BUSINESS BRIEF

Tape Encryption – Necessity or Overhead?

October 2008

Tape encryption, as part of a data security strategy, is increasingly becoming a requirement for organisations needing to provide better levels of protection for backup and archive data.

Encryption of archived data was, until recently, the preserve of organisations with highly sensitive data and reasonably large budgets. However, the need for encryption today is driven not only by the increased value of business and personal data but by central government and financial compliance regulations. This affects a wide swathe of organisations - from very large multi-nationals to highly niche retailers – and on systems that aren't just mainframe based.

The Need

Encryption is inevitably a balance between the needs of the business, the regulatory frameworks and the available technology. Our clients are experiencing a significant demand for this technology driven by legislation and high profile leaks of sensitive, and unencrypted, data. Also, as organisations need to retain data for longer periods of time, there is a requirement to ensure that data at rest – often stored by third parties – is truly secure. There is no doubt that encryption adds a layer of management and complexity to tape backup infrastructures but most organisations are asking the important question "can we afford NOT to adopt encryption technology in this era of increasing regulatory oversight?"

Tape Encryption

The most popular methods of encrypting tape data are either 1) via the backup application 2) using an encryption appliance or 3) tape drive-based. This last method has been made possible with the recent introduction of tape drives with built-in encryption capabilities. This business brief focuses exclusively on tape drive based encryption which has become the most cost effective and high performance tape encryption solution.

A fundamental element of the encryption solution is the creation and management of encryption keys. This business brief will also highlight some of the major issues associated with this topic.

Tape Technology

Not all tape drives support encryption at the drive level - this ability has only been available in the last two years from the tape market leaders such as IBM. However the encryption algorithms adopted by individual tape drives are likely to be the same (AES-192 or AES-256) and the choice of *symmetric* or *asymmetric* encryption can significantly affect the operation and levels of encryption granularity available for the tape media. The choice is determined by how much flexibility and strength your business needs in its encryption policies.

Key Management

Key management is almost more important than the encryption process itself – without the correct key the data written to tape is completely irretrievable! Therefore the design of the key management component needs to address issues such as:

- Selecting key generation platform
- Key management & policies
- Key backup and retirement
- Key replication & retrieval
- Disaster recovery
- Key serving and sharing

Managing Tape-Based Encryption

Within a tape drive encryption solution the key management is achieved in one of three ways - application, system or library managed. At the time of writing, key management in the backup application can only be achieved using Tivoli Storage Manager but undoubtedly other vendors will catch up. For system and library implementations, keys are managed by an external software application. For an IBM tape environment this software is Encryption Key Manager (EKM).

Tape Encryption Policies

The flexibility of an encryption solution is determined by policies which can be highly flexible and granular to allow different keys and encryption methodologies within the backup infrastructure. These policies can be used to determine how encryption is performed for an individual backup or restore or even manage the effective purging of time-limited data by the destruction of relevant restore keys. For example, the policy could dictate how encryption keys are issued to maintain effective "Chinese walls" within the data contained on the tapes.

Common Problems

In our experience, the fear of losing access to encrypted data and the perceived complexity often drive IT departments to resist the adoption of a tape encryption solution. However, with careful planning we can advise and guide organisations through some of the issues shown below:

- Integrating with existing company security policies
- What to do with legacy data sets?
- Key management processes
- Fear of losing encryption keys
- Company-wide policy enforcement
- Complexity of hardware and software solutions
- Infrastructure choices

How CorpTech can help

CorpTech provides infrastructure solutions to help organisations meet their data backup, archive and storage compliance obligations. We will give you an honest overview of the current tape encryption options available and assess their suitability for your business.

Encryption Feasibility Workshop

CorpTech can facilitate a one day encryption workshop to identify business requirements, outline encryption policies, assess current infrastructure capabilities and suggest potential solutions.

Ring us on 01372 365071 for more information.

BENEFITS OF TAPE ENCRYPTION

Business:

- Delivers absolute data security for onsite and offsite media.
- Improves regulatory compliance and reduces business risk.
- Re-enforces "Chinese walls" between departments and businesses.

Operational:

- Minor impact on backup performance (<1%)
- No tape capacity impact.
- Instantly purge tape data by deleting encryption keys.