

# The other side of the data security coin

Securing your internal data network is as important as controlling threats from the Internet



The storage network is crucial to any enterprise: it holds essential data and provides the capacity for running business-critical applications and services. Unfortunately this makes the storage network a target for malicious attacks from outside the organisation and makes it vulnerable to damage from within. We invited Andrew Wilson, Sales and Marketing Director, Hitachi Data Systems in the UK, to suggest pointers to a safer data storage environment.

Storage security has never been more important than at the present time, when business and regulatory compliance demand confidential data security. Yet while 72% of EMEA companies acknowledge that regulatory issues are an important driver in their storage investment, the issues that result from security breaches, such as financial loss and brand damage, can be just as serious as receiving a fine or legal action for non-compliance.

A carefully planned and well-executed security strategy throughout the enterprise is essential, so what should companies take into consideration to reduce the risk of data corruption and loss?

## Don't assume your data is secure

It is a common belief amongst business and technical personnel alike that because the storage network exists far from the many entry points and is not on an Internet Protocol (IP) network, that it doesn't need additional security. This assumption is often what makes the storage network the weak link in the secu-

urity chain. While your average employee may have little idea of how the storage environment operates or how to access key data, a malicious attacker will often take advantage of this attitude to the storage environment. Securing, hardening and frequently monitoring the storage system is crucial to prevent unauthorised individuals obtaining and potentially misusing valuable data.

## Understand the storage network

Storage networks are often looked upon as simple systems that merely provide data storage. This can lead to misconfiguration of the system making it vulnerable to accidental security breaches.

Those in charge of the storage network need to understand how to secure all parts of the environment in order to prevent this. In a small or mid-sized business a lack of technical knowledge or training can result in perfectly adequate equipment operating without proper protection because one element has been left unsecured.

# Security policies that are enforced will encourage employees to realise that data security is their responsibility also. Only 53% of firms in the EMEA region have a policy for the security of data stored on mobile devices

In larger enterprises it is also often the case that one or two experts administer storage security but a number of other technical personnel have access to the storage environment to carry out other tasks. There are cases where otherwise well-secured storage networks have been compromised by a technical team member 'borrowing' a cable from part of the storage network, having assumed it was an insignificant test environment, taking down part of the service by accident and leaving the entire system vulnerable. Implementing a company-wide labelling system of cables and other vital equipment will enable the relevant employees to see what they are being used for and whether or not they are safe to remove.



### Secure the management network

The management network can serve as the easiest point of attack within a storage system as this is what allows control of the storage network environment. Often it is a simple box that acts as a bridge between the storage network and the company IP Local Area Network (LAN) and it is frequently improperly secured at the IP end. The management network should operate at the same security level as other entry points, as well as utilising controlled access management and authentication procedures to make unauthorised use as difficult as possible. This will prevent an opportunistic attacker exploiting this common weakness.

### Segregate security domains properly

It is now standard practice to separate and firewall the organisation's network into appropriate security domains, ensuring that data can only be seen by authorised personnel. Unfortunately in many cases the storage system is connected in an unprotected way to multiple networks throughout the enterprise. This means that a single attack on the storage system puts all networks at risk.

The solution is to install different servers and applications with different data sets and ensure that the storage volumes at the back end are protected from rogue applications and servers. If this is done incorrectly, a new box plugged into the network without the correct security installed may try to take ownership of the disks around it. This can potentially cause problems with overwriting and loss of valuable data.

### Encrypt moving data

Encryption on disk storage is often a useful tool but many organisations are wary of the prospect of losing encryption keys and rendering their data useless. In fact, 43% of companies in EMEA admit they do not have a data encryption policy at all<sup>2</sup>. Yet the risks of this are far outweighed by the benefits when data is transferred to a portable device or tape. The potential for portable data to be lost by the carrier and get into the wrong hands is not such a scary prospect if it is impossible for that data to be viewed or used. Encrypting moving data should be an essential component of any organisation's security strategy.

### An enterprise-wide security strategy

An effective security strategy will cover people and processes in addition to technology. Clear policies and procedures that are regularly enforced will encourage employees to realise that data security is their responsibility also. Only 53% of firms in EMEA report having an internal policy for the security of data stored on mobile devices<sup>3</sup>. This is a surprising statistic given recent reports of lost laptops, disks and USB keys. Companies need to apply and enforce security strategies which cover data-at-rest as well as data stored on mobile devices.

### Share skills & knowledge

Often storage administrators and the security team exist as separate divisions within an enterprise. This can mean the administrators have little knowledge of security best-practice and the security personnel do not have a sufficiently in-depth knowledge of storage to be able to see the weaknesses in the network. This can be the result of a lack of training, a territorial attitude or simply a lack of contact with one another. Cross-pollination of skills and knowledge is essential to prevent storage being the weak link in the security chain and it is important for companies to promote these practices.

Electronic and logical security can be extremely effective in preventing malicious or accidental attacks on storage networks but this

is only part of the story. Physically securing equipment is a frequently neglected part of storage security and some organisations have paid the price for this. Regularly reviewing storage security practices as part of the company's overall strategy is fundamental to preventing attacks.

For a large enterprise, include a review of how many people have keys to the data centre and how secure the room is; for a small or mid-sized enterprise, check that the keys to the storage rack haven't been left in the lock. Taking time to remind all employees that an attacker doesn't need to get through layers of electronic security to get hold of data if he or she can simply walk in and take it will pay dividends.

Following these tips will help you protect one of your most valuable assets: the data your company relies on to complete its mission-critical activities. Bear in mind that implementing a set of policies that help all employees in keeping company data secure is just as important as ensuring your technical team has taken the necessary steps to secure the data electronically.

Research from Hitachi Data Systems, EMEA Storage Index research, conducted in January 2007



## Data Storage - a necessary evil

The Storage Expo series of events in London provide businesses with their best overview of the rapidly changing storage scene

Organisations are facing unprecedented growth in data storage requirements with capacity demand projected to continue increasing at more than 50% a year for the medium term. It would follow that, within a decade, the amount of data storage required will have reached 60 times its present level.

A forthcoming event, Storage Expo 2007, is a vehicle for the data storage technology sector to present its wares and provides the pointers to trends and technologies in the sector.

### Conference supported by 100 + exhibitors

More than 100 of the leading vendors of storage solutions will be exhibiting alongside an extensive, cutting-edge free education programme. This established annual event enables organisations to compare the latest products and services, providing the ideal opportunity to assess how to incorporate the latest storage technology into IT infrastructure.

The conference provides a platform for recognised experts in the field of data storage, who look at the latest business advantages that a well considered storage strategy can deliver for an organisation.

Storage practice has been driven by the push of regulation, legislation, and business continuity rather than the pull of sound business practice. The impetus is shifting towards business practice as organisations must find more efficient ways of holding business-critical intelligence.

### Keynotes help promote demand for investment in storage

The keynotes at Storage Expo are intended to reflect the change in the data storage landscape. November 1st, for example, is the deadline for UK Financial firms to comply with Markets in Financial Instruments Directive (MiFID); one of the largest compliance issues that financial sector has had to accommodate for a decade. MiFID will govern all transactions from core investment business through retail banking to virtually any other organisation that has financial transaction elements.

This session will explore the impact on companies of the latest swathe of compliance law that is coming into force. Information to date indicates that many organisations are falling behind in their implementation: there will be potentially catastrophic consequences for their trading operations.

Compliance legislation, governance and liability are not confined to the financial sector, however and the requirements for the storage of data to take account of them are having a widespread impact across business. This session is intended to explain the significance of the latest wave of compliance regulation and legislation.

Storage Expo 2007 is taking place at London Olympia on October 17 & 18. Admission is free and details can be found at <http://www.storage-expo.com/>

