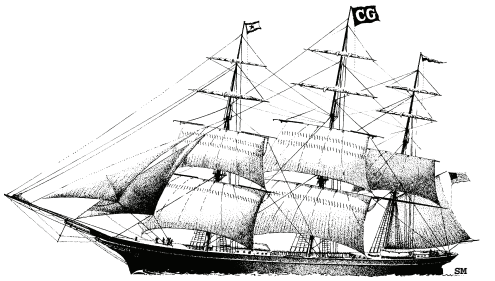
THE CLIPPER GROUP
Navigator™



Navigating Information Technology Horizons℠

Published Since 1993 Report #TCG2007036 March 5, 2007

Security for Small Data Centers — Right-Sizing Tape Encryption

Analyst: David Reine

Management Summary

The birth of a child creates many changes in the lifestyle of the typical, previously carefree, couple. Gone are the days of quiet nights alone with each other; gone are the days of spontaneous travel to exotic locations. Gone, too, is that cute, little, two-seat sports car with a 0-to-60 time of five seconds! The new parents must replace it with a more practical mode of transportation, a reliable vehicle with sufficient storage capacity to carry all of the baby supplies that you need, a baby carriage, or, perhaps, even a portable crib, and hopefully, *the same pickup* to merge into the high-speed traffic lanes on the cities highways. We are not talking a truck or a large van, more like a minivan or your father's station wagon, something with *enough capacity*, yet still stylish. Even more important, however, are the safety features to protect the valuable contents of your automobile. We are talking about more than just an antilock braking system or front and side airbags. This vehicle needs to have a 5-star rating from the National Transportation Safety Board. Nothing less will do for this cargo!

A similar story is occurring in smaller data centers of enterprises around the world, as CIOs look for a backup/recovery or archiving solution sized to meet the needs of their particular environment. The tape system must have the capacity to handle the daily and weekly demands of the smaller data center, sufficient speed to complete its task within the allotted window, and it must be reliable to ensure that yesterday's transactions were backed-up without requiring human intervention. Unfortunately, a new trait is now mandatory for any tape system – it must be capable of creating encrypted media to protect the enterprise, and its executives, in case of loss or theft of valuable employee or customer personal information. This has not been a problem for the largest data centers. They have always had the resources to accomplish this task, if not the resolve. The same cannot be said for department or branch managers within that organizational structure, or, more importantly, the IT managers in the thousands, no, tens of thousands, of small and mid-sized enterprises (SME) around the world. They do not have the same budget or staff to implement the complex backup system necessary to secure SME data. Now they do.

IBM has recently announced the availability of a low-cost tape library ($30K, without drives) that can secure up to 37.8TB of data at 4Gbps over a high-speed Fibre Channel link. Moreover, this library is capable of automatically encrypting the data written to high-capacity media without any operator intervention. If your department or SME needs to protect its data, and executives, then please read on.

IN THIS ISSUE

SME Data Protection Requirements

The loss of data by any enterprise data center, large or small, can have a debilitating effect on the growth of that enterprise. The impact on smaller businesses can be even more damaging, affecting their very existence. The costs associated with protecting your customers, and employees, after a data loss could break a smaller business, probably putting it into the red, damaging its reputation, and causing customers to look to competitors for goods and services. Governments around the world have now stepped in, passing legislation to ensure the privacy rights of their citizens. Each enterprise must do everything in its power to protect its data or risk the wrath of the government, as well as criminal charges. **The risk of loss is greatest during the transport of tape media, either from or to your data center.**

However, the enterprise simply cannot stop sharing data. The data center shares information, as a matter of business necessity, with remote offices and with partners. They send it to secondary data centers for backup and recovery purposes. They send it to vaults for disaster recovery and business continuation. **The data on that media does not have to be at risk, however.** Encryption of any data that is leaving the security of the data center, in transit, has always been an option, unfortunately, a very expensive option. The data center can encrypt with software, but these applications are costly and can have a dramatic effect on the performance of mission-critical servers, using valuable CPU cycles to encrypt data, slowing response to any query made during the encryption process. The data center can also encrypt using an in-band encryption appliance, hardware, and software integrated together. This is even more expensive. Unfortunately, both of these solutions can also have a negative effect on the quantity of media created in the backup or archive process. **Furthermore, the data center cannot compress encrypted data**. Therefore, a typical industry-standard tape drive with an LTO or SDLT format will not achieve the 2:1 compression ratio that manufacturers promote nor will it achieve the 3:1 ratio available on enterprise-class drives.

In a distributed server environment, the enterprise can generate sharable data on a mainframe and on open systems, deployed throughout the network in remote offices. The data center needs to be able to encrypt tape media from both locations in a controlled manner in order to protect it and simplify the management process. In the larger enterprise, this means that the encryption algorithm must be available on both the mainframe and open systems platforms, while the SME requires a solution that will work with Windows and Linux on a variety of platforms. In addition, the SME or remote installation requires a much smaller tape library platform, as the SME may measure the backup/archive requirement in terabytes, versus petabytes in the data center.

Encrypting a tape cartridge is easy; managing the keys to ensure that the data center can decrypt the data is not. Encryption key management is critical to the ability to access the data, especially the ability to re-key the media if evildoers compromise the keys, without having to rewrite the entire cartridge. The enterprise can implement key management with any of several techniques, managing at the system level, by the application, or at the library. The important factor to remember is that the management technique used should be platform independent. All enterprise environments must use the same encryption process and management interface.

In order to protect the data, and make maximum use of tape capacity, you need to encrypt after the compression process. With automatic compression available at the tape drive, the most efficient place for encryption needs to be at the drive, also. The IT staff will soon learn that, for better or worse, each vendor has their own unique spin for tape encryption deployment. Let us look now at IBM's solution for the mainframe data center with the need to exchange tapes with another enterprise with a mainframe or with a smaller open systems installation.

The IBM Data Encryption Solution

Tape encryption is like an insurance policy. You must pay up front to protect yourself from a disaster destroying your life's work. How much you pay depends upon the value you assess to recover from that disaster. In recent months, we have seen repeated examples of enterprises losing tape media either through an accident or through criminal acts. In many cases, the cost to protect customers from identity theft after such an incident runs into the millions of dollars, between notification to the affected customers and enrolling them in a credit-reporting bureau[1]. What is the value then of protecting the enterprise or SME from potentially embarrassing data theft and the ensuing legal action? What would be the impact on the executive staff of not following the best practices for the protection of your customer's personal data? **What is the value then of a tape drive that automatically encrypts the data on each tape cartridge, eliminating the need for an in-line appliance or server application?** On the other hand, how can the SME, or remote office, afford to deploy on their open system server the same sophisticated encryption library as the data center deploys on their mainframe?

IBM has taken an open systems' approach to tape encryption for the SME and branch office environment, providing a common solution – cross platform –

[1] See **The Clipper Group Navigator** dated September 10, 2006, entitled *IBM Introduces the First Encrypting Tape Drive to the Data Center*, available at http://www.clipper.com/research/TCG2006080.pdf.

to ensure that the enterprise can share data between heterogeneous systems. IBM has implemented a Java-based encryption key management system, with a scalable platform format based upon the recently-announced *System Storage TS1120*, a high-*performance*, high-capacity encrypting tape drive[2].

IBM's *Encryption Key Manager* (*EKM*) supports 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*. IBM also supports Sun's STK silos, as well as their own tape libraries. EKM is a shared resource, deployed in multiple locations within an enterprise. It can support TS1120s in generating, protecting, storing, and maintaining encryption keys. EKM simplifies the key management task and allows auditability. EKM enables the sharing of encrypted data and its destruction, by deleting all copies of the encryption keys at the tape cartridge or in the EKM. The drives do not store the encryption key data.

IBM can encrypt up to 700 GB of uncompressed data onto a single cartridge[3], using the TS1120 at native speeds of up to 104 MB/second. The TS1120 is the first tape device to feature 700 GB physical capacity, by far the largest enterprise linear physical capacity available in the market, and a 40% increase over the previously announced 500GB cartridge. Designed for use in applications such as backup and restore, archiving, and those requiring security or an audit trail, the IBM *3599 Tape Media* cartridges include a WORM format to prevent tampering with regulated data. The 3599 cartridge may be integrated into the *TS3500 Tape Library*, the *3494 Tape Library*, the Silo Compatible *Tape Drive Frame 3592 Model C20*, as well as into standalone environments. The 700 GB media was released in January 2007 with a starting price of $5,400 for a 20-cartridge pack ($270.00 per cartridge).

At a cost of $35.5K, IBM has priced the TS1120 very competitively versus other enterprise drives priced at over $40K for Fibre-Channel attachment. A purely open systems data center may find this price too high and defer the encryption decision until later in 2007 when LTO-4 becomes available at around $10K for a drive capable of writing an 800GB cartridge[4]. An enterprise CIO may have trouble justifying a TS3500 Tape Library with TS1120 tape drives for a branch or remote office with smaller data needs. Therefore, IBM has now announced the *TS3400* for the small data center that has significant security requirements.

The IBM System Storage TS3400

The IBM *TS3400 Tape Library* is a compact storage solution that is rack-mountable in a 5U space or can sit on a desktop in an SME environment. **It brings enterprise tape performance to the SME and branch office environment**. Capable of supporting one or two TS1120 tape drives with 4Gbps Fibre Channel attachment, the TS3400 has a potential throughput of over 600MBps when the data is fully compressed. With a raw capacity of 700GB on a tape, each removable magazine can support up to 6.3TB of native data on nine cartridges, 18.9TB compressed. In addition to the standard 700GB cartridge, the TS3400 also supports 700GB WORM media as well as the previous generation of 500GB cartridges, standard and WORM. Moreover, the TS3400 supports 100GB cartridges, both standard and WORM, for high-speed data access.

Configured with two magazines, the TS3400 can hold up to 37.8TB of data and supports up to three I/O slots for the easy insertion or removal of tape media. It is easy to deploy and easy to manage with a built-in bar code reader and remote management capability.

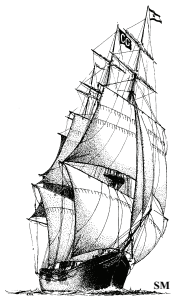
The TS3400 is highly reliable, scaling encryption down to the smaller data center, with the same features as the larger IBM tape libraries:

- Hot-swappable tape drives;
- Hot-swappable and redundant power;
- IBM's *Multi-Path Architecture* to access two logical libraries;
- IBM's control path and data path failover;
- Built-in encryption capabilities and encryption key management via application, system, or library.

Conclusion

IBM has designed the System Storage TS3400 to have high capacity and high performance in a mid-sized data center with a concern for security and reliability. With scalability to almost 40TBs of compressed data, the TS3400 enables the enterprise data center to share confidential information with partners and to transmit data outside of the security of the "glasshouse" without concern for data loss or theft.

If your enterprise is already using TS1120 tape drives and you want to replicate the data center environment in remote locations, or if your data center is strapped for space and you need to deploy an additional encryption capability, the TS3400 is the ideal solution. It can protect the investment that your IT staff has already made in tape assets with a modest additional cost. Encryption can protect your enterprise from data theft while, at the same time, the TS3400 eliminates the need to over-provision remote locations. The TS3400 just might be your enterprise's best *insurance* purchase in 2007!



[2] Ibid.
[3] 2.1TB of compressed data with a 3:1 compression ratio.
[4] 1.6TB of compressed data with a 2:1 compression ratio.

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**, **Clipper Notes**, 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.