CIOs and "Data Protection"

Data Recovery Success is the important criteria not Backup

By Tony Lock, October 2010

Originally published by

The following article was originally published as part of the Freeform Dynamics advisory column on CIO Online. This is focused on the business impact of development in the technology industry. Original articles can be accessed at www.cio.co.uk (registration required).

The rapid growth in the amount of stored data means that the importance of data protection has never been greater. It is surprising then that few organisations find the time to proactively develop data protection strategies. In the majority of companies data protection evolves, at best, in an ad-hoc manner. In some organisations it does not change at all until an event focuses attention back on this core requirement. Little attention is spared to look at whether the strategy is effective, cost-efficient or comprehensive until something goes wrong.

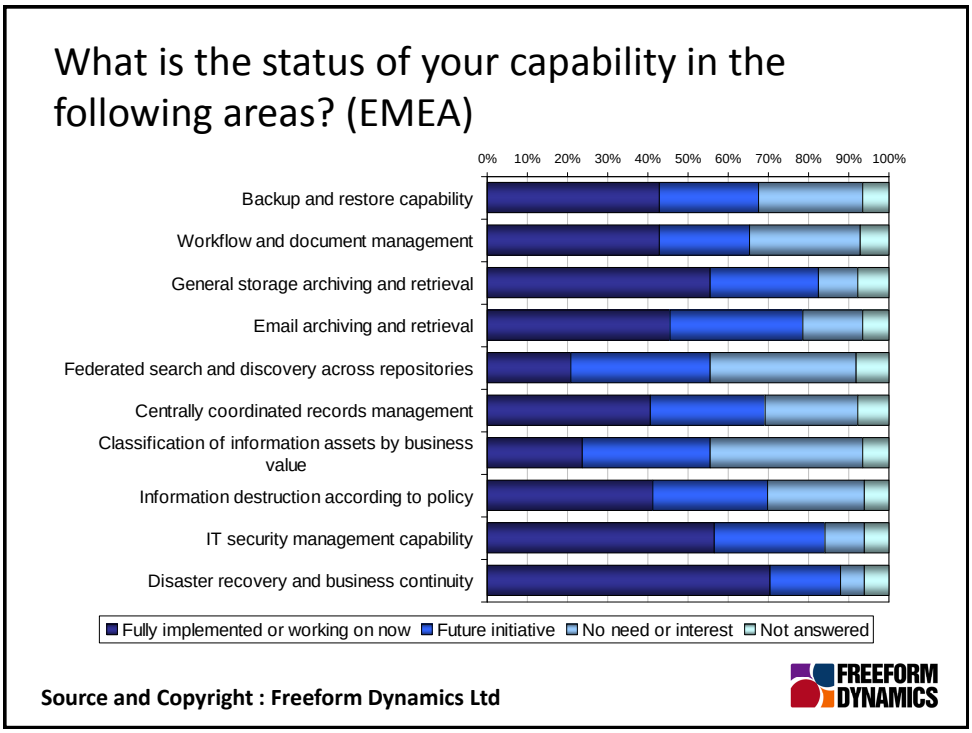
Data protection is anything but new, but changes are happening that are expanding the capabilities as well as the urgency of practical implementations. The last few years have witnessed a huge wave of technological developments advancing both well-established solutions - for example backup and recovery - as well as introducing new offerings such as Data Loss Prevention (DLP). These new technologies are being given an added impetus by the rise of data protection legislation that is imposing tougher penalties on both companies and executives where data breaches occur, as well as expanding protection with concepts such as data breach notification. There are also growing regulations that are forcing the recovery of certain data to happen within much shorter time windows than have been acceptable in the past.

In general terms data protection can be considered to encompass the following areas:

- Data storage and availability – raid, replication, tiered storage, etc.
- Backup, recovery and archiving
- Data privacy and disclosure – Encryption, key management, legal discovery, etc.
- End of life – secure data disposal

Just considering the fundamental processes of data backup and recovery is enlightening. Organisations have been undertaking this task ever since IT started yet few managers are convinced that they have systems that cannot be improved. The figure below shows the results of a

survey of European organisations. Fewer than half of organisations consider that they have fully implemented backup and recovery processes.

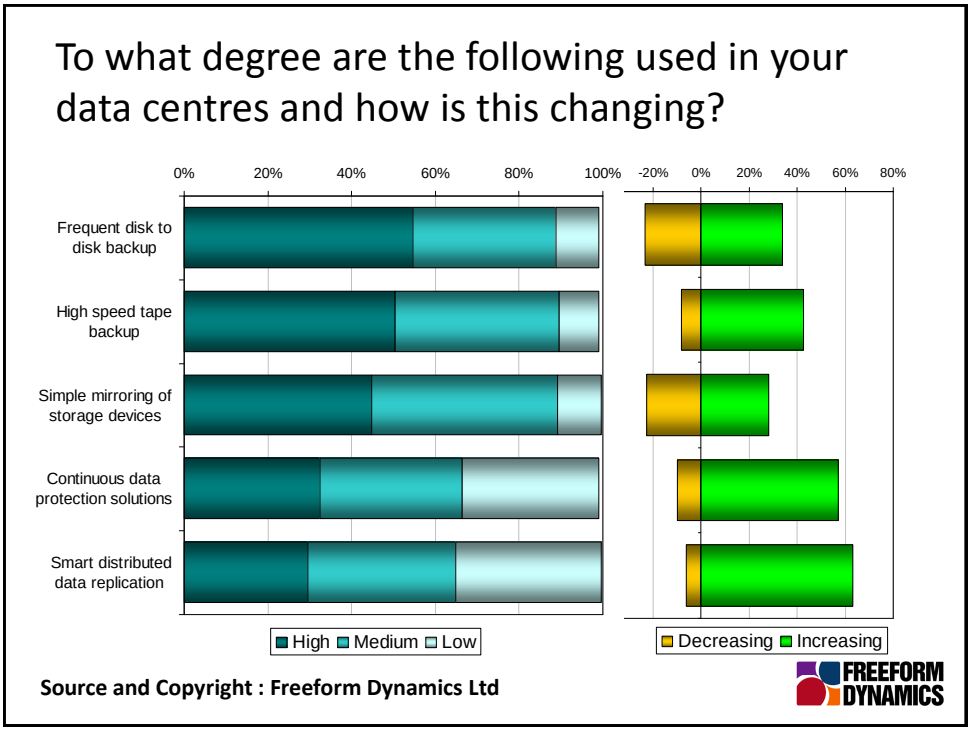


Perhaps the most surprising result is that nearly one in four respondents feel that they have no need or interest in backup and restore capabilities, even if this is the most vital and basic form of data protection for all types of information. This is a damning indictment, as even home users are starting to recognise that they should do something to protect their important data should they experience some form of computer or hardware failure. However, it must be admitted that whilst recognition of the need amongst consumers is high, most do it poorly or in a haphazard fashion at best and most often after a painful lesson in reality.

Given the importance of data protection and how little attention backup, and particularly recovery, receives until something goes wrong, this is an area CIOs should take some time to reconsider. Improving this aspect of data protection can dramatically improve risk reduction whilst the "do nothing" approach holds the potential to lead to expensive disaster or even ruin. It is worth spending some time evaluating just what the real state of affairs here is, and that includes regular "real world" demonstrations, not just completed processes. The result is certain to be "enlightening".

There are many ways in which the primary data protection tasks of backup and recovery can be modernised from the traditional "backup to tape" approach that has dominated IT for decades. New options – such as snap shots, point in time copies, replication, backup to disk to tape (B2D2T) and Continuous Data Protection (CDP) - can decrease the cost and increase the effectiveness of data protection, demonstrably reducing operational risk.

Each of these has its benefits and can be deployed independently, but integrating them together can result in an optimised solution where the whole is more than the sum of the parts. The combinations of different approaches to protect data may allow the organisation to better protect its operations, for example by combining snap shot systems to allow very fast data recovery, coupled with remote replication for resilience and backup to tape at the remote location for long term data retention.



A glance at the chart above highlights that use of new data protection technologies is beginning to gather pace. Putting together the business case for investment based on ROI alone may be challenging, unless there are very obvious business requirements for data protection to be met. Looking at the overall business value of the solution should take into account the operational risk of not investing.

CIOs should focus on the speed and reliability of information recovery and increasing to the availability of data. That said, another technical driver exists, especially for replication and snap shot solutions. In certain situations it may be difficult, or sometimes even impossible, to run standard backup jobs within the available time windows increasing the burden on IT infrastructure during peak hours or leaving the business at risk with incomplete backups. Equally, a business requirement for resilience and disaster recovery can be behind the adoption data replication solutions.

With new technologies available and long standing challenges still unresolved, now is a good time to look again at how to manage your data protection systems, particularly around backup and restore. For many, for too long, things have carried on just the way they always have simply through having a lack of focus or dealing with other pressing priorities. It's not just the business that is demanding this - the increasing weight of legislative drivers along with industry regulation and data privacy requirements make doing nothing an untenable option.

About Freeform Dynamics

Freeform Dynamics is a research and analysis firm. We track and report on the business impact of developments in the IT and communications sectors.

As part of this, we use an innovative research methodology to gather feedback directly from those involved in IT strategy, planning, procurement and implementation. Our output is therefore grounded in real-world practicality for use by mainstream business and IT professionals.

For further information or to subscribe to the Freeform Dynamics free research service, please visit www.freeformdynamics.com or contact us via info@freeformdynamics.com.