THE CLIPPER GROUP
Navigator™
Navigating Information Technology Horizons℠

Published Since 1993 Report #TCG2006080 September 10, 2006

IBM Introduces the First Encrypting Tape Drive to the Data Center

Analyst: David Reine

Management Summary

The availability of high-end home entertainment centers has spoiled us. We have become used to sitting in our favorite chair, picking up the remote, and listening to the highest quality sound systems that money can buy. Fortunately, quality systems from companies such as Bose and Denon are now available at more affordable prices for the audiophile. Unfortunately, we now insist upon installing these high-quality radios in our cars, so that we can enjoy the same sound on the highway as we travel or merely commute to work. This is unfortunate because car radios have never been the most secure accessory in the dash. They are easy targets for the professional thief who is looking to make a quick profit. We can lock the car, but that is just a band-aid. The thief can break a window. Moreover, what do you do in a convertible? How can you actually secure the sound system? One solution that has become popular is to encode the radio to the connector in the car so that it will only work in that vehicle. **These encrypted devices may cost a little more, but they protect you from theft** – the radio is worthless to anyone else.

Security issues do not end with the commute to the office. The data center faces the formidable challenge to secure the data that is the lifeblood of the enterprise. Storage area networks (SANs) have enabled us to consolidate enterprise data in a single, controlled environment, shared by any server on the network with access permission. We implement a variety of RAID architectures to protect the enterprise from the loss of data, either criminal or accidental. Further, the data center staff tries to protect the enterprise from disaster by backing up the data on a regular basis, daily and weekly. We write backups to tape so that we can send a copy off-site to comply with industry and corporate regulations. However, how can the CIO, or anyone else, secure these tapes once they have left the data center? News headlines of lost or stolen tapes have been a regular occurrence of late. Perhaps Mr. Phelps from *Mission Impossible* had the right strategy after all: tapes that self-destruct. Unfortunately, that would not prevent unauthorized personnel from being first to read them. What is best is to have a tape that *only* the data center, or an authorized partner, can read. One solution that has gained popularity is data encryption. Unfortunately, software encryption uses too much CPU time and a "black box" appliance can be expensive. IBM has come up with an alternative – a tape drive that encrypts data automatically.

In order to reduce the complexity associated with encryption and to improve the process surrounding encryption management, IBM has included encryption within its *TS1120* Tape Drive, at an affordable price. To learn how tape encryption can help your enterprise, please read on.

IN THIS ISSUE

Data Protection in the Data Center

Any publicity, good or bad, may be great for a movie star. Bad publicity, however, can be fatal to an enterprise perceived to be unreliable in the manner in which they protect customer privacy. Every week, there has been a steady parade of revelations from the private sector, as well as the public sector, identifying yet another case of a security breach. Since February 2005, personal data from 91 million citizens[1] was exposed, subjecting them to possible identity theft.

In reality, exposing, or losing, personal data has always been a problem. One example of a security breach is a misplaced data tape. For decades, data centers have used off-site depositories to protect the enterprise from site disasters – fire, flood, tornado, etc. – and hundreds, perhaps thousands of reels have been lost on their way to the vault, on the wrong loading dock, in an unmarked box, or even within the vault. Until recently, however, there was no legislation mandating notification to every individual affected whenever his/her personal information was exposed. In July 2003, California passed just such a law, mandating disclosure of all security breaches. This opened the floodgates, with more than 20 states following California's lead. With this added scrutiny, there is a need for greater data security.

What is the impact to your enterprise if customer data is exposed? You certainly can measure the immediate financial impact in the notification cost and the cost to enroll all potential victims in a credit monitoring service. We can look at two recent events from July to size the problem.

- First, FedEx lost a Cablevision Systems Corporation tape en route to the company's 401(k) plan record-keeper in Dallas, TX. No customer data was on the tape; however, it did affect 13,700 current and former employees.
- A second event caused grief to Nelnet, Inc, of Lincoln, NE. A computer tape containing personal information for 188,000 student loan customers (and parents) was lost when shipped via UPS.

What is the cost to send out 188,000 notifications, including postage? What is the cost to enroll 188,000 people in a fraud alert program with Experian or Equifax? More importantly, what is the cost of the damage to corporate image? Compare that to the cost of encrypting the data on the tape. Loss, or theft, of computer tapes is not the only cause of security breaches[2], but it is a major factor and needs corrective action. Notification is a band-aid; it does not fix the problem.

Enterprises put information on magnetic tape for many reasons, not the least of which is that it is the most cost-effective, high-capacity, portable storage available. (See Exhibit 1, below.) That will continue to be the case for the near future. Portability is mandatory for today's data center, not only for backup and archiving to a remote location, but also for sharing of information with partners. However, in a risk-averse atmosphere, the data center must improve information security. One method of securing data - to ensure that unauthorized eyes cannot view it - is *data encryption*, a technology that has been around for many years. Until recently, however, encryption has been deemed too complex, and too costly, a solution for all but the government, where security outweighs all other concerns, and they can always print more money! The incremental costs associated with encryption, from the cost of crypto processors to the degradation in performance, have been too high a price to pay for many enterprises, not to mention the impact on data recovery. In order to be widely accepted, encryption vendors must simplify their tools, seamlessly integrating them, and make them economical to the average enterprise. Expensive process changes are not acceptable; nor are implementing complex solutions that require training all of your storage administrators to become security specialists. In addition, the data center needs improved encryption management, to control the encryption keys. Some enterprises have adopted the ostrich approach by putting

Exhibit 1 – Advantages of Tape

- Low-cost – Priced as low as $.25/GB;
- Portable – May be stored off-line and off-site;
- High-capacity – Up to 500GB, native;
- Long-lasting – May be stored for decades;
- Durable – Can withstand warehouse conditions; and
- Securable – Can support encrypted, WORM data.

[1] See www.Privacyrights.org.

[2] In July, someone stole a laptop computer from the U.S. Department of Transportation containing the personal information of over 132,000 citizens.

their heads in the sand and ignoring the problem, until an ugly headline rears its head and takes a bite out of another part of the enterprise anatomy.

Fortunately, new technology offerings are now available to satisfy the most stringent privacy regulation and protect the enterprise from any security breach.

Data Encryption Methods

There are a number of ways currently in use to invoke the encryption of data to protect personal privacy. Here are some of the methods.

- *Host-based encryption* – Implemented at data creation, this strategy eliminates any chance of data interception, **or subsequent data compression**, requiring further consumption of host computing resources to do a software compression, or increasing the volume of stored data. This method also requires significant processing time or the use of encryption accelerators, adversely affecting performance and cost. The data center must retain encryption algorithms with the data in order to decrypt. This method is very secure, but expensive.
- *In-band encryption* – This appliance-based encryption method[3] protects the data during transport from point of creation to a device. It is a network-level encryption, exposing data between host and appliance. It is easy to install, with no change to the existing data infrastructure or host performance. However, the appliance typically is proprietary and adds incremental cost, usually requiring a dedicated system for a set number of storage devices, increasing the cost as the volume of encrypted data grows. It is easy to implement, but costly to acquire, scale out, and maintain.
- *Library-based appliance* – In this method, encryption is initiated by volume serial number, and the library makes the request to the encryption key manager, depending upon the policy established for cartridge location. This method requires no changes to the data center configuration.

Encrypting data before compression makes the data uncompressible. This could double or triple the number of cartridges required, causing the data center to outgrow any existing library infrastructure. Server-based encryption requires significant processing time, affecting mission-critical application performance and productivity, and affecting any other application sharing the server in a virtual environment. These methods can seriously affect IT TCO.

One new solution is now available that will avoid these pitfalls: using the tape drive, itself, to encrypt compressed data.

IBM Tape Encryption Solution

In 1952, IBM was the first company to ship digital data stored to magnetic tape. In 2006, they continue to lead the industry in tape innovation, with integrated encryption. There are two significant components in IBM's announcement of embedded encryption: availability of a revised *TS1120 Tape Drive*[4], and a new *Encryption Key Manager (EKM)*.

The TS1120 Tape Drive

The TS1120 is the first, and only, encrypting tape drive available. With a native capacity of 500GB, each cartridge can support up to 1.5TB of information, with a 3:1 compression ratio. IBM has already experienced significant success with the TS1120, with over 7,000 units installed in less than a year. With support for encryption and WORM cartridges, the TS1120 can address all of the data center's security concerns. Three key encryption benefits are offered on the TS1120.

- IBM has included encryption hardware within the drive so that the data center staff can secure *any information* (either all of it, or only subsets, as selected by the customer) going to tape at the device level no applications have to be modified to support encryption, whether backup, archive or mission-critical. This is a cross-platform solution.
- There is no complexity added to the IT infrastructure – the new *3592 E05* drive looks the same to all interfaces with minimal impact to the 100MB/s performance (<1%).
- IBM has incorporated encryption into the drive at a premium of about 10% - increasing the list price from $32K to only

[3] See **The Clipper Group Voyager** dated March 7, 2006, entitled *The Data Demands Discretion – DISUK Encrypts the Tape*, available at http://www.clipper.com/research/TCG2006014.pdf.

[4] See **The Clipper Group Navigator** dated November 29, 2005, entitled *Sun Challenges IBM for Enterprise Tape Drive Supremacy – T10000's Improvements Fall Short*, which is available at http://www.clipper.com/research/TCG2005077.pdf.

$35,500[5], significantly less than the cost of any entry-level encryption appliance.

- By doing encryption at the device level, the IT staff can compress all data prior to encryption – saving both space and money when compared to server solution – controlling data growth.

See Exhibit 2, at the right, for additional potential benefits.

Encryption Key Management

Encrypting a tape cartridge is easy. Managing the encryption keys is not. IBM's new Encryption Key Manager (EKM) is an innovative, new component of the IBM *Java Virtual Machine*, supported on a wide range of IBM operating environments, including *System z, System i, System p,* and *System x*, along with a variety of open systems platforms, running *Windows*, *Linux*, and Sun's *Solaris*. EKM is designed to be a shared resource, deployed in multiple locations within an enterprise. EKM can support several TS1120s in generating, protecting, storing, and maintaining encryption keys. EKM simplifies the key management task and allows auditability. Encrypted data can be destroyed by deleting all copies of the encryption keys used to encrypt it – either at the tape cartridge, or in the EKM.

EKM acts as a process awaiting key generation or key retrieval requests. Before the TS1120 can write encrypted data, it must request a key from the EKM. Upon receipt of the request, EKM will generate an AES[6] key and deliver it to the drive in an encrypted wrapper (the AES key is not sent in the clear). The drive then writes the encrypted key to the cartridge memory and three additional places on the cartridge for redundancy. When an encrypted cartridge is read, the wrapped AES key on the tape is sent to EKM where the AES key is unwrapped, and then rewrapped for transmission back to the drive, which can unwrap it and use it to decrypt the encrypted user data written to the cartridge. Because of the relationship between the key and the data, key management becomes the most important aspect of encryption.

Conclusion

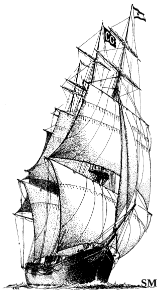
It is becoming clear that data itself cannot be controlled; however, access to the data can be managed via encryption. Whether we like it or not, in order to mitigate the risk of exposing customer or employee data to unauthorized view, the data center staff must encrypt all tapes leaving the secure environment of the data center. New privacy regulations and widespread security threats dictate it; new technology enables it. IBM enables the data center to get the maximum value from enterprise data while securing strategic information and addressing regulatory concerns.

Exhibit 2 –
TS1120 Encryption Benefits

- High-performance tape drive encryption;
- Address security concerns and regulatory requirements;
- Share data securely with partners;
- Heterogeneous server support;
- Cost effective encryption of large quantities of data
- Avoids host CPU encryption overhead;
- Minimize impact to existing processes and applications; and
- It allows z/OS customers to leverage their existing investment in zSeries proven cryptographic and security features.

IBM's new encryption capability not only allows the enterprise to protect itself from negative headlines and possible litigation, it also simplifies the sharing of data with partners who no longer need to deploy the same IT infrastructure to share data, only a common tape drive. With its Java base, the EKM is highly portable and can run on anywhere the IBM Java Virtual Machine can!

The TS1120 - with encryption - reduces, if not eliminates, risk and liability, enhancing the use of tape in backup and archiving environments. IBM is not the only company that can implement an encrypting tape drive; it is simply the only company that has! Implementation of a tape solution instead of D2D can reduce the TCO for the data center. If security and lower cost sound like a winning combination to you, IBM may have the solution for which your data center has been searching.



[5] IBM will upgrade an existing TS1120 E05 for only $5,000, with the return of the older device.

[6] Advanced Encryption Standard.

About The Clipper Group, Inc.

The Clipper Group, Inc., is an independent consulting firm specializing in acquisition decisions and strategic advice regarding complex, enterprise-class information technologies. Our team of industry professionals averages more than 25 years of real-world experience. A team of staff consultants augments our capabilities, with significant experience across a broad spectrum of applications and environments.

- ***The Clipper Group can be reached at 781-235-0085 and found on the web at www.clipper.com.***

About the Author

***David Reine* is Director, Enterprise Systems for The Clipper Group.** Mr. Reine specializes in enterprise servers, storage, and software, strategic business solutions, and trends in open systems architectures. He joined The Clipper Group after three decades in server and storage product marketing and program management for Groupe Bull, Zenith Data Systems, and Honeywell Information Systems. Mr. Reine earned a Bachelor of Arts degree from Tufts University, and an MBA from Northeastern University.

- ***Reach David Reine via e-mail at dave.reine@clipper.com or at 781-235-0085 Ext. 123. (Please dial "123" when you hear the automated attendant.)***

Regarding Trademarks and Service Marks

The Clipper Group Navigator, **The Clipper Group Explorer**, **The Clipper Group Observer**, **The Clipper Group** *Captain's Log*, **The Clipper Group Voyager**, and *"clipper.com"* are trademarks of The Clipper Group, Inc., and the clipper ship drawings, *"Navigating Information Technology Horizons"*, and *"teraproductivity"* are service marks of The Clipper Group, Inc. The Clipper Group, Inc., reserves all rights regarding its trademarks and service marks. All other trademarks, etc., belong to their respective owners.

Disclosure

Officers and/or employees of The Clipper Group may own as individuals, directly or indirectly, shares in one or more companies discussed in this bulletin. Company policy prohibits any officer or employee from holding more than one percent of the outstanding shares of any company covered by The Clipper Group. The Clipper Group, Inc., has no such equity holdings.

Regarding the Information in this Issue

The Clipper Group believes the information included in this report to be accurate. Data has been received from a variety of sources, which we believe to be reliable, including manufacturers, distributors, or users of the products discussed herein. The Clipper Group, Inc., cannot be held responsible for any consequential damages resulting from the application of information or opinions contained in this report.