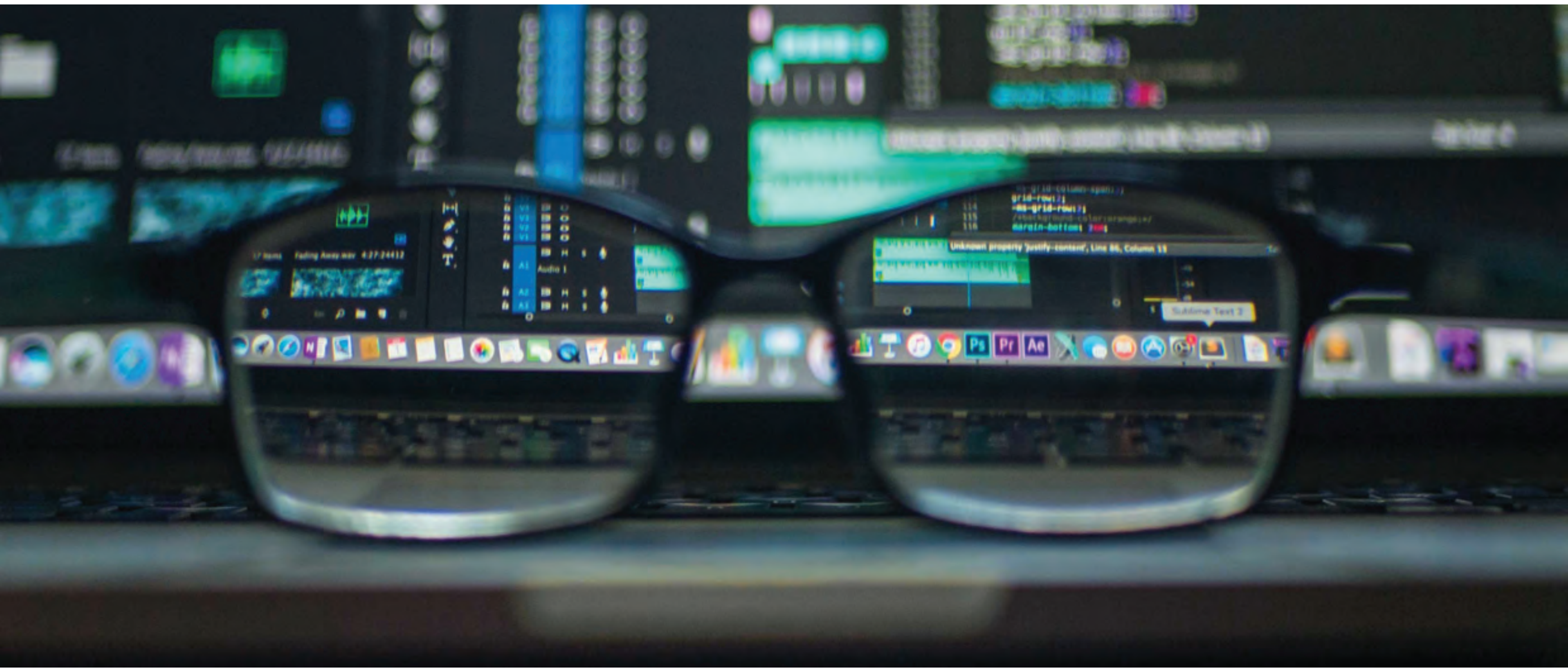
Abtec
Network Systems

White Paper for
IT Professionals



Building
Better Disaster Recovery Plans

Focussing on building a more effective DR plan to ensure your business is better prepared for unplanned outages

Andrew Beynon and Chris Topham
September 2018

Abtec Network Systems Ltd, Barents House, Market Harborough, LE16 9HW
Web: www.abtecnet.com Tel: 01858 438 500 email: enquiry@abtecnet.com

ABOUT ABTEC

Abtec Network Systems is one of the UK's leading IT, networking and communications specialists.

Recent projects include:

- Designing, deploying and managing the IT and communications infrastructure at the workers' villages for the construction **Hinkley Point C**
- Fit out of DALI lighting, CCTV, Cisco WLAN and fibre LAN for Amethyst Group's new 210,000 sq ft logistics unit
- Deploy and manage the IT and communications network for Imperial College's Translation and Innovation Hub offices

INTRODUCTION

When was the last time you reviewed and tested your disaster recovery (DR) plans?

For many small to medium enterprise IT professionals, the answer will be 'too long ago'. Yet, information technology is the backbone of a modern business. The 'always on, always connected' workplace culture demands the minimisation of interruptions and downtime.

Building DR plans can be complex and time consuming. Testing them takes co-ordination across the organisation and creates interruptions for the rest of the business. So, it come as no surprise that research indicates that too few companies formally plan and test disaster recovery scenarios.

What may be surprising to learn is that only a minority of SME businesses' DR plans will go beyond protecting an organisation's data. Protecting data, in particular personal data, is important; in fact all organisations that hold personal data are now obliged by the **Data Protection Act 2018 (GDPR)** to provide resilience for systems processing personal data.

But, a business is more than its data. There's the knowledge, processes as well as intangible elements such as how it communicates with clients. Can these be covered by your DR plans?

The aim of this whitepaper is to stimulate the steps to create a more effective, more encompassing disaster recovery plan. To enable you reduce downtime whether you're facing a major disaster or minor interruption.

GDPR

The Data Protection Act 2018, the UK's implementation of the General Data Protection Regulation (GDPR) stipulates that organisations should "ensure that any systems used in connection with the processing function properly and may, in the case of interruption, be restored, and ensure that stored personal data cannot be corrupted if a system used in connection with the processing malfunctions."

GOING BEYOND DATA

One of the objectives of a disaster recovery plan is to minimise the economic impact of interruptions to the business, regardless of the size of that interruption.

In essence, it used to support the business in getting to an agreed level of operations, enabling it to continue to function.

The majority of DR literature focuses on the protection of data and data systems from interruption. However, when we examine the most common causes of outages and interruptions we find that there are many disruptive triggers that affect IT resources beyond data and data systems. Mitigating these risks will help us build a better disaster recovery plan.

Let’s look at some practical steps we can take to broaden the scope of our disaster recovery plans.

STEP 1

BUILDING RESILIENCE IN THE INFRASTRUCTURE

Resilience and security should be at the heart of any good infrastructure design. However, that doesn’t mean having to duplicate every resource. There are a range of options to consider, depending on your budget and how critical those resources are to your organisation. For example; running your applications in a virtualised server environment, rather than bare metal; having a secondary circuit that can automatically take over if the primary fails.

The good news is that the true cost of implementing resilient services has reduced over the years. wide area network (WAN) costs have fallen dramatically, making them well within reach of most businesses.

QUESTONS TO ASK

- *What would happen if my primary WAN connection went down?*
- *How many internet applications, such as Salesforce.com, does my organisation rely on?*
- *How would external users, such as remote sites or homeworkers, be affected of the headquarters’ primary connection had an outage?*

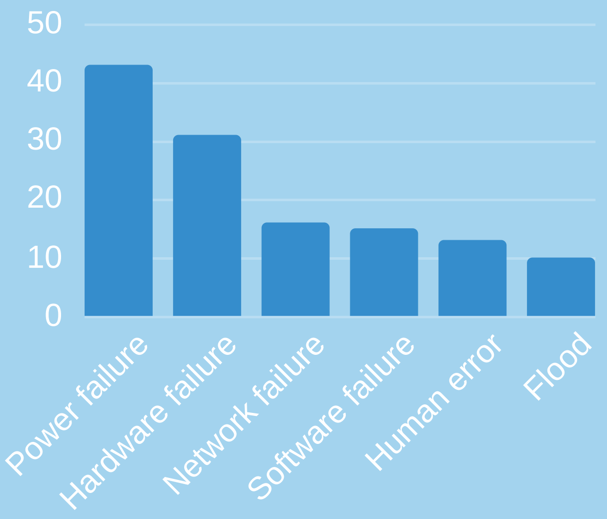
Causes of Unplanned Downtime

40%
Operations errors

40%
Application failure

20%
Environmental factors

Source: Gartner Inc, March 2014



Source: Forrester Research Inc

STEP 2

REDUCE THE RISKS

Prevention is better than cure. Spending time and budgets in reducing risks can be a much better use of resource than fixing issues.

Start by conducting an audit itemising the devices that access your network, and don't forget employees' devices brought from home. Disable unsecure protocols on your devices, such as Telnet, and remove default administrator accounts. Using non-standard port numbers for applications, SSH for example, won't remove a security threat, but it will remove an obvious target.

Identify the touchpoints that a possible threat could enter your infrastructure, and remember that it's the human link that is often the weakest. Email is a case in point. A good, cloud based, email filtering service will help keep many threats out of your network. This, along with a simple training programme to help employees to spot malicious emails, can greatly reduce risks.

Get into the habit of a server patching regime, making sure security patches are up to date. Also, consider using an infrastructure monitoring tool. A standard tool will inform you when a failure occurs on your network, and a sophisticated tool, like Cisco's Stealthwatch, can identify and alert you to unusual behaviour on your network, including attacks.

And if these suggestions are going to stretch your resource too far, consider bringing in a third party to help you. A reputable IT firm will be able to define and deploy a prevention strategy, it's what they do.

QUESTONS TO ASK

- *How many malicious emails does my business receive a day?*
- *Do my users know how to spot malicious emails?*
- *Do I know what devices my colleagues use on my network?*
- *How many insecure protocols do I use in my infrastructure?*
- *Are my servers' security patches up to date?*

STEP 3

THINK ABOUT YOUR CLIENTS

Disasters force organisations to focus on internal issues, such as; staff safety, regaining power, or stemming virus outbreaks. This is often at the expense of client relationships. During this period, do you still want to be able to communicate with your clients?

If your telephone system is housed in your premises, a power or network outage could stop all inbound and outbound communications. Your telephony provider may be able to divert your main telephone number to a mobile phone or another site, however, what about the rest of your direct dial numbers? The introduction of SIP technologies has given IT professionals much greater control over their communications, including the ability to rapidly divert individual Direct Dial In (DDI) numbers.

Similarly, for organisations that host their own email server, an outage could stop the flow of emails. This would not only affect users at that site, it would also prohibit homeworkers and remote site staff from using this service. Better options could be to migrate to a hosted email service, such as Microsoft Office 365, or co-locating your email server into a resilient, managed, data centre.

QUESTONS TO ASK

- *Where is my telephone system located?*
- *Can I divert all of my landline telephone numbers quickly?*
- *How would I access corporate emails in the case of an outage?*
- *What happens to emails that customers send during the outage?*

STEP 4

INCREASE THE AIR GAP

You perform regular backups of your data; great. But where do those backups reside? If they can be accessed from anywhere else on your network (no matter how restrictive the permissions) they are vulnerable. A common ransomware strategy is to infect backups before production data, rendering a roll back useless.

A useful backup methodology is the 3-2-1 rule:

- Have at least 3 copies of your data
- Use 2 types of storage media
- Use a different location for 1 copy

Ideally, that location should be air gapped, which means a site that cannot be accessed from the original network. Removing a tape, for example, from the original network site, to a remote location without access to that network, is a good example of air gapping. The problem with tape backups, however, arises when you want to restore from that media. As well as having to find replacement hardware to restore from and to, there's also the issue of the length of time to restore.

Another option to consider is to make that backup location in a private 'cloud'. A reputable IT service provider will be able to provide a secure infrastructure that uses an alternative authentication mechanism and even checks the integrity of the backups. Some providers will now even let you run your infrastructure from that cloud, ideal if you need to get your business back up and running quickly.

QUESTONS TO ASK

- *How regularly do I perform backups?*
- *Where do my backups reside?*
- *How would I restore my infrastructure from my current backup regime?*
- *What is my senior management team's expected timescale for restoring the infrastructure?*

THE HUMAN FACTOR

From our experience, many businesses will focus their efforts mitigating high impact, low probability events. A much more common cause of unplanned outages is the human factor. Take one of our clients, the landlord of a prestigious, multi tenanted, high rise commercial building. It had drawn up extensive DR plans for highly disruptive events such as fire, earthquake and acts of terrorism.

Yet, it was human error, in the form of a sub-contractor, that led to the top floor tenant's high pressure water supply flooding two of the building's communications rooms filled with switches, routers and servers.

The disruption lasted for four weeks – the cost of which is still being counted.

The point here is that often, it can be the smaller, human problems that cause more disruption than 'disasters'. In 10 years' time those human factor problems will far outweigh those caused by catastrophic events such as earthquakes.

STEP 5

SECURE REMOTE ACCESS

Snow may not be a disaster, but it could certainly cause disruption as key employees are unable to reach the workplace.

Supporting a homeworking policy can help provide resilience in your workforce. But as with everything else this needs to be planned, tested and monitored. There are a range of security option when it comes to network connectivity for remote workers. For occasional homeworkers a simple VPN connection may seem to be enough. There are, however, inherent risks with this approach. The area of risk is in authentication, particularly if your users don't have to set strong passwords within their Windows environment.

A solution to reduce this risk is to implement two factor authentication (2FA). 2FA services typically include a server application that connects to an Active Directory. This will provide a short duration code to the users, registered, mobile that they will need to enter, along with their login details, to access the corporate network.

These services are now widely available with the price range of small businesses.

STEP 6

UP IN THE CLOUD

If you have a number of business premises and your data centre is based at one of those locations, a local outage in the data centre could affect all users across the business. Moving all of your servers and data to a managed cloud environment might be a desirable option, but could be a difficult business case to sign off. Another option would be to create a hybrid, on premise and cloud, environment.

Migrating your critical data and applications could bring the benefits of higher availability, a reduction of operational costs and better resilience. If an outage occurs in your on premise data centre, important applications and data will still be readily available for your users.

QUESTONS TO ASK

- *What is my business' plan for its employees if a disaster were to strike?*
- *Is it appropriate for employees to access data remotely?*
- *How can we secure data, and prevent data loss, with remote workers?*

QUESTONS TO ASK

- *What are my current overheads in running my on premise data centre?*
- *What would be the impact of an outage in my data centre?*
- *How much would this cost the business?*
- *What are my business critical applications?*

CONCLUSION

By widening the remit of a disaster recovery plan beyond data, we can build a valuable plan that will enable the business to cope with a larger range of business interruptions.

Let's be realistic, some of the suggestions here require a significant investment of your human resource. You may feel that your IT team is already stretched. A better option could be to engage a reputable IT team who have a proven track record in creating DR plans. Your business could benefit from their experience, helping you create a working DR plan faster than if you were doing this in isolation. This way your business is better prepared, and you can focus on deliver excellent IT services for your users.