TANDBERG DATA
Securing your Information

Archiving and Compliance

Over the last several decades, businesses have become even more aware of the need to back up and archive their data as part of their overall business continuity and disaster recovery plans. To protect themselves adequately, businesses must improve how they manage and safeguard their organizational data and records. Good records management includes both backup and archiving.

While backup and archiving are often used interchangeably, it is important to distinguish between the two terms. Backup is used for short term data recovery. Data archiving is used for long-term data retention and regulatory compliance requirements.

Archived files can be kept for decades, usually at an offsite location and keeping more than one copy is essential if you want to properly safeguard your data. Tape is typically used for archiving because of its affordability, archival life (30 years), reliability and portability.

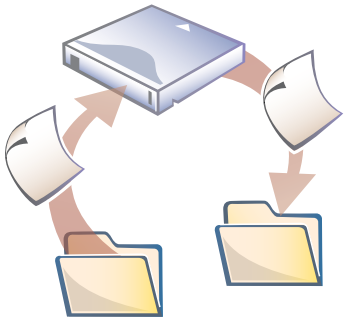
Research into disk access patterns on a NAS at the University of California, Santa Cruz, discovered that 95% of data is never accessed beyond six months from creation, but most of this data needs to be maintained for compliance. Additionally, archiving unused data to tape significantly reduces data centre costs. Research by the Clipper Group has shown that *a tape archiving solution is 23 times cheaper to run than a disk solution and consumes 290 times less power than disk*, allowing companies to reduce costs to meet their green initiatives.

The key to success for any backup or archiving solution is its simplicity; how easy it is to restore the data at a later date. It's important to acknowledge that legal requirements affect different types of data and business sectors in unique ways, additionally legal requirements vary from country to country. The first challenge for an organization is to understand its legal obligations—what are the data retention periods, does the data need to be encrypted or stored in a non-changeable format like WORM (Write Once Read Many).

Many businesses have been slow to react; they are putting their data and businesses at risk. Greater than 50% of SMBs have no documented procedures for protecting data and only 20% regularly encrypt data as it is backed up to tape. So what are the issues?

- **The lack of clear responsibility in IT organizations** – is it a storage or security issue?
- **Concern over security measures** – what's the impact on recovery times?
- **Cost** – is there a budget?
- **Complexity** – what technology should be used?

Archiving and Compliance



It's important to note that implementing proper procedures and processes for data management (backup, archive and compliance) will actually benefit the organization:

- Reducing IT operating costs overall
- Supporting litigation or avoiding the issue in the first place
- Speeding up investigation of issues

ELECTRONIC DATA AND LITIGATION

Failure to have the best possible archiving system and procedures could mean the difference between winning and losing an important legal case. It may also have a significant impact on the cost of the litigation. A poor document or electronic data retrieval system would mean added expense, in the form of experts required to filter and investigate all the available electronic data. The cost of electronic disclosure is expensive and it is also taken very seriously by the courts.

As anyone involved in IT security will know, some of the greatest threats to an organization come from within. In many instances email and digital information will provide evidence of wrongdoing. As many employers will know to their cost, employees are well protected under law, and the employer needs to be sure of its grounds before making a dismissal. Without the ability to retrieve reliable digital information from emails, etc., an employer will be exposing itself to unnecessary risks.

In most cases, a wronged party has six years from the date that a contract has been breached or a civil wrong committed to bring a court action. Even when a court action is taken promptly, a case may not come to court until several years after the event, and memories of the exact events will be hazy, or those involved may be unwilling, or unavailable as witnesses. Often the only clear evidence will be contained in digital information.

A party in a dispute may have a significant advantage over its rival if it can retrieve the evidence faster and at a lesser cost than the rival. The lack of readily available evidence may lead to a settlement of a dispute that might otherwise have been successfully fought and won

SARBANES-OXLEY

The Sarbanes-Oxley Act is a piece of US legislation that regulates financial reporting. Passed in the wake of the Enron episode and several other notable financial scandals in the US that involved suspect financial reporting, the Act was designed to revive investor confidence by compelling US companies to produce accurate and transparent financial information. Any company with a listing on NASDAQ or the New York Stock Exchange has to comply with the Sarbanes-Oxley Act, even if it is a European company with headquarters outside the US. UK subsidiaries of US corporations are usually required to ensure that the transactional data that they hold and share with their US parent will meet the requirements of the Act.

Sarbanes-Oxley requires that strict records retention policies and procedures must be in place, but it does not specify a specific data storage format. It does require corporate officers to implement internal controls on their information to ensure completeness, correctness, and quick access. One exception to the specifics: accounting firms are specifically mentioned in Sarbanes-Oxley. The act calls for

accounting firms that audit publicly traded companies to keep related audit documents for no less than seven years after the completion of an audit. Violators can face fines of up to $10 million and 20 years in prison.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

As most companies realize, compliance with the PCI DSS is difficult. Unlike other security-focused regulations, such as HIPAA and SOX, much of the PCI DSS is highly prescriptive. The intent of PCI DSS requirement is pretty straightforward: It's designed around the idea that the fewer people with access to resources, the fewer opportunities there are for those resources to be compromised. This includes access to both the data itself, as well as the to the systems that store, process and transmit that data. The requirement specifies measures to ensure organizations manage and govern user access according to the principle of least privilege—defining (and approving) which personnel need what levels of access to do their jobs, and limiting access within systems to only the minimum required.

For those involved in the PCI DSS compliance process, encryption can be confusing, however the PCI DSS is explicit that merchants must use encryption this includes data at rest and data stored on backup tapes at off site locations.

SUMMARY

Tape is tried and tested and it forms the last line of defence for many organizations (what if the unknown happened?). Tape technology has evolved significantly; LTO tape, for example, is generally two times faster than disk, and offers large storage capacities up to 3TB compressed on a single cartridge. Tape also supports WORM and encryption, allowing data to be safely and securely stored offsite. The use of encryption can also be used to manage the lifecycle of data. By deleting or destroying the encryption key, organizations can effectively destroy data stored offsite, without having to retrieve individual tapes.

Today, businesses can choose from a variety of backup technologies and solutions to protect short-term data. For long-term data storage and compliance requirements organizations should look to utilize tape. As stated, the key to successful archiving is to understand legal obligations and to implement good procedures and processes for the protection of data, whether short- or long-term.

About Tandberg Data

Tandberg Data is a leading global supplier of data protection solutions for small and medium-sized businesses. The company's wide range of cost-effective storage products and services provides customers with best-in-class tape, disk, removable disk and software solutions for backup, archiving and disaster recovery. These solutions are marketed through a global channel of qualified resellers, distributors and major server OEMs. An extensive service and support network supports all Tandberg Data products worldwide.

WP-ArchiveSolutions_EN_2012

Tandberg Data GmbH
Feldstrasse 81
44141 Dortmund
Germany
Tel: +49 (0) 231 5436 - 0
Fax: +49 (0) 231 5436 - 111
00 800 8263 2374 (00 800 TANDBERG)
salesemea@tandbergdata.com
www.tandbergdata.com/emea

Tandberg Data Corporation
10225 Westmoor Dr., Ste. 125
Westminster, CO 80021
USA
Tel: 303.442.4333
Fax: 303.417.7170
Toll Free: (800) 392-2983
sales@tandbergdata.com
www.tandbergdata.com/us

Tandberg Data (Asia) Pte Ltd
Trivex Building,
8 Burn Road,
#09-02/03,
Singapore 369977
Tel: +65 6593 4700
Fax: +65 6281 7358
salesapac@tandbergdata.com
www.tandbergdata.com/apac

Tandberg Data (Japan) Inc.
Dai 6 Ito Building 5F,
4-4-7 Ebisu, Shibuya-ku,
Tokyo, 150-0013
Tel: +81 3 5475 2140
Fax: +81 3 5475 2144
TDJ_sales@tandbergdata.com
www.tandberg.co.jp

TANDBERG DATA
Securing your Information