The Questions:

For many years, there has been considerable activity in the usage of communications products and services, leading to the development of even more sophisticated networks & technologies that are now an indispensable part of our daily life. Such sophistication has meant that if there is an *"unplanned data outage"*, the impact and subsequent disruption is significantly greater, and is therefore more likely to impact on your enterprise.

How does an organisation build a data recovery plan for all occasions?

While there's no easy way to cover all of the requirements for the variance of data recovery plans, it is possible to limit the impact from any unplanned outage of data assets. The starting point for this should be establishing policies & procedures that can put in place as control measures for identified impacts, risks and threats - those that could affect your data resources - supported by a backup strategy. Such a strategy should begin with a concept of a data repository, and in the event of "loss", how fast does the enterprise data need to be recovered?

With "time" in mind, you now need to determine the Maximum Tolerable Period of Disruption (MTPoD) for your organisation. It will provide you with an indication as to the maximum amount of time that your enterprise's key products or services can be unavailable or undeliverable after an event that causes disruption to data operations, certainly before stakeholders perceive unacceptable consequences.

Alongside this there is a need to identify the Recovery Point Objective (RPO) for restoration of data, taking into account current methods of backing up, timings and scheduling, as well as the type of media being stored. It should be noted that the RPO when reviewed against the MTPoD may identify that there is a need for additional investment, and that a business case is required, factoring in the potential for delays in delivering your plan.

Alongside confirming the RPO and any additional investment, you should also be producing the Recovery Time Objective (RTO) from department/business unit Business Impact Analysis (BIA) results, and their list of recovery times for critical and essential technology assets.

With these results, as well as the time taken to backup data using current method(s)/network(s)/technology - taking into account Data Security and Data Retention - it is now possible to measure the value of "down-time"

in lost revenue and/or production and place a value against the data recovery time, thereby supporting on-going Disaster Recovery (DR) investment in "Organisational Resilience".

What are the pitfalls to avoid? How do you avoid them?

One would hope that most organisations have recognised the likely pitfalls that could happen, and how best to avoid them.

The "tender-loving-care" for managing **data** resources can sometimes become rather less important, as more interesting technology or applications are implemented. Whatever the case, enterprises must consider a minimum standard, detailed as such:

Pitfalls that should be avoided:

- Policies & procedures not observed
- Failure to backup all devices & systems
- Lack of long term archiving & record keeping
- Reliance on data recovery from various media sources
- Keeping operating system (OS) & virus control up to date

Avoidance measures:

- Monitor change of staff & access to systems
- Ensure backup processes & procedures are managed correctly
- Establish
- Check data
- Automate

Therefore, unless a rigorous approach is taken and regular testing & exercising of processes & procedures occurs, specifically relating to data recovery, the likelihood is that at a point in time you will need to recover critical data and without "something-in-place" it will go wrong!

What are the best practices? How do you implement them?

There are a range of best practices that any organisation should consider and take guidance, they are:

- ITIL (Information Technology Infrastructure Library)
    - Essentially, IT services should be explicit and strictly focused on client needs. This should be combined with clearly defined responsibilities for service provision within the IT organisation, and effectively designed IT processes. As a result, the IT organisation concentrates on the services required by the customer side, rather than being focused on technologies.
- ISO 20000
    - ISO/IEC 20000, like its British Standard; BS 15000 predecessor, was originally developed to reflect best practice guidance contained within the ITIL framework, although it equally supports other IT service management frameworks and approaches including Microsoft Operations Framework and components of ISACA's (Information Systems Audit and Control Association) & COBIT (Control Objectives for Information and Related Technology) framework.
- ISO 22301
    - This standard explains the purpose of Business Continuity Management System (BCMS), a management system used to manage business continuity and controls within an organisation. Bringing business continuity deliberately under overt management control is a central principle throughout the ISO/IEC 22301 standards. Its predecessor was British standard; BS 25999.
- ISO 27000
    - This standard explains the purpose of an Information Security Management System (ISMS), a management system used to manage information security risks and controls within an organisation. Bringing information security deliberately under overt management control is a central principle throughout the ISO/IEC 27000 standards. Its predecessor was British Standard; BS7799 – Part 2.

As far as implementation is concerned, "one size" does not fit all, in fact each organisation has (or should have!) developed its data resources over a period of time using different processes & procedures.

The key objective is to gain agreement on the "risk appetite": how important and valuable is the information held electronically for your organisation?

Sometimes the answer is readily available, sometimes not. Generally the level of risk is dependent on the type of operations being conducted or the engagement with Stakeholders. Whatever the case, decisions have to be made as to the importance of data, and the "depth" of best practice to be implemented.

What else needs to be considered when creating a data recovery plan for all occasions?

A realistic impact analysis of systems should see the 80/20 rule at work, where 20% of high-risk and mission-critical systems require 80% of the available resources. It is therefore critical that organisations recognise which system(s) are critical, and those that are essential, putting in place specific data recovery measures.

The key areas for consideration are:

- Cost;
    - Space (i.e. own or third party, on and/or off-site)
    - Distance (i.e. network provision, commissioning, purchase and/or rental, maintenance)
    - Speed & Capacity (i.e. Fibre/high bandwidth network to secondary site)
    - Complexity (i.e. tape, mirroring, replication, electronic vaulting mix)
        - Tape
            - On and/or off-site (e.g. in-house storage, third party)
        - Mirroring
            - On and/or off-site (e.g. shared or secure area)
        - Replication
            - On and/or off-site (e.g. Cloud)
        - Electronic Vaulting
            - On and/or off-site (e.g. Storage Area Networks (SAN))
- Challenges;
    - Data replication on backup media
    - Long term archiving & record keeping
    - Data recovery from various types of media
    - Disaster recovery delivery of RPO & RTO to users

Any organisation seeking to protect itself by providing specific resilience measures to protect its information resources must be prepared to invest time and effort into due diligence activities, thus ensuring an acceptable level of service assurance that will ensure data recovery. This investment must continue to be reviewed over its life cycle, taking into account changing technology and changing business requirements that could put at risk any backup and recovery arrangements. These kinds of preparations ensure that resilience is maintained, and kept operationally ready for a time when there is a service disruption and you need to restore critical data for your enterprise to survive.

References:

https://en.wikipedia.org/wiki/Backup

http://www.wikihow.com/Back-Up-Data

Author:

Steve Yates FBCI, FICPEM, MEPS

Director

Acertia Limited

Telephone: +44(0)845 5678 999

Email: steve.yates@acertia.co.uk

Website: www.acertia.co.uk

"The key objective of Acertia is to give organisations full confidence in the effectiveness of their resilience plans and business continuity - following delivery of appropriate consultancy and training - from development through to full testing and exercising"