Demystifying Disaster Recovery;

The hard truth about business continuity's best friend

READ ABOUT:

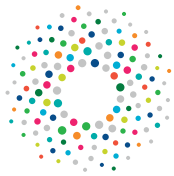
- The most common disasters to strike
- The true cost of a DR event
- How DR is commonly approached in businesses
- How DR has evolved
- The elements of a good solution
- The real benefits of implementing a DR solution

Disaster recovery is an often misunderstood facet of what some consider a complex industry – Information Technology. But it really doesn't have to be and with today's multitude of service providers and solutions, the use of clever technology to secure your business is far more obtainable than most would believe.

In this paper, we will look at how DR or what many businesses consider to be a DR solution is commonly deployed today, whilst addressing the widely held business fears and motivations to implement a solution – in turn simplifying the perceived complexity of DR and identifying a solution and best practice that meets forward thinking businesses requirements today.

So, what is DR?

Disaster Recovery solutions form part of every company's business continuity plan. Typically, they provide the recovery



mechanism for multiple business threats, such as the loss of business premises or a massive failure within the production environment, ensuring that the business can continue its operations in the event of a disaster.

Although most businesses recognise the importance of continuity in the event of a disaster, most organisations only implement elements of a proper DR solution. Solutions implemented differ from business to business and range from data being backed up offsite or in some circumstances an external replica of their production environment, but commonly these solutions are rarely tested and in the event of a real disaster will only provide partial recovery.

But why would any business leave themselves open to threat?

Simply put, DR can be complex and the associated costs can be preventative – for instance, in some occurrences it is necessary that the business has an equivalent 2nd site with all of the production servers and network built ready for use, which just isn't feasible for many businesses today. Additionally, it can be quite complex to define the RPO and RTOs required as well as the processes to be used in the event of DR, so companies simply shy away from the responsibility with the hope that what elements of DR that they do have in place is sufficient for their business in the event of a disaster.

Furthermore, the complexities of a proper solution and costs incurred mean that the business' board often can't fully reconcile the threat with the solution and are reluctant to release the funds necessary to implement the technology, until they fully understand. Conversations on the subject and impetus to implement a DR solution, therefore, tend to run aground as IT personnel and CxO's quite often use different language, so the proposal is rarely seen through to completion.

Disasters everywhere

In today's world where businesses have such reliance on technology, potential disaster is never too far away. But, what are the threats that businesses commonly experience today?

With the integration of technology through every element of most organisations today, threats encountered can be far reaching and range from simple hardware failure and viruses to poor change management (the creation of critical events by the business themselves by not adopting a proper change management and introducing a problem that could have been avoided) and even complete site loss.

Possibly the most common disaster encountered centres around server corruption failure, whereby the business then needs to bring back the server in a former state as quickly as possible. This recovery is often required on the original site and tends to be within the capability of existing personnel and infrastructure. Less common but significantly more impactful, is the complete loss of the operations site due to power outage, fire, flood or other natural disaster – in reality, most businesses are just not prepared for such an event and in instances such as this whereby such severe circumstances are encountered, DR is essential if the business is to survive.

So, what is the real impact of a disaster on a business?

High Profile Disasters

RBS
Cause: Accident
The Royal Bank of Scotland was hit by a huge disaster in 2012, when a faulty software update caused a four day outage for the bank, leaving 6.5 million customers without access to their money and in turn stalling new house purchases and even stranding people abroad. The disaster not only affected the banks reputation but landed them with a £56m fine from regulators.

Amazon
Cause: Act of God
In June 2012, Amazon's North Virginia data centre was hit by a major power outage caused by a severe storm hitting the east coast of the United States. The outage impacted many popular services including Netflix and Instagram – the latter of which was down for 15 hours in total.

Just Eat
Cause: Power Failure
The take away app was severely affected when their UK head office was hit by a power failure. With the head office housing the businesses infrastructure and acting as a central hub for all other country offices, the power failure affected not only UK services but its entire service delivery across the world.

Blackberry
Cause: Infrastructure Failure
In 2011, Blackberry was hit with a series of disruption to services, affecting its entire network of phones and millions of users around the world. The failure was blamed on a core switch failure within RIM's (Research in Motion – Blackberry's manufacturer) infrastructure, resulting in, some might suggest, irrevocable damage to Blackberry's reputation as well as it's financials.

Virgin Blue
Cause: Hardware Failure
In September 2010, Virgin Blue suffered a hardware failure resulting in a complete outage of the airline's check-in and online booking systems. The outage severely interrupted business operations for 11 days, affecting around 50,000 passengers and 400 flights. The business suffered a huge amount of negative press, along with profit loss to the sum of £10,713,022.

Stats:
Financial Loss

Gartner calculated that depending on the industry sector, network downtime costs companies on average **£3,966** per minute which equates to **£212,494** per hour.

Additionally, they calculate that the average large organisation has **87 hours** of network downtime each year, which could equate to a loss of **£18,486,978**.

The impact felt by any business when disaster strikes really depends on the disaster itself and the level of protection & continuity planning they have in place. A single server failure, for instance, will create an outage which may cause users to grumble and a potential delay for services to be delivered to customers, but this is likely to only cause embarrassment and not business failure. On the other hand, a complete site failure is undoubtedly going to result in a significant loss of revenue, large costs to recover and the potential to go out of business.
With the potential to go out of business and the range of possible impacts incurred, there is obviously plenty of motivation for businesses to implement DR properly. So, why does recovery from a DR event remain a secondary concern for many businesses? Again, this often depends on the particular business, their approach to risk management and what they have encountered historically, in terms of disaster, compliance, audits, insurance or even the sale or floatation of the business.

Additionally, it will depend on the core objectives of the business and subsequent worries of not having a DR solution in place and how this may affect achieving those objectives. For instance, each board member in their role is likely to have individual objectives to fulfil, be it financial, technological, operational or even personnel, which is likely to influence their need for DR and in turn influence their view on the subject, which in combination with other board members views can ensure the matter is never resolved or realised.

The importance of implementation

As highlighted, the implementation of a robust DR solution tends to be waylaid with the involvement of CxO's and a breakdown of conversation between IT and board members. However, common needs can be found amongst decision makers and the driving forces for businesses to implement DR do arise. These can centre around a view taken of the operations of the business itself, often put upon it from external pressure, such as insurance requirements, auditing of the business, accreditations, regulatory compliance or when a business seeks investment or looks to sell. In each instance the importance of a proper DR solution is highlighted, which transcends to all business functions and board member roles, significantly helping buy in. However, these situations should not be the real driving force and businesses today should look to implement DR to enhance the production environment capacity and therefore business capability.

Disaster Recovery; That'll do approach

In an attempt to implement a DR solution or at the very least to alleviate the fears of not having any sort of DR in place, businesses typically focus on implementing storage and virtualisation technologies - to enable rapid recovery from a server failure – along with implementing long term backups. However these systems typically won't be fully integrated and will rely on the IT team to ensure they are operational. As such and because they are relatively complicated, it is common for the systems to be rarely tested and updated, possibly rendering them obsolete.

Although, these are important elements to implement they only take a business part of the way towards a full DR solution. They may protect a business for a low level event but won't provide sufficient protection for a significant outage and certainly not for a full site failure. With this in mind, every business should ask themselves – can they operate without their systems for 24 or 48 hours, let alone the week it might take to rebuild an entire system in a new location.

In reality, most businesses just don't test DR, so whatever elements they have implemented are unproved and in turn don't provide the business with the reassurances they seek. DR commonly remains untested for a combination of reasons, but predominantly because the process can be complicated, expensive and never at the top of a businesses to do list.

Furthermore, testing DR is generally one way - by which we mean, that to truly test most DR solutions you have to actually put the business within a DR situation, making it impossible to get back to production state without going through the whole DR process. Somewhat understandably, this situation is something many businesses wish to avoid and certainly not something that most IT departments are motivated to implement.

Therefore if disaster does actually strike, this becomes the only time that the DR solution is actually tested for success or failure, which if the latter is already too late. In these instances, most organisations cope with a small event or a scare, however very few cope or even recover from a major event such as site loss.

Mark Brookbanks, Panoptics Managing Director, comments "DR pretends to be most IT departments top priority but is very rarely fully fulfilled, as such businesses often claim that they've got it but never truly have. Gone are the days when outsourced DR is ineffective, so businesses no longer have to be restricted by IT departments capabilities & skill sets to implement DR, as the market has matured and there are now readily available solutions that can fulfill the majority of user requirements. The emphasis, in our opinion, must therefore be on the business as a whole, rather than their IT department, to provide the support and drive to implement a solution that meets the business needs and mitigates the risks posed. With education and the right information, businesses will begin to realise that there are other benefits to DR which can be realised before a disaster even strikes."

DR is expensive and out of most businesses reach, right?

The simple answer is no; it really doesn't have to be and the real reason why DR is perceived as such, is because it is widely misunderstood and the costs involved can seem incalculable. In reality, the main reason why many businesses find DR out of reach is because they can't solve the challenge of getting the business in its entirety to come together to define a policy and then take that all the way through to

design and implementation of a suitable solution. After all some policy is better than none at all.

In most successful scenarios, ownership of DR is taken by a senior stakeholder, often the CEO, who empowers the business units to contribute to an overall policy and drives the project through to completion. This approach typically ensures that the Disaster Recovery becomes an integrated part of the Business Continuity Plan and of real use to the business as a whole.

The changing face of Disaster Recovery

It's fair to say that DR has evolved. The adoption of Virtualisation has meant that there is now significant resilience in most production environments, therefore small disasters are already protected against and no longer such an issue. Additionally, with the advent of cloud and the take up of the technology, it has further enabled businesses to access more robust DR solutions as it has opened the doors to a number of vendors that can deliver seamless backup and replication solutions independent of the hardware & software in use.

With this advancement, it is now possible to utilise a single tool to manage both backup and replication, whereby the private cloud solution avoids the cost of a 2nd datacentre by providing a virtual datacentre instead. The service providers also now possess the understanding within the technology workspace to enable the solution to be tailored to each individual customer's requirement, meaning that an exact fit can be found for virtually any scenario and specification.

So, what should businesses focus on?

Firstly, is the DR plan owner or architect still in the business? Is their plan still relevant to the business as it is today and can its implementation still be achieved? This is a simple element in what is a complex strategy, but one that is all too often overlooked. If the DR solution is out of date it is very likely to not be effective when called upon.

Secondly, businesses should be testing the solution regularly. With this in mind, businesses should seek a solution that automatically and consistently informs the business that it is working properly, so as to free the business from technology choices such as storage and other core functions. As an analogy to further explain - think of how you buy electricity and water as an individual. You don't care about the pipes and cables beyond your house, you just want to choose the supplier with the right tariff and then consume the services as you need them. Similarly, this is true with quality DR solutions today as the technology available now will enable businesses to consume the solution as they require, freeing them to concentrate on the business itself, rather than the "what if?".

Thirdly, selecting a DR partner wisely is critical. Do they truly understand the complexities of your business' network and what impact this may have in the event of DR invocation, plus is their underlying Infrastructure the required quality to ensure DR is seamless in the event of an incident? To highlight the potential issue, consider the standard IP addressing of most business' networks - this is likely to compete with VLANs and IP addresses in a 2nd datacenter, so the partner must ensure that in the event of DR invocation there are no IP conflicts and the end users see a seamless transition. Simple in practice perhaps, but it's this attention to detail that makes a truly great DR service provider standout and will make the difference to your business in the event of a disaster.

Finally, a sound DR plan is important, in so much that the business should think about RPO and RTO rather than technology. The business needs to come up with a well-defined policy and then fit the technology around it rather than buying technology then getting the best they can out of it. Each business should have a clear RPO & RTO policy which gets updated with the advent of new applications and data uses. Additionally, the DR plan should be a measurable, considered policy that enables growth or change with the changing business requirements and is simple to adopt in terms of the technology that underpins it.

Elements of a good DR solution

So, what actually constitutes a good DR solution and what should businesses look for when selecting to work with a service provider? Simply put, a good solution will remove the complexities of DR. With this in mind, a truly sensible DR solution should integrate seamlessly with your business's backup, be independent of hardware in use, provide clear and reasonable demarcation of responsibilities as well as being simple and easy to adopt.

The solution we have found that meets all of the criteria above and allows the deployment to be completely integrated into the individual environment, whilst also being great value, is Veeam. With Veeam, Panoptics provides seamless integration of backup and replication, whilst providing hardware independence to either of our datacentres with the ability to failover to our hosted Virtual Machines. As such, the solution avoids the typical capital expenditure and lengthy technical designs necessary to enable a solution as robust, whilst also integrating with the customers own Veeam implementation if they already own one, yet further reducing cost and complexity.

Simple steps to successful DR implementation:

With the advancement of technology and service solutions, any business can implement DR successfully. Just follow these simple steps:

1. Define the business's Recovery Point Objective (RPO) and Recovery Time Objective (RTO)
2. Ensure the Network IP addressing will work in DR
3. Find a solution partner that can meet your business's requirements
4. Implement the solution and ensure there is complete documentation
5. Measure the outcomes
6. Analyse and refine the delivery

Okay, I'm convinced but what are the real benefits of DR?

Benefits realised with the implementation of a sound DR solution typically fall into two camps, both of which help your business gain the confidence necessary to compete effectively in today's challenging business environments. The first is risk mitigation – DR provides businesses with the ability to operate without the fear of disaster – and secondly, DR ensures the business maintains or even achieves regulatory compliance.

However, these benefits can be easily extrapolated to become more understandable for the myriad of industries where DR is critical. Essentially, if you get DR right it is possible to improve your entire production environment capacity, as well as realise the multitude of benefits associated with insurance compliance, due diligence during mergers & acquisitions, borrowing money and even the ability to achieve business accreditations such as ISO, which otherwise may have been out of reach – as

it answers a lot of the questions these elements require before they've had the time to enquire. But perhaps the greatest benefit achievable with the greatest return on investment is customer confidence – with DR, any business can prove their stability in the delivery of their service or products, opening larger opportunities which may not have been so apparent without DR in place.

The Panoptics difference

So, how would Panoptics help realise these benefits and why choose Panoptics over any other service provider? To answer this, we draw your attention to our company strapline – "Simplifying Complexity" – we make DR simple! To add to this, Panoptics is a service provider with a difference, we have the right technology as well as the right approach, with the experience to help every client make the right policy decisions and map the service to meet your exact requirements. Plus, our solution is incredibly competitively priced.

But the real advantage is our core infrastructure in combination with the technology we use – Veeam. Yes, there are other service providers using Veeam but each of them will struggle to match our enterprise class cloud integration in terms of ISP, Virtual datacentre and managed service capability – that's a fact. But what about those service providers not using Veeam we here you say. Well, without sounding bullish... they simply can't compete, not only will they lack the core infrastructure that provides the foundation of our quality service, but the technology will rely on multiple technologies, going against everything you want to achieve with a simple DR solution. This is why we have become a trusted partner to a diverse range of businesses from SME's all the way through to internationally recognisable brands.

The proof is in the pudding

We understand that it's all well and good professing to be the best, but why would any business believe the claim without seeing some sort of proof – after all, if after implementation you realise the solution is rubbish, it's already too late. So, to put our money where our mouth is, so to speak, we did exactly what most IT departments never do – we tested the solution and invoked a true recovery from a disaster.

Check out the video here, **Disaster Recovery: Veeam Instant Recovery - Speed Test** - we're sure you'll be impressed!

If you would like to find out more and discover how Panoptics can simplify your business complexities, get in touch and we would be happy to help.

The Solution: **Why Veeam?**

Trusted by over 183,000 businesses worldwide & recognised as the No.1 VM Backup, Panoptics decision to harness the power of Veeam for its delivery of Backup and DR solutions is one borne from the knowledge that it is truly the best technology available today.

Veeam® is a powerful, easy-to-use and affordable Backup and Availability solution. It provides fast, flexible and reliable recovery of virtualized applications and data bringing virtual machine backup and replication together in a single software solution with award-winning support for VMware vSphere and Microsoft Hyper-V virtual environments.

Awards:
Winner of over 80 industry awards, including the more VMworld awards than any other vendor plus the only two time winner of the VMworld award for New Technology. Additionally, in 2015, for the third year in a row, Veeam was included as one of the "Visionaries" in the Gartner Magic Quadrant for Enterprise Backup/Recovery Software, as well as winning "Backup and Recovery/Archive Product of the Year" at the SVC Awards.

Key reasons to use Veeam:

> Fully integrated cloud based disaster recovery
> RTO < 15 minutes for ALL applications and data
> RPO < 15 minutes for ALL applications and data
> 100% automated backup testing and recovery verification
> 0% failure rate
> Storage agnostic
> Proactive visibility
> Easy to deploy and configure
> Built-in, source-side compression and deduplication

About Panoptics:

Panoptics is an innovative IT Service provider focussed on simplifying complexity which was founded with a defining principle to deliver IT services and solutions with a difference. Panoptics' comprehensive offering covers the complete spectrum of IT requirements including Managed Services, Supply Services, Datacentres & Connectivity.

Discover how Panoptics can help with your Disaster Recovery requirements.
Get in touch today!

PANOPTICS

0203 137 6351
www.panoptics.com