TechCentral.ie

TechPro magazine | Advertise | Contact | About

Changing times, changing needs

While recovering from a backup is still a viable option for many, time pressure and complexity of systems have prompted demand for greater flexibility in services, says PAUL HEARNS

Image: Stockfresh

Read More: 99999 back-up Datto Decisions disaster recovery Landmark Technologies Sungard AS synology Trilogy Technologies webroot

15 June 2019 | 0

Disasters are best avoided.

That simple axiom is now a specific trend within the area of business continuity and disaster recovery (BC&DR), along with business resilience and efficient recovery.

Once upon a time, recovering from an outage or failure was generally accomplished by rebooting, reinstalling or standing up new servers and then restoring data from a back-up.

While that venerable approach is still fine for some organisations, it has become an archaic practice for many. These days, the recovery time objective (RTO) is often more critical than the recovery point objective (RPO).

This is probably best characterised by the average cost of downtime that is most often bandied about from analyst Gartner, though research comes from 2014. Back then, the calculation was that each minute of downtime costs an enterprise an average of $5,600. As if that were not motivational enough, fast forward to 2018 an IDC survey of Fortune 1000 companies found that the average hourly cost of an infrastructure failure was around $100,000, while the average total cost of unplanned application downtime per year is $1.25 billion to $2.5 billion. No matter which timeframe or mass scale is

Sign up for Techcentral.ie

Stay on top of the day's tech news with our free **Technology Minute** e-mail newsletter - just add your e-mail here

E-mail

Events

Wed 10 Jul

A New Era of IT Professionals

Online

Sat 20 Jul 10am - 6pm

Dublin Maker

Merrion Square, Dublin

View All Events

Submit Your Event

Polls

Will Huawei smartphones escape a US ban?

No (36%)

Yes (64%)

See other polls >

A-Z Brand index

Click here to go to our index for resellers to source brands and determine who distributes them locally.

More from this Channel

British Airways to be fined for GDPR infringements

£183 million fine is 1.5% of 2017 turnover employed, that is a lot.

It is little wonder that current BC&DR trends hint at disaster avoidance as a strategy, along with resilience and insurance.

However, all of this is compounded by even more things to worry about than ever before.

Data theft and manipulation, extreme weather events becoming commonplace and fake news have all been raised by various commentators in the arena, not least of which is the annual Disaster Recovery Institute (DRI) annual report, the "4th Annual BCM Trends and Predictions Report".

It highlights the fact that cyber attacks aimed at harvesting data often involve organisations that are not the end target and may merely be holding data that might contribute to an end goal, or be a supply chain link that offers an in.

Even farther out than that, the US government has issued a warning for organisations to protect against electromagnetic pulses (EMP) which may be artificially generated as a weapon, or come naturally from solar flares, such as back occurred in 1859.

The "Executive Order on Coordinating National Resilience to Electromagnetic Pulses" from March of this year states "An EMP has the potential to disrupt, degrade, and damage technology and critical infrastructure systems. Human-made or naturally occurring EMPs can affect large geographic areas, disrupting elements critical to the Nation's security and economic prosperity, and could adversely affect global commerce and stability. The Federal Government must foster sustainable, efficient, and cost-effective approaches to improving the Nation's resilience to the effects of EMPs."

As if this were not surreal enough, a nugget from Gartner's top strategic predictions for 2018 and beyond says that by 2022, the majority of individuals in mature economies will consume more false information than true information.

"The tools while in recovery mode, can synchronise data to the original live environment, cutting down on time and making it easier to go to virtualised continuity solutions for many organisations. More virtualised options will be an increasing feature of BC&DR tools and services in the future." Chris Tate, Datto

"With an increasing amount of fake news, companies need to closely monitor what is being said about their brand and the context in which it is being said. Brands will need to

This is fine...
In denial, or in the know — some are clearly divorced from reality, what about the rest?

ICS CIO Profile – Colm Gartlan
IT director, Norbrook Laboratories, Chair of the ICS CIO Advisory Board

ICT Skillnet: Blockchain skills shortage – the opportunity
Putting Ireland at the forefront of Blockchain revolution

ICT Skillnet: Master the Internet of Things
Developing a pipeline of engineers for future needs

cultivate a pattern of behaviour and values that will reduce the ability of others to undermine the brand," said Gartner.

Picking up on the recovery time aspect, Chris Tate, business development director, EMEA, Datto, said that ransomware attacks have highlighted the shortcomings of restoring from tape and other more traditional back-up media. These methods are often too time consuming and not fit for purpose in many instances where the downtime is just too costly.

This, with other trends, has led BC&DR solutions more in the direction of continuity and resilience, than recovery.

However, Tate also said that ransomware is now becoming bespoke. As many decryption keys have been published and made widely available, criminals are becoming more sophisticated in their approach, narrowly targeting tailored packages to do the job.

Virtual options are making more of an impression, too, says Tate. Getting back to the original state before a disruption is being made easier, rather than using an emergency virtual mode.

Tate said that Datto tools while in recovery mode, can synchronise data to the original live environment, cutting down on time and making it easier to go to virtualised continuity solutions for many organisations. He says more virtualised options will be an increasing feature of such tools and services in the future.

With decades of experience in the business of back up and recovery, Sungard Availability Systems has seen much in terms of the reasons for invoking a recovery. According to Noel O'Grady, director for sales in Ireland, worldwide invocations on its services have seen civil unrest and terrorism move up the list of causes, but hardware and power drop as reliability in both spheres has increased.

However, O'Grady points out that as complexity has been introduced into supply chains and architectures, communications of one sort or another has risen dramatically in the list of reasons for invocations.

"We always look at it from the standpoint that disruption to a business is inevitable at some point," said O'Grady. "If you look at the general trend in business, we have increased the complexity of most of our supply chains, as well as our systems and particularly around multi-systems. This invariably means that something in there is going to cause a disruption that needs to be planned for."

The approach taken by Sungard, says O'Grady, has been to encapsulate core services, around three major headings. At the centre is back up, to keep data safe.

"That's the first step, in terms of resilience," he said. "The next box containing that is disaster recovery as a service (DRaaS). It is not enough that you just have your data, you need to be able to recover an environment that works and helps the business continue."

Utility cloud has been instrumental in providing that level of protection, O'Grady said.

"It is not enough that you just have your data, you need to be able to recover an environment that works and helps the business continue." Noel O'Grady, Sungard AS

“AWS has enabled us to deliver a service which is ideal for these types of workloads,” he said.

The other trend being seen, he reports, and what is the last box that wraps around the other services is what is termed the managed recovery programme (MRP).

“That goes a step further, where a lot of people who may have had DR, when they had a problem and went to invoke, found that production and DR did not match. They also may find out with some DRaaS, that there is compute switched on, but the applications are not necessarily working,” said O’Grady.

MRP was designed as a solution to take it a step further, he says, where a discovery exercise is undertaken for a client’s entire environment and application inter-dependencies and then, in real time, over the lifetime of the contract, there is assurance that production and recovery match each other.

“We are getting towards 100% success in recovery,” O’Grady reports, whereas the industry averages are in the 30% range.

He says a key differentiator for the vendor is that as well as what he calls the “capability side”, the back-up, DRaaS, MRP, and the work area recovery, it also offers consultancy for business resilience and continuity.

Quite often, that completes the whole life cycle for the customer, from assessment to strategy development, plan writing, implementation, testing and operation, he says.

In offering advice to those who might be about to engage or expand capability in this area, both vendors emphasise knowledge.

Datto’s Tate advises organisations to explore the entire support and supply chain environment of the services, getting to know the parties involved and the complete solution end to end. He says talking to the vendor to explore every aspect is vitally important to understand how its features and capabilities will impact and how they can be best leveraged to ensure the right fit for individual organisations.

Sungard’s O’Grady focuses on the specifics of testing.

“Whatever you do, it is your testing that is the key part,” he maintains. “Whatever service you buy, if you are not testing it, it is not real.”

Most services, he says, will a package of two tests per annum or so, and more can be had, but “it is only when you test, and you test with real systems, real people, real services, do you find out how good it is.”

“If you are not testing, you could be spending a lot of money that will not give you a return when you have a problem,” said O’Grady.

The old mantra for back-up of any sort is still applicable, even in today’s as a service consumption world of cloud and multi-cloud options — test or be damned.

The points about complexity are worth noting too, as many organisations may find that as their production environments have expanded to embrace cloud services, APIs and multiple resource calls, their back-up capabilities may not have developed to the same level of sophistication. It would be worth an examination to see if current and planned services in BC&DR can cope.

With the sharp focus brought on by ransomware, resilience and recovery services have moved on apace, but only if organisations have taken heed, updated systems and engaged with the experts will they keep a step ahead.

(Image: Stockfresh)

Weighing up the costs and risks of storing data on business premises

Organisations of all sizes and across all sectors are gathering and storing data on a scale like never before. It comes with a range of associated costs and risks that can be dramatically impacted by where and how that information is stored.

There is a common misconception that storing sensitive data, or indeed any information, on your organisation's own premises, is the best solution to keep it safe. However, having the physical data close to hand and a sense that it is under your control, is not sufficient in most cases.

"There is a common misconception that storing sensitive data, or indeed any information, on your organisation's own premises, is the best solution to keep it safe. However, having the physical data close to hand and a sense that it is under your control, is not sufficient in most cases."

The reality is that for the vast majority of businesses, the cost of providing a level of security and resilience equal to that which is available in a purpose built off-site facility is simply beyond their capabilities.

Storing data on your own business premises can be hugely – and prohibitively – expensive.

There is typically a large capital outlay required to purchase the associated power, cooling and security hardware and software. Money that could be spent on other critical business matters.

A set-up on a business' own premises will also require in-house server hardware and software IT employees and security personnel on hand to provide support 24 hours a day, 365 days per year.

This must all be weighed against storing data off-site which would typically become part of an organisation's operating expenditure with a monthly or quarterly payment. With our remote hands services, hardware and software support personnel can carry out these tasks on an hourly rate.

The costs are not restricted to the initial investment and ongoing maintenance.

When you factor in the risks to data, from a breach or accidental damage, the associated costs could rise much further.

Risks include malicious attacks or theft of data storage hardware and software while the information can also be compromised accidentally through, for example, fire or flooding.

Richard Willis, managing director of Belfast-based broker Willis Insurance and Risk Management said firms were becoming increasingly aware of the need to protect data.

"In the modern business world, there is a strong reliance across all sectors on secure data systems in order to ensure business continuity and keep sensitive information safe.

"For that reason, any outage, whether caused by failures of power or cooling or due to fire, flooding or a physical security breach is a cause of major concern.

"The cost of protecting against such outages on your own premises can be significant. Professional data centres that are designed specifically to guard against the most common types of outages are an extremely effective means of managing that risk more economically and securely."

A growing number of firms were opting to store servers in data centres, where they can be maintained in a highly resilient and secure climate-controlled environment, specifically designed to provide optimum protection.

The colocation of servers and networking equipment in a third-party data centre, provides businesses with a site that has the infrastructure and physical security required to keep its deployment secure and operational all year round.

5NINES owns and operates a network of data centres across the world, including in the Netherlands, Finland, and the United States.

Its latest Tier III+ data centre based at the Atlantic Link enterprise campus in Coleraine is Northern Ireland's only commercial carrier neutral colocation facility.

The first of six data halls, each of which has the capacity for more than 200 racks, opened at the 4,180 sq meter (45,000 sq ft) facility in 2018.

Specialist services include wholesale for customers with large requirement for space and power, 24-hour remote hands assistance and dedicated back-up services while private and fully customisable data suites or cages can also be provided.

Paul Besley is general manager Northern Ireland, 5NINES

paul.besley@99999.co.uk * www.99999.co.uk

Strategy allied with education

The constant news of data leaks, hacked email accounts and compromised corporate networks, has signalled that these types of disruptions are sadly becoming the norm. Following an incident, it is critical that businesses understand (and can communicate internally and externally) how long they will be offline and when services will be resumed. This requires a forward-thinking approach which ensures business continuity in the event of a disruption. Mitigating the rising risks of attacks, such as crypto-jacking and ransomware attacks, can be achieved through a combination of the appropriate technology, user awareness and a water-tight disaster recovery plan (DRP).

Enterprises need to ensure that firstly, adequate defences are put in place especially around business-critical processes and data. Secondly, valuable data must be backed up, so systems can be restored quickly, if needed. As part of this, DRP must be tested regularly help understand the time it takes to restore systems to a useable state and what data is likely to be lost due to back up schedules. Installing a layered security solution is essential, combined with the use of a reliable back-up solution – including airgapped back-ups as a last resort is a must.

Lastly, employee education underpins a strong defence strategy and end users should be aware of the potential attacks they face and understand the methods cybercriminals use to target them. They need to be careful what emails and attachments they open or run and what links they click on. With effective user education and training put into place, employees can be converted from the weakest link to the first line of defence.

Outages and service disruptions can have devastating effects on an organisation in terms of financial and reputational impact. Having a thorough and comprehensive business continuity plan for any eventuality will help reinforce trust in the organisation's ability to provide a service, even in adverse conditions.

Tyler Moffitt is senior threat research analyst with Webroot

"Mitigating the rising risks of attacks, such as crypto-jacking and ransomware attacks, can be achieved through a combination of the appropriate technology, user awareness and a water-tight DRP."

The power of three

Hackers are getting cleverer, and cyber attacks are growing. Ransomware and malware attacks may have declined in Ireland recently but phishing and trojans are still a huge threat and new hacks are created daily. Therefore, it is vital to not only to secure your data, but also to ensure that your data is recoverable, should your organisation be compromised. And you can be sure you will be at some point.

"We recommend three back-up copies: one on-premises, one in the cloud and one offline."

The first port of call is to ensure your data is backed up. You decide how many back-up copies are needed and where they are located, but there should always be one offline copy. At Trilogy, we recommend three back-up copies: one on-premises, one in the cloud and one offline.

The second is to create a disaster recovery plan and implement Disaster Recovery as a Service (DRaaS). A disaster recovery plan (DRP) is a documented process used to protect and recover IT data and critical services in the event of a disaster. It details what is expected of key personnel should an incident occur. DRaaS ensures that the organisations' critical applications are up and running based on the Recovery Point Objective (RPO) and Recover Time Objectives (RTO) set.

It is not just the huge growth of new threats that organisations need to prepare for, GDPR Article 32 “Security of Personal Data” explicitly recommends all organisations adopt data protection controls and the ability for data to be restored “in a timely manner.”

To manage this in an environment where there are skill shortages, means that businesses are turning to third parties to help. Managed Services Providers can manage the entire back-up and disaster recovery processes, ensuring they are encrypted and tested as per GDPR requirements.

Outsourcing business continuity and disaster recovery tech requirements gives companies peace of mind and frees up time for IT staff to concentrate on other areas.

John Casey is sales director with Trilogy Technologies

Data is the lifeline of your business – protect it!

Your company’s data is your most valuable asset.

It is not an overstatement to say that without your data, you have no business. All companies need to protect themselves against data loss which can happen due to a variety of factors from human error, software corruption to cyber-attacks. We often say, “it’s not a case of if disaster happens, but when disaster will happen”.

In addition, downtime is expensive; it leads to lost revenue, lost productivity, can prove costly to recover not to mention its’ negative impacts on your business’ reputation. Based on findings of the Aberdeen Group, one hour of downtime can cost small companies as much as €7,000; that’s approx. €68,500 for mid-size businesses and over €640,000 per hour for large enterprises. Further research shows that 90% of companies losing data from a disaster are forced to shut down within 2 years. Considering this, having a contingency plan is imperative to ensure total Business Continuity for your business.

“It is important to note that back-up is not equal to disaster recovery. Understandably, many people don’t grasp the difference between both. Yet the distinction is crucial.”

It is important to note that back-up is not equal to disaster recovery. Understandably, many people don’t grasp the difference between both. Yet the distinction is crucial. Broken down to its simplest, a DR solution is what enables you to restore quickly and efficiently when needed. Being able to back up is only one part of the equation and while ensuring that you take clean, regular back-ups of all your systems is essential, these back-ups have no value if you cannot restore quickly and easily when you are hit by hardware failure or a ransomware attack. Fully protecting your business involves getting copies of these back-ups offsite and one great option is to replicate to a purpose-built Disaster Recovery Cloud allowing you to literally flip a switch and failover to a secondary network running in the cloud in just minutes. Therein lies the difference between a Back-up and DR solution.

SMEs need a solution they can trust, one that will protect everything their organisation has within their data centre with the main objective being minimal downtime and zero data loss. Landmark Technologies can make business continuity and disaster recovery (BCDR) a less unnerving task, our partnership with StorageCraft allows the storage of data both locally and virtually.

For further information, contact Landmark Technologies LTD on (01) 620 550

info@landmark.ie * landmark.ie

Ken Kelleher is managing director of Landmark Technologies

Prevention is better than cure – minimising the risk of data loss with 2 simple steps

No more keeping fingers crossed.

Drive failures can go undetected and may occur anytime, and they will either lead to volume degradation or volume crashes. It is less of a problem if a hard drive failure results in a degraded volume since you only have to rebuild your RAID array by finding out the damaged drive and replacing it with a new one. However, it is a bigger threat when it comes to volume crashes. If you don't have a back-up plan or a DR solution in place, it is very likely that you're going to experience catastrophic data loss.

So, is there anything we can do to forestall drive failure?

Yes, there are two precautionary measures that we can take to minimise the possibility of data loss caused by drive failure: running regular SMART tests and setting up event-triggered notifications.

First, perform a SMART test on a regular basis to keep tabs on your drive health status and take immediate action when necessary. SMART is the acronym for Self-Monitoring, Analysis and Reporting Technology, which is a monitoring system used to gauge drive reliability and provide information on the current status of the drives. SMART attributes are examined by utilising several parameters to see if the drive is starting to develop problems. The results can serve as an indicator of the remaining lifespan of a drive.

"Is there anything we can do to forestall drive failure? Yes, there are two precautionary measures that we can take: running regular SMART tests and setting up event-triggered notifications."

Pay extra attention to the following three SMART attributes that are related to bad sectors: Reallocated Sector Count (ID 5), Reallocated Event Count (ID 196), and Current Pending Sector Count (ID 197). A bad sector is a cluster of unreadable data caused by wear and tear, over-heating, collision, file system error, etc. Upon detecting an impaired sector, it will be redirected to a reserved space – a spare sector. This reallocation process is called "remapping." Note, though, that increasing remapping operations will slow down drive access and may spell the end of your drive.

It is ideal to have a low value of the above attributes, as these values can be used as a benchmark to detect looming drive failures. Both Google's and our statistics show that these attributes are highly correlated to a higher chance of drive failure. Drives that have developed bad sectors are 10X more likely to result in failed drive access than those which don't have any bad sectors.

Other than running SMART tests regularly, the other thing you can do on your Synology NAS is configuring notification event settings in “Internal Storage” under the Advanced tab in Control Panel. Select the events and take necessary action upon receiving a notification message triggered by them.

Let’s get started with three common error terms: ICRC, IDNF, and UNC errors. An ICRC error is a communication problem occurring when data is transferred between the host and the hard drive, while an IDNF error occurs when the drive is unable to read data that is located at a corrupt sector. A UNC error implies that the data the hard drive attempts to read is damaged and cannot be corrected usingECC (Error correction code). The following are events3 related to these errors:

1. Drive reconnection (ICRC error) alert

2. Drive re-identification (IDNF error) alert

3. Drive reconnection alert when Synology NAS boots up

4. Alert of drive with read abnormality (UNC error)

When you receive a notification regarding any of these errors above, it could be an early warning sign of a failing drive. If the issue continues, it may suggest that the drive is not working properly. We strongly recommend that you back up your data and replace the current drive. Other than the above-mentioned alerts, there are three other events that you should pay attention to as well.

5. Bad sectors on drive increased

6. Drive I/O error

7. SSD lifespan warning4

Since accumulated bad sectors will gradually lead to data loss in the long term, you’ll receive a warning when the detected bad sectors are increasing. Bad sectors may also lead to drive I/O errors. However, your drive may be still working properly after several retries. If this error keeps occurring, please back up your data and examine the hard drive status by conducting a SMART test. By the way, you can refer to the Synology Products Compatibility List to check the expected lifespan of your SDD. Consider replacing your drive with a healthy one when you receive a warning, as it could be a sign of impending drive failure.

In general, it is only a matter of time before a drive fails, but we can take simple yet important precautions against drive failures before they ultimately lead to data loss. Take pre-emptive action upon receiving hard drive alerts, for ignoring these warning signs may cost you big when disaster strikes. You can take a more proactive approach by performing diagnostic SMART tests on a regular basis to gain insights into the current status of your drive.

In addition to these preventive measures, we also need to prepare for the worst by regularly scheduling back-up tasks in case of unexpected drive failures. Be well-prepared and you can minimise the possibility of data loss.

Vincent Tsai is a product marketing manager for Synology

Read More: 99999 back-up Datto Decisions disaster recovery Landmark Technologies Sungard AS synology Trilogy Technologies webroot

More Articles
← Previous Next →

Related Articles

Synology introduce DiskStation DS419slim for SOHO and first time users →

When an MSP becomes and MVP →

TechLife | TechPro | TechTrade | TechRadio | TechBeat | Blogs

Privacy Policy | Sitemap | About | Contact | Advertise

TechCentral TechFire TechTrade Tech EXCELLENCE AWARDS TechPro

TechBeat

Published by Mediateam Ltd., Ireland technology media leader since 1976,
55 Spruce Ave, Sandyford, Dublin 18, A94 N125.

mediateam