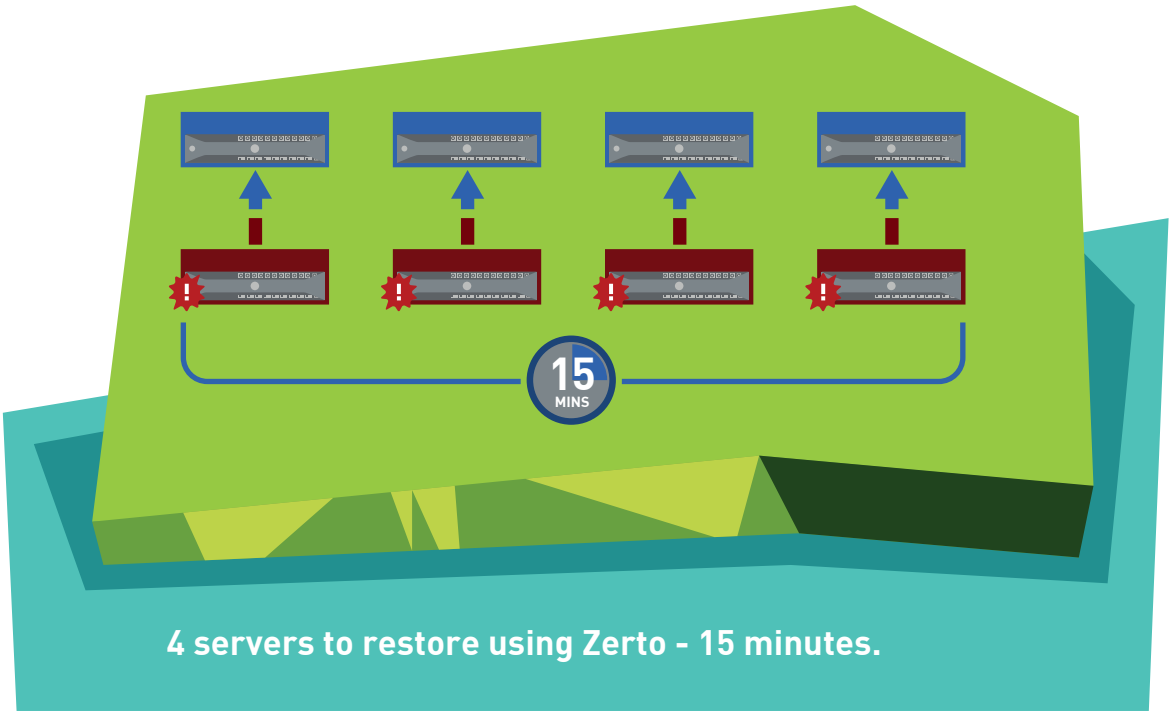
Patching this particular issue while relatively easy, is also time consuming. Someone in the organisation needs to take responsibility for updating the plan every time there is a change that has an impact on the business-as-usual running of the business.

04. Bullet-proofing your DR plan

Creating a bullet-proof plan requires a bullet-proof solution. Not the best you can afford but the best you can buy. Something that offers you the peace of mind of a secondary IT environment but without the cost. A no-brainer.

And that is exactly what is now available. Disaster Recovery as a Service or DRaaS are cloud-based solutions that enable you to replicate your entire primary environment at a fraction of the cost of traditional solutions.

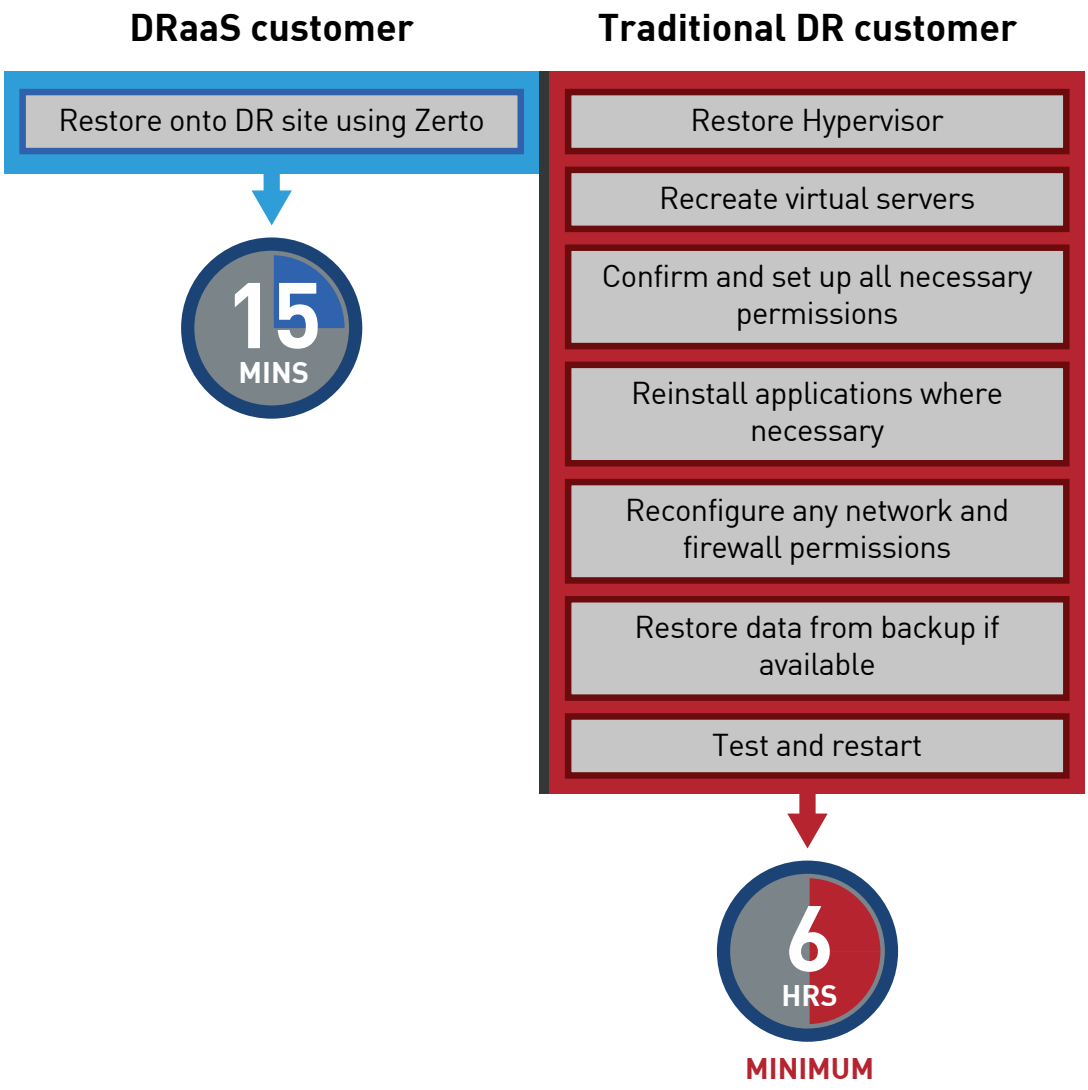
Using a clever piece of software that sits on your virtualised estate, DRaaS providers can keep a snapshot of your primary environment that is continously updated. In the event of a disaster your system fails over to the DRaaS provider's estate and your business continues to function as if nothing has happened. The biggest benefit of all is you can be up and running in a matter of minutes.



These claims may sound dubious but in a recent white paper, Forrester reported that "many who have taken the plunge report that these claims are not as far-fetched as they seem at first glance." [4]

[4] The Forrester Wave: Disaster Recovery as A Service Providers, Q1 2014, by Rachel A Dines, January 17, 2014

The below diagram compares typical recovery times for companies using a solution like Zerto's compared with a traditional DR solution.



Money, money, money

Traditionally, Disaster Recovery solutions cost a fortune because doing it right required buying two of everything. Cloud-based solutions are different. Rather than buying the kit and having to worry about managing and upgrading it, all you have to do is reserve space in your provider's environment.

The reservation cost is low, charged on a pay-as-you-go basis and you are in full control of how much you need. This pricing model makes the upfront capital investment minimal and any failover costs predictable.

Testing, testing, testing

While testing traditional DR solutions is risky and disruptive, DRaaS testing is automated and non-disruptive. This means that you can test more often and ensure that your plan remains sound no matter how the business changes.

Tailored to you

One of the biggest challenges with traditional DR models is the inflexibility of the contract. Making changes to your agreement with your supplier was typically difficult during the life of the contract. This is not an issue with DRaaS. Since you are only paying a reservation cost upfront you can tweak your agreement with the supplier so that it remains relevant to your business at all times.

Fast, effective pain relief

As competition continues to increase across all market sectors, businesses cannot afford downtime. The result is RTOs have become more aggressive. As traditional models struggle to keep up, DRaaS solutions are cutting recovery times to mere minutes.

Simply put DRaaS isn't making enterprise level Disaster Recovery available to businesses of all sizes. It is making them obsolete and replacing them with a new era that will ensure every business can escape a catastrophic IT failure unscathed.

Of course this type of service is only availiable to companies that have virtualised their IT. So if you're still running a physical environment, especially one that's running on legacy technology, this offers a powerful catalyst for moving your infrastructure into the cloud.

05. How to choose a DRaaS partner

As business decision makers realise the benefits of moving to a DRaaS model, it is inevitable the conversation will move to who should provide it. There are already a number of different offerings on the market and so it's important that you choose the right one for your company.

While price will always be a consideration there are a number of other factors that you should also take into account.

SLAs

The ability to meet your RTOs will vary from provider to provider. Ensure that the partner you choose can meet those objectives and has the flexibility to continue to meet them as your business grows.

Transparency in pricing

On the surface DRaaS offers a cost-effective solution that delivers significant savings compared to traditional models. While prices will certainly look attractive, it's important you know exactly what you are paying for and how much it will cost. You don't want to get involved with a supplier only to find a hidden cost rearing its ugly head down the line.

Testing

Certainly testing DRaaS solutions is painless but that doesn't make it free. Make sure you know how much the testing costs. While you want to test your plan, you don't want to have to pay the earth to do so. Having said that some providers do offer free testing as part of their packages.

Project management

Any provider worth their salt will steer you through the set up process so that the solution is tailored to your primary IT environment and meets your Recovery Time Objectives. However, whether it's a traditional solution or a cloud solution, your Disaster Recovery solution is only as robust as the plan that supports it.

A quality provider will not only help you to build your plan but also ensure that it evolves with your business and never goes out of date. This can only happen when there are systems and processes in place that ensure consistent communication between you and your provider.

Resilience

Your partner's DRaaS service is only as robust as their environment. To make sure your supplier is as resilient as you need it to be you should investigate how secure their data centre is, the measures they've taken to guarantee it remains functional in the event of a disaster and if possible that their response includes a secondary site that their own systems can fail over to.

About Timico

Timico is an independent managed service provider, supplying business strength managed network, Unified Communication, mobile and managed hosting solutions. Key customers include Travis Perkins, St John Ambulance, Informa, Honda UK and Murco Petroleum. Timico's MPLS network enables the secure delivery of applications and data to all office, retail and homeworker locations. Timico owns and operates its own core IP network, Tier 3 data centre and carrier-grade VoIP switch and is also a fully licenced mobile service provider. Since being founded in 2004, Timico has consistently been one of the fastest growing privately-owned companies in the UK tech sector.
Visit **www.timico.co.uk** for more information.

About Colin Bell

Colin Bell is Director of Cloud & Hosting at Timico, delivering managed hosting, Infrastructure as a Service and business continuity solutions to businesses and partner customers across the UK. Colin has worked in hosting since the early days of the industry, initially as EMEA Sales Director for Rackspace and subsequently as Managing Director of business-critical managed hosting provider NetBenefit, part of Group NBT plc. Prior to this he held sales and marketing leadership roles in a number of fast growing technology companies.

WHITE PAPER

A white paper by Colin Bell, Timico's Director of Cloud and Hosting.

timico®
connect · host · manage