WHITE PAPER

A STRUCTURED APPROACH TO UNDERSTANDING, EVALUATING AND ASSESSING THE **DISASTER RECOVERY PLAN** FOR YOUR BUSINESS

Contents.

1 Introduction

1 Typical Architectures

2 A Classic User Case

3 How Does the Infrastructure Adapt to Failures?

- 3 Network components
- 3 Storage
- 3 Database
- 3 Web & DNS

4 Conclusion

"An effective Disaster Recovery solution involves the whole business, not just the IT Department."

INTRODUCTION

Developing an effective Disaster Recovery solution involves the whole business, not just the IT Department. It's imperative that there is participation from all functions, and levels, to ensure that the business as a whole is protected in the event of failure of a core system, or total loss of a major site, and anything in between.

TYPICAL ARCHITECTURES

With more traditional On Premise architectures, there are a great deal of options available to provide protection, but keeping the solution bias towards physical platforms may introduce significant limitations on how, and what to recover.

These can include:

- Hardware procurement cycle and costs
- Staff availability and utilisation
- Storage replication tools and knowledge
- Remote Access and Connectivity capacity
- Physical locations for additional hardware
- Out of Hours access to the primary site
- Data back-up plan, tape storage and restore schedule
- Fixed and mobile telephony platform

"An effective planning method is to break down the business into recognisable groups."

By working through these considerations to develop the plan, and ultimately the recovery solution, you can appreciate how to score the infrastructure and business by priority. Not only does this approach give you insight into how to carry out the recovery plan, it also makes the process of budget definition and allocation more straightforward. This in turn makes the business case easier to construct and present.

An effective method to achieve the necessary results is to break down the business into recognisable groups and associate the underlying ICT per group, location or function. This approach simplifies the identification of specific needs at a functional level, and become more generalised as you move away from the functional view to local, regional and repeatable elements, common to larger areas of the business.

annodata
wider choice, better advice
A KYOCERA GROUP COMPANY

www.annodata.co.uk

A CLASSIC USER CASE

Let's look at a fairly typical example, a business with 30 employees, with a Sales team, Customer services, HR, Finance, Admin and Management team and some Technical support/Delivery staff and two staff in IT.

"Being able to appreciate the effect of losing just one element of the infrastructure helps to identify the appropriate solution required to protect it."

MD X 1

- Senior Managers x 2
- HR x 2
- Finance x 3
- Sales x 10
- Admin x 3
- Technical delivery/support x 4
- Customer services x 3

THE HARDWARE PLATFORM IS ALSO FAIRLY CONVENTIONAL:

- Active Directory Server x 1
- Exchange Server x 1
- Application Server (CRM) x 1
- Application Server (Finance) x 1
- SQL DB Server x 1 (Clustered)
- Internal web (Intranet and Extranet) DNS and ancillary services server x 1
- Single system, dual controller storage (HP MSA)
- Single system, dual drive tape back-up (HP MSL)
- No SAN fabric – servers directly connected via HBAs
- Non resilient LAN hardware (Cisco or HP ProCurve)
- Non resilient WAN hardware – single router (no HSRP)
- Non resilient Security hardware (separate device from router)

The business is sales led, so ensuring the Sales team are supported is very high on the priority list when discussing the DR approach, although the technical staff still need to deliver what the Sales team sell, and the Customer service team always need to be contactable by the customers.

Working out the priority by function can become fairly complex, as each function has almost equal importance to the business in terms of its value and contribution, so it may be easier to start from where the staff are based.

Sales and Technical staff are usually out with customers, so the infrastructure has already been engineered to provide remote access to those groups, hot desks at the office and some form of mobility solution for when they are out. As long as the access to the data they use is maintained, these two groups are satisfied.

Customer services are all office based, and while the team is smaller, their role dictates how the systems are accessed and used, pushing them up the priority list. The same applies to Finance and HR, both functional groups are office based, both have specific systems that are fundamental to their role, and both have regulations around management of data, all things that dictate to some extent how the infrastructure is deployed, and then how it will be made available in the event of a recovery scenario.

The next groups, Management team, Managing Director and the Admin team have a similar set of requirements. Management team members require reporting data, and access to email, the MD needing high level reports presented, rather than needing direct access to the data to create their own. The Admin team all handle the data, quotes, forms, etc. to drive the business processes, and therefore generally require access to more systems than function specific staff, so their needs must be addressed in the plan in terms of how this access can be replicated in the event of a disaster.

At an infrastructure level, the business is contained within the boundaries of a small scale hardware, application and database environment, most of the services being shared across all functions, with the exception of the Finance Application.

The SQL database cluster is shared by Exchange and the CRM application, with a table assigned to the Finance Application to reduce the need for further hardware. The CRM is browser based, but locally installed, and the DNS/Internal Web server delivers this functionality to all users.

Exchange is used by everyone, and (based on this example of a single office) the LAN, WAN and Security hardware the storage is split across the applications and user data stores, backed up to tape and stored offsite. The telephony is Avaya IP Office, with both ISDN and SIP services enabled.

"All infrastructure elements are inter-related and the business could be impacted by a failure in any one of them."

HOW DOES THE INFRASTRUCTURE ADAPT TO FAILURES?

With a slightly clearer picture of the organisation we can determine how the current infrastructure will adapt to a focused failures within the site, and the impact to each of the functions of these failures.

"Disaster Recovery isn't a one size fits all approach. Each business is different and each application, group of users and company will have specific requirements."

NETWORK COMPONENTS

Network components, across the full scope – LAN, WAN and Security would stop the business operating if one or more hardware devices failed. The non-resilient solution means that users depend on a single device to deliver the connection, be that to their desktop/ laptop or centrally in the case of the router or Firewall. The connection itself in non-resilient, so if there were a failure of the plant outside the building and the cable to the site were cut, then there would be no Internet connectivity until the cable is restored.

STORAGE

The storage solution is next, on a similar level to Exchange, in that it's used by everyone, all the time, processing data for folders, applications, database and mailboxes, it is the data repository and a critical component of the infrastructure. While it has been deployed with dual controllers, and dual power supplies, the configuration must be that the system is configured for active/passive distribution, rather than load balancing to be able to take advantage of the resiliency built in.

Due to the performance characteristics of the database, both for the core applications and Exchange, there needs to be a high number of disks available for that storage group, with a RAID 10 (RAID 0 + 1) configuration. This solution does offer high levels of redundancy within the disk storage, giving very good protection at a local failure level. If one of the controllers fails, because of the active/passive configuration, then local resiliency is adequate to maintain system operation, sending out an alert to advise of the need to replace the failed controller.

DATABASE

Looking at the database application, SQL is split across a pair of servers operating as a cluster, allowing the compute and connection load to be distributed, but also providing local level resilience here too, should one server suffer a hardware component failure, the other server in the cluster is able to deliver functionality back to the applications. It is typical to size the servers in such a way that the load is evenly balanced, so that should such an event occur, there is little or no performance loss experienced by the applications and ultimately, the end users.

WEB & DNS

Another core component is the Internal Web/ DNS server that manages many of the ancillary tasks within the infrastructure. No DNS means no Internet connection, and in cases where there are dynamically allocated IP addresses to storage devices, Virtual servers etc., the name resolution service stops, and the device is no longer reachable. CRM systems that rely on these services and internal Web services will no longer be accessible by the users, and if the same server is used within the domain to provide IP addresses via DHCP, no new connections can be made within the network until the service becomes available again.

Losing DHCP and DNS when the business operates an IP telephony solution also limits the functionality of the system. Handsets cannot establish a connection to the server, and are unusable, and the server itself cannot make necessary connections within the network to operate correctly. If the CRM system uses CLI as part of the Customer service experience, this will also be unavailable until DNS is restarted.

If the tape back-up solution failed, aside from not being able to create and maintain sufficient copies of data, it also creates log file entries and alert notifications on the server, and places the log data into a volume on the storage device. If these alerts are not addressed, the log entries themselves can become problematic, by slowing the server down with the size of file generated, and slowing other services down should the volume fill up.

A similar issue arises with database housekeeping. As the database re-indexes it creates a temporary file that varies in size proportionally with the database itself. If there is insufficient space in the storage allocated to this, the re-index can stop, which may stop the database operating, and in turn stopping services supporting Exchange, and stopping other applications from working, but it can cause a wider failure on the storage device by taking up all available space, which would then mean insufficient headroom for everything using the storage device, and all services could stop until space is found and reallocated.

"Being able to appreciate the effect of losing just one element of the infrastructure helps to identify the appropriate solution required to protect it."

CONCLUSION

From this high level view it's easy to see how interrelated these infrastructure elements are, and how the business could be impacted by a failure in any one of them, and the importance of going through the process to assess each functional group within the business and how the underlying IT solution underpins what they do. Being able to appreciate the effect of losing just one element of the infrastructure helps to identify the appropriate solution required to protect it, and by knowing the interrelated nature of the rest means you are better informed on how to approach DR more holistically.

Disaster Recovery isn't a one size fits all approach, as demonstrated above, each business is different and while this is a fairly typical example of both the organisation and the systems supporting it, each application, each group of users and each company will have specific requirements. That's why Annodata have invested heavily in the skills and partnerships over 20 years to develop the approaches to the issue, and be in a position to offer industry leading solutions that cover every eventuality.

Annodata recognise the commercial challenges that are synonymous with more traditional DR solutions and offer innovative options that deliver exceptional results, while being commercially sensitive.

Annodata is one of the UK's longest standing providers of Managed Services, covering Document Management, Unified Communications and IT.

For more information on how Annodata can help you become a more efficient enterprise, please contact:
marketing@annodata.co.uk or Tel: 01923 333 333

annodata
wider choice, better advice
A KYOCERA GROUP COMPANY

www.annodata.co.uk

v1 – Sept17