

# Compliant Storage Strategy

With virtually every organisation experiencing a relentless growth in the volume of information that they need to store – together with an increased reliance on that information for their day-to-day business operations – traditional approaches to adding storage capacity could just be creating more problems than they solve.

Furthermore, with increasingly tough regulations, an ill-conceived storage strategy could raise serious compliance issues.

This paper evaluates options that could help you to:

- Reduce your storage costs
- Simplify systems management
- 'Virtualise' your storage estate
- Improve data security – Data Encryption & Data Destruction
- Benefit from classifying your data
- Tier your storage – to boost performance and minimise costs
- Establish tamper-proof archives

and extend the life of your existing storage systems

As the amount of data you need to store increases, more effort has to be devoted to establishing how you can ensure that the information that underpins your organisation is:

- Easily accessible – to boost efficiency
- Secure against internal and external threats

Compliance and legal considerations are also likely to dictate that some information should be archived in a 'tamper-proof' manner.

The latest storage methodologies can deliver against all of these requirements, whilst also helping to contain costs by minimising the amount of resource required to manage a complex storage environment. However, in order to help maximise the return on investment from your existing storage infrastructure, we'll consider how a typical storage environment can be adapted to meet evolving needs.

## Is your storage environment difficult and costly to manage?

For most organisations, their IT infrastructure has grown and evolved into what is now a very complex environment – as, over many years, new systems have been added in response to new requirements. Despite care being taken to ensure that new systems could be integrated into the organisation's existing infrastructure, technical considerations and pressure on resources are likely to have led to an IT environment that now includes large numbers of disparate systems, each with their own data storage.

Different systems are likely to have very different management interfaces, resulting in a storage environment that is difficult, time consuming and costly to manage and support. Yet, as the pressure to expand storage capability continues, there is a pressing need to break the link that sees increases in storage capacity dictating repeated increases in storage management resource.



## SMIS offers benefits

If you're looking to add new storage subsystems to your environment, new devices that comply with the Storage Management Initiative Specification (SMIS) could offer significant benefits. SMIS is an open standard for storage network management interfaces and has been adopted by many major storage vendors including Sun Microsystems. Currently, if your storage network includes devices from different vendors it's highly likely that you will need several suites of management applications from multiple vendors. However, with time, as you replace existing storage devices with SMIS compliant products you will be able to manage your storage estate far more efficiently.

## 'Virtualise' your current storage estate... to simplify systems management

If your storage environment is not SMIS compliant, there are still products that can help you to reduce the cost of systems management. Some of the latest storage devices, such as Sun Microsystems' StorEdge™ 6920 System, not only provide additional storage capacity but can also work within your existing network to turn an array of different storage products into a 'virtual', single, centralised storage facility. There's no need to migrate data from your existing storage devices, yet your entire storage environment can be managed as a single entity – simplifying systems management and reducing operating costs.

Furthermore, as the Sun StorEdge 6920 System is compatible with a variety of different manufacturers' storage systems – it's able to 'virtualise' your current storage systems, whilst leaving you free to add third-party storage devices to your 'virtualised' storage network in the future – so there's no 'lock-in' to a single vendor.

With a unified set of reporting mechanisms and management interfaces, SMIS could help you to manage more storage... with less resource.

# Storing data securely

The penalties for failing to stop data falling into the wrong hands can be severe. In some cases, breaches in the security of personal data can lead to prosecution, compensation payments and damaging publicity, whereas the loss of commercially sensitive data can often destroy valuable competitive advantage. Yet, though the total cost of a security breach can be extremely high, many organisations devote too little investment to tackling security risks.

Although most organisations are familiar with the use of firewalls to prevent unauthorised access to their systems, there are other equally important security provisions – such as data encryption and data destruction – that should not be overlooked.

Encryption – so that data cannot easily be read by anyone who accesses it without authorisation – is a valuable method of securing data from external and internal threats. Even if your firewall is breached, encrypted data is far less likely to be of any use to the attacker. So, data encryption helps to deal with a threat that is often underestimated – the threat from internal sources.

Small, portable storage devices such as memory sticks can make data theft much easier. However, without the necessary decryption capability, data that may be stolen by contractors or internal staff is likely to be of no use.



“Disgruntled or disloyal staff can be a major threat to data security, as they are already on your side of your firewall. In addition, loyal staff can sometimes unintentionally reduce security levels and unwittingly allow information to be accessed by unauthorised third parties.”

Stephen Macey  
Dataforensics Ltd

## Encrypt data at every stage

The latest data security solutions enable organisations to encrypt data at virtually every stage in its life – when data is generated by a software application, as data ‘rests’ in your storage infrastructure or when it is loaded onto backup tapes.

## Classify your data

The various different types of data held within your organisation will require differing levels of security and encryption. In order to determine the appropriate level of security for each piece of data, data should be classified into groups. Unfortunately, with the extremely large amounts of data held within the typical organisation, classifying data can be an onerous task. However, in most cases there really is no alternative and delaying the classification process only adds to the task in the long-term. With the almost exponential growth in the volume of data an organisation has to store, the task of classifying data will also grow exponentially if not tackled as soon as possible.

Initially, there may be a tendency to define a large number of classes of data. However, the greater the number of classes – the more effort that will be required for sifting through data and classifying it. For many organisations, between three and five classes should be sufficient to cover all types of data.

Even with a relatively small number of classes, the process can still be very time consuming. However, suppliers that offer specialist storage consultancy services can manage and implement your classification project, so that you can continue to focus on your core business activities.

Estimates suggest that 35% of all data stored by enterprises has no formal owner and is not monitored in any way

One very useful by-product of classifying data can result when duplicate data sets are uncovered. Recently, a large organisation discovered that a terabyte level database existed in nine separate locations within its IT infrastructure. Naturally, freeing up several terabytes of storage can generate massive savings in storage expenditure.

There have been well documented cases of unencrypted backup tapes going missing whilst being transported... resulting in compensation costs of several millions of pounds

# Reduce your costs by tiering your storage infrastructure

Having decided on a data classification policy which defines the level of importance of your classes of data, you should be able to establish security and encryption policies for each class. In addition, how each class of data is used within your organisation can dictate the manner in which it is to be stored and this could help you to minimise your storage costs by adopting a tiered storage strategy.

By using different storage technologies to meet specific storage performance needs, a tiered storage architecture enables you to 'right size' your storage, so that expensive, high performance devices are only used for the top tier of data.

Consider a three tier storage environment where:

**Tier one is for data that your organisation needs to have available for rapid access**

**Tier two is for data that only needs to be accessed reasonably quickly**

**Tier three is for data that is likely to be accessed relatively infrequently**

As data held in tier one must be highly available and easily retrievable, this tier will require high performance devices and a high level of fault tolerance. However, tiers two and three can be configured using lower performance, lower cost devices.

With the introduction of low-cost storage products that include higher levels of intelligence and deliver improved reliability – such as the latest RAID 6 SATA based devices – it is possible to boost performance even within the lower tiers of your storage environment. However, as SATA disk drives are generally somewhat less reliable than fibre channel drives, care must still be taken to balance cost against performance. For mission critical environments that demand the highest levels of availability, high performance solutions such as the Sun StorEdge 9990 System offer significant operational benefits.

## Long-term archiving... and compliance

With regulations specifying that data must be retained for a defined period, Write Once Read Many (WORM) drives can offer advantages. As data held on WORM devices cannot be overwritten, the data is virtually tamper-proof – making WORM devices invaluable for storage tasks where you need to prove the integrity of the data archive process.

"Bell Microsystems' approach to the whole project has been very professional and I've been impressed with their attitude and attention to detail. The quality of their service has been excellent and, by using proven project management methodologies, they've helped us to minimise risk throughout the project, reduce the complexity of the infrastructure and meet our financial targets. The Bell Microsystems team has a high level of technical knowledge relating to systems, storage and SAN solutions." **Eddy Black, Transport for London**

## Where do I start?

If all of this seems like far too big a task, you're not alone. Many organisations have delayed tackling storage issues and have responded to the need for more storage capacity, by making their storage environment more and more complex. This is an expensive approach – both in the short-term and the long-term – as complexity leads to increased systems management costs and the tasks of classifying data, improving security and tiering storage become even more difficult in the future.

The good news is that it is not necessary to do everything at once. With care, it is possible to define a storage strategy that enables you to evolve, from your current storage structure, to where your business needs it to be – with incremental changes that are easier to control and reduce operational risk.

Often, the biggest single task is classifying data and, if you're to avoid losing the resource you need to cover day-to-day operations for an extended period, it makes perfect sense to use a specialist supplier to help define your classification policy and set about categorising your data.

## Getting more from your existing storage investments

Bell Microsystems' storage team specialises in helping businesses and public sector organisations to analyse their data storage requirements, assess their existing storage environment and then adapt it to extend its working life and meet new requirements. We can check for duplication of data, 'free up' spare storage capacity and look for opportunities to simplify and reduce the cost of managing a disparate, multi-vendor storage environment.

The Bell Microsystems team can also manage and resource the data classification process, then determine how best to map your storage needs onto the latest tiered storage methodologies.

Working with several best-of-breed hardware and software vendors, we can help you to improve data security, enable regulatory compliance and reduce legal risks, whilst also boosting the return on investment from your current storage infrastructure.

Bell Microsystems also offers a full Asset Management Service, whereby redundant IT assets are subjected to a rigorous asset redeployment / disposal process. Data is irrevocably removed, to DoD 5220.22-M standards, so that discs can be redeployed within your organisation, sold to generate financial returns for your organisation or disposed of by Bell Microsystems and securely recycled in accordance with the WEEE (Waste from Electrical and Electronic Equipment) directive – leaving you safe in the knowledge that the security of your data will not be compromised.



**Web:**  
[www.bell-group.net](http://www.bell-group.net)

**Email:**  
[info@bell-group.net](mailto:info@bell-group.net)

**Head Office:**  
New Hampshire Court  
St Pauls Road  
Portsmouth  
Hants  
PO5 4AQ

Tel: +44 (0) 23 9282 5925  
Fax: +44 (0) 23 9282 5928

**London Office:**  
78 Cannon Street  
London  
EC4N 6NQ

Tel: +44 (0) 207 618 6458  
Fax: +44 (0) 207 618 8145

© 2006 Bell Microsystems Ltd.

Sun and Sun Microsystems, the Sun Logo and Sun StorEdge are trademarks or registered trademarks of Sun Microsystems, Inc in the United States and other countries.

All other company and product names listed are trademarks or registered trademarks of their respective companies.

E&OE.

