BIZCOMMUNITY

Avoiding the consequences of data loss

By Gareth Tudor

29 Aug 2013

Protecting data has become of the utmost importance for organisations today, as information if the lifeblood of a business. There are many consequences should sensitive information fall into the wrong hands, however, as the workforce has become increasingly mobile, protecting all of an organisation's data has become more complex and challenging.

In order to avoid the pitfalls of losing confidential data, both regulatory and to the continuity of the business itself, it is critical to have an all-encompassing, secure backup, recovery and data protection solution in place. These solutions should incorporate protection of the mobile workforce as well as office-bound data contained on PCs and servers, and in data warehouses and data centres.

Compromising data is a very real possibility, for many reasons. Hard drives and other hardware components may fail, data may be corrupted, natural disaster such as flooding or fire may strike, and equipment containing information may be stolen, amongst other challenges.

Mobile workforce

Naturally, the mobile workforce is especially vulnerable to loss of devices containing company data. Today, many employees and executives use laptops, tablets and even Smartphones enabling them to work on the go. This means that these mobile devices contain significant amounts of business information, from emails and documents to client details and even sensitive company information such as financials. As mobile as they are, these devices are more prone to being lost and stolen, and this information could easily fall into the wrong hands. Aside from the inconvenience of losing these devices and their data, regulations and guidelines such as King III and the Consumer Protection Act impose harsh penalties on organisations that do not take every conceivable measure to safeguard sensitive and confidential data.

Added to this challenge, the loss of information can impact a person or organisation's ability to work. Without backups, business continuity can be adversely affected, and several studies show that the majority of organisations that are unable to recover their information following a significant data loss event will fail within a short period. In the information age, data is absolutely critical to business, and must be protected, backed up, secure and available, and able to be recovered at short notice.

Offsite cloud-based backup is one of the most comprehensive options available today for protecting and enabling the recovery of data, removing the manual tasks associated with tape-based backup and enabling geographically independent, automated and continuous backup. Data can also be accessed from anywhere, and recovered quickly to any device, ensuring organisations and individuals are back up and running with all of their information in the shortest possible time.

When considering cloud backup solutions, however, it is important to select a secure solution from a reputable service provider that meets the regulatory requirements and compliance objectives of any particular organisation. This ensures that data is always available remotely, and is always recoverable while meeting best practice and regulatory guidelines.

Backup is critical

For mobile devices, as well as PCs and desktops, backup is also critical to ensure that should these devices be lost or stolen, the information they contain can be recovered. Cloud-based backup has the additional advantage of catering to a mobile workforce, as it is not geographically dependent. However, preventing information on Smartphones, tablets and PCs from falling into the wrong hands relies on more than just data backup, since if these devices are stolen their information can be compromised.

Data encryption is another innovative cloud-based service that can assist organisations to avoid the consequences of data loss. Using these tools, data on a variety of devices can be encrypted, with security policies attached to various portable media, including mobile devices as well as external hard drives, flash drives, CDs and DVDs. This means that even if a device itself goes missing, without the encryption key the data itself cannot be viewed. Encrypted data is password protected, and following access management rules can be forced into quarantine should the device containing the data go missing. Drives can even be remotely wiped if necessary to prevent data falling into the wrong hands. In conjunction with cloud-based backup and recovery, this data can then be recovered to another device and the person can carry on working with minimal disruption and risk to the business.

Data protection is something no organisation can afford to be without. When it comes to comprehensive protection and security, cloud-based technologies are often the ideal solution for backup, recovery and encryption, ensuring that information is backed up and easily recoverable, and preventing information from falling into the wrong hands.

ABOUT GARETH TUDOR

Gareth Tudor is the CEO at Altonet, an ISP and provider/integrator of backup and restore solutions. Tudor started his career in finance after he qualified as a chartered accountant (SA) and has subsequently garnered a wealth of experience in a number of businesses, including his own.

- Metadata - playing a vital role in back-up and recovery - 3 Sep 2014
- How secure is your critical data in the cloud? - 18 Aug 2014
- Leveraging the advantages of BYOD - 19 Jun 2014
- Avoiding the consequences of data loss - 29 Aug 2013

View my profile and articles...