



[SC Magazine UK](#) > [Features](#) > [Storage: Locked up](#)

Barry Mansfield

October 01, 2007

FEATURES

Storage: Locked up

Faced with ever more data to be kept, tougher regulations and high-profile security breaches, it's time to rethink storage.

Storage: Locked up

Storage: Locked up

As most information security professionals already know only too well, the steady stream of data loss incidents hitting the headlines is not doing them or their employers any favours. And we are not just talking about wayward laptops. Recall the Time Warner debacle of 2005, when the names and social security numbers of around 600,000 of its employees were lost after crates of backup tapes went missing. And there have been other cases where storage media has been compromised or stolen.

A survey commissioned by storage company Decru questioned 100 UK IT directors in the financial, manufacturing, retail, distribution and transport markets. The results showed that in a quarter of the companies surveyed, 50 per cent of IT staff had access to read sensitive company information. In the retail, distribution and transport industries, this figure was even higher.

The full implication of this survey becomes clear when you look at the numbers. The companies polled each employ between 1,000 and 3,000 staff, and typically have up to 50 and 70 people in the IT department - that means around 2,240 people have access to confidential data.

Carl Greiner, senior vice-president for infrastructure at analyst group Ovum, points out that most data is still stored in the data centre, which is usually very secure. The problems arise when it is accessed by people who are not supposed to see the information, or when it leaves the data centre entirely, having been transmitted to another site for backup recovery or if the tapes are despatched to an offsite archive. "It's the latter event that gets a lot of press when something goes wrong," Greiner says. "The data has to be taken out by an assigned individual.

Companies have to do the risk assessment to decide which employees should have access to what data. That hasn't changed and never will, even if you encrypt the tapes. If that individual has the encryption keys, then he or she can still get at it. As an organisation, you're only as good as your initial defences."

The limitations of encryption

There are good reasons why companies haven't been encrypting their backup information in the past. The main stumbling block has been that, until fairly recently, most solutions on the market were too slow or too complex to be integrated into already intricate IT environments. Back in 2005, industry analyst firm Enterprise Strategy Group claimed that 93 per cent of companies were leaving their tape backups unprotected, trusting the drivers who delivered them to offsite storage locations.

But it seems that corporates, at least, have now learned their lesson. "We're seeing more and more companies choosing to encrypt tapes as they go off to the archives," says Greiner. "When you transmit data between locations you can encrypt the data too, but there is an overhead associated with that. There are many approaches. Compliance laws mean firms need the right setup for the environment they are trying to support. It's not a case of one size fits all."

Greiner believes the finance sector, being so heavily regulated and with the most to lose, is more switched on to the importance of secure storage. He thinks that most corporations are now "very astute" and know their requirements.

"It is a mixture of technology advances and new compliance laws that have transformed the attitude of business to storage security," says Greiner. "Going back in time, most of this information was on the mainframe. Now, all of a sudden, we are putting in SAP and doing enterprise resource planning (ERP) and human resources. Firms may not have put the proper security around these when they had them on the mainframe."

Sign of the times

The proliferation of mobile technology often accounts for oversights in security. "IT management can't really secure what's on somebody's laptop," Greiner points out. "People have minds of their own, so you have to try to instil some security mechanisms in your employees they can follow."

Technology is having an impact too. Storage capacities have grown in size dramatically and cost has fallen, while read/write speeds are faster than ever. All of this has an effect on accessibility, and the need for secure storage strategies needs to be carefully worked out. Information security professionals need to think about which technology is best for different applications and who uses it. Disk and tape technologies can be used side by side in many organisations.

So are boardroom attitudes to storage security really changing? Greiner thinks so. "I've noticed that audits have been more complete," he says. "CSOs have been asking the right questions. To follow up does cost money, of course, but I think the risk is now recognised more widely. Secure storage remains on the agenda because the regulations are constantly widening to encompass different types of data. Personal information wasn't always considered critical from a corporate perspective. In earlier days it was all about protecting financial information, but now that's been extended to personal details. So organisations have had to keep their eye on the ball."

However, Sue Clarke, a senior research analyst at Butler Group, maintains that the attitude of UK-headquartered companies still has some catching up to do compared to the US. "I don't think organisations are taking security seriously enough here," she says. "And I don't believe they will in future, until we have disclosure laws similar to the California Security Breach Information Act (SB-1386) that require you to come clean when personal information has been compromised. In the UK, those who do come clean and are honest about security breaches are fined. So what's the incentive to own up to the mistake?"

A question of priorities

Perhaps attitudes to data security will gradually be transformed as a result of a growing trend in the industry. Against the background of massive data growth across all industries, information lifecycle management (ILM) has come to be accepted as a critical business goal. Most organisations realise that they cannot simply continue to store and then blindly manage data of all types on primary storage media.

Information with immediate relevance to active business processes merits a place on high-performance and high-availability primary storage. It also warrants special attention, with frequent or continuous data protection and business continuity processes in place. Most data, however, has no immediate relevance to a company's ongoing operations and does not need to be highly available or rapidly retrievable in the wake of a systems failure or disaster. An ILM survey commissioned by BridgeHead Software suggests that 80 per cent of data has not been accessed within the last 90 days, and at least 60 per cent will never be looked at again.

Nigel Ghent, UK managing director at EMC, regards ILM as a powerful IT strategy, based on the simple fact that not all information is created equal. "Today's urgent email is more important than last year's staff memo," he says. "Over time, the value of information keeps changing. That urgent email may become a critical element for legal discovery or just more data cluttering your storage infrastructure. Based on its changing value, your information requires different levels of accessibility, availability and protection. This is at the heart of ILM."

Non-critical data does not need to be stored on the most expensive storage technology or consume the expensive equipment and operational costs of continuous or frequent data protection and recovery infrastructure. Because the odds that this information is going to be accessed are decreasing with time, the underlying data can be migrated to progressively less expensive media.

ILM in action

South Yorkshire Police is aiming to make cost savings of £1.1 million over five years by adopting an integrated ILM strategy from EMC, enabling the force to deliver the right level of protection, replication and recovery, at the lowest possible cost. Roy France, IT manager at South Yorkshire Police, wanted to move large volumes of older information to online storage media. This project is a good example of how it is possible to save money in doing so without compromising security. It also enabled the force to make historical data quicker to recover.

"Everything the force does is concentrated on the fast, continual retrieval of information, and we need to be certain that information is always available, year after year," France says. He cites the example of an individual stopped for motoring offences who gave false identification details but was later found to have outstanding convictions for a serious offence committed 20 years ago.

The difficulty in implementing ILM is that it requires the entire organisation to be disciplined, systematically classifying information so that IT management of the underlying data can be clearly defined and automated. Few organisations can claim to have reached this level of information management.

The next generation

In the meantime data is still growing exponentially. This has made room for data lifecycle management (DLM), which involves the automatic fine-tuning of the placement and management techniques used for data throughout its lifecycle. DLM operates on what the company already knows about data from its attributes and textual or other analytically induced content. From the resulting data classification, policies can be created to automate the repositioning of data.

Protected DLM goes further, enabling archives to be written with multiple copies dedicated to multiple media types and locations, automatically backing itself up and providing rapid accessibility for disaster recovery scenarios.

The arrival of protected DLM shows that the new technologies are reaching maturity, but it still struggles to justify itself in the absence of a business and legal culture that adequately promotes security awareness. With disk capacity and speed constantly improving, tape is certain to play less of a role in the storage industry in future. But the need for encryption and authentication will remain. The ability to store ever increasing volumes of valuable data internally, combined with a relatively weak regulatory framework outside the US, means that enterprises will continue to take risks with their data - and are likely to be hit even harder when they do suffer a breach.

The state of California's example shows that business will only take action when reputations are on the line. As other jurisdictions adopt US-style data protection laws, and the true frequency and scale of security breaches in the data centre comes to light, secure storage is certain to become the talk of the boardroom in the rest of the world.

CASE STUDY: ROGERS STIRK HARBOUR + PARTNERS

Global architectural practice Rogers Stirk Harbour + Partners has offices in London, Barcelona, Madrid and Tokyo and an international project team of 150 architects. The firm's projects includes Heathrow's Terminal Five, the Millennium Dome, Lloyds of London and Madrid's Barajas Airport.

According to IT manager David Liu, there were several driving factors behind the partnership's decision to change its storage setup. "One of the reasons was that, as a growing international firm, we need to ensure that our data is accessible 24/7 across the globe," he explains. "The solution had to be able to evolve with our changing requirements."

There is a legal obligation for architectural firms to retain drawings for the lifetime of the structure, Liu says. Project plans must be stored meticulously as well, to ensure safe and reliable backup for architects who need to recover large files as quickly as possible. Having to handle large computer-aided design (CAD) files in addition to digital blueprints, large bitmap files and daily email and word-processing documents puts a great burden on storage systems. "CAD files can be several hundreds of megabytes in size, and with the number of files growing, this was proving a drain on our existing storage solution. The access times were just not fast enough," Liu recalls.

The firm needed to centralise and consolidate its existing applications and disk-to-tape storage setup. The challenge was that it needed to consolidate different types of data, such as Exchange and SQL files. "Many of the service providers we approached were only able to offer one solution to support either high or low-end applications, but not both," Liu says. "B2net, as a vendor-independent storage integrator, was the only one to propose a solution to consolidate both in one solution."

"Previously, we were using traditional direct-attached storage and D2T backup, which was too slow and cumbersome for us," he continues. "We bid for multi-million pound contracts, and it is imperative that our projects run smoothly. The potential costs of even the most minimal periods of downtime are vast, and lost data must be recovered rapidly to ensure the timely execution of each phase of the architectural process."

B2net's proposal involved a mixture of network appliance kit including SnapManager for Exchange and SQL, 7TB of SATA disks and BakBone Software's NetVault Enterprise. The company noticed an improvement in speed almost immediately. "Our backup window went straight down from eight hours to nothing, and email retrieval now takes seconds instead of hours," Liu enthuses. He adds that the new set-up has improved the partnership's control over its data dramatically.

"It allows us to be proactive rather than constantly fire-fight," he says. "We are now in a position where we can anticipate increases in our storage demands and scale to fit accordingly, which addresses the firm's fluctuating storage requirements. We can provide storage on demand whenever needed, which has proved particularly beneficial for peaks in project activity."

HOW TO MAKE STORAGE MORE SECURE

- **Secure tape media content** Backup and recovery are primarily a means for data preservation, not protection against tape media access. In order to secure the tape media content, strong encryption (128 bit key length or longer) can be used. Equally important is key management, which determines how keys are created, implemented, protected, distributed, updated and terminated.
- **Logical security** (authorisation, authentication, encryption and passwords) includes securing your networks with firewalls and running anti-spyware and virus-detection software on servers and network-addressed storage systems.
- **Encryption through the backup application** Putting data encryption on the backup server adds performance overhead, impacting application response and performance.
- **Encryption within the tape library** This is not widely available yet and can increase the library cost. Key management must also be taken into account, as the tape library is generally not a secure platform and multi-vendor, remote, or third party managed library systems can become even more difficult to manage.
- **Encryption with a storage security appliance** A tape media security appliance offers centralised management, protected and managed keys, flexible deployment and integration with backup applications.
- **Physical security** (restricted access and locks on server, storage and networking cabinets) includes maintaining a low profile. It's best not to keep your server and storage setup in too obvious a location. Make life as difficult as possible for would-be data thieves.