Protect Your Enterprise – Remotely Track Your Tapes

Analyst: David Reine

Management Summary

Whenever you make a major investment, you want to protect it. If you purchase a house for several hundred thousand dollars, you make sure that it is insured against loss from fire or flood. You may not be able to prevent someone from breaking in, but you can insure the contents against theft. You are not worried that someone will steal your house. It is not portable. It is secured to a foundation and under your control. Your automobile is another story. That is mobile. Even if you lock it, you cannot guarantee that a professional thief, or a teenager looking for a joyride, won't break in, jump start it, and drive it away. **You cannot prevent someone from stealing your car**. Alarms and other deterrents are not enough. That is exactly why you want to protect your expensive automobile by investing in a retrieval device such as *LoJack,* costing less than a thousand dollars. The *LoJack Stolen Vehicle Recovery System* consists of a small radio frequency transceiver hidden in your vehicle. Each LoJack has a unique code that is tied to the Vehicle Identification Number (VIN). When you report a theft to the police, a routine entry into the police crime computer matches the LoJack System's unique code against the state VIN database. This automatically activates the LoJack Unit in your vehicle, which emits an inaudible signal. Law enforcement authorities who are equipped with LoJack Police Tracking Computers are always listening for a LoJack signal. Police use the LoJack Police Tracking Computers to track and recover your stolen LoJack-equipped vehicle. **With LoJack, you can take control and ensure that if someone steals your car, it will be found**. This is precisely why new car dealers offer LoJack to you as an option. If you value your car, it is an option that you will consider.

A similar scenario exists in every enterprise data center. Every data center has at least one server. It could be a mainframe worth millions of dollars or a network of open systems server costing tens or hundreds of thousands of dollars. The enterprise installs these servers in secure, protected environments. A hacker may penetrate your firewall and access your data banks, but you are not worried that someone will physically steal your processing system. You have terabytes, or even petabytes, of information in the enterprise data center. You install a variety of security features to insure that you can protect the information in your storage devices, but you are not concerned that someone will actually steal a disk array that costs tens of thousands of dollars, or more. You even protect that data from a disk crash or natural disaster by backing it up to another disk for immediate recovery or to a tape for off-site storage. Aha, the tape! A data center can store over a terabyte of information on a single tape cartridge that costs only $100 and is shipped by truck to a partner for input into their process or to an off-site vault for later retrieval. *How do you protect that cartridge from accidental loss or theft? How much do you invest in protecting a piece of media that costs $100?* The answer is easy: you don't! However, what is the value of the data on that tape? What will it cost you if the tape is lost or stolen? How much will it cost to notify each customer and employee whose name and Social Security Number were on that cartridge that their personal information might have been exposed? **That answer appears all too frequently in the headlines of every newspaper: millions of dollars**! Now, that is significant and must be addressed.

Data Center Requirements

First, it is understood that tape has the ability to store large quantities of data in a cost effective and energy efficient manner and it is removable, making it a preferred medium to backup and archive mission- and business-critical data. In fact, disk can be 23 times more expensive then tape in overall TCO and 290 times more expensive in terms of energy consumption.[1] **Unfortunately, the fact that it is removable exposes tape, and the data on that tape, to the risk of loss or theft whenever it leaves the control of the data center.** There is a need for the CIO or CSO[2] to be able to maintain visibility and control over all removable media as it travels from one location to another. The CIO and the CSO have a vested interest in the ability to maintain a chain of custody for the data under their responsibility as it moves between the data center and partner, vault, or disaster recovery sites.

Fujifilm has recognized this need and collaborated with SC-Integrity (SCI), a leading covert cargo theft-detection company that entered into an agreement with LoJack Corporation in 2006 to bring the well-known auto-theft brand together with the SCI in-transit cargo service. This service, now called *LoJack InTransit* is the underlying technology that enables you to track, in real-time, the location and status of critical enterprise tape cartridges, and recover any missing media shipped with a *Fujifilm Tape Tracker*, a wireless tape tracking unit and *Fujifind*, the interactive web-based application used to pinpoint Tape Trackers.

Fujifilm Tape Tracker

Designed to fit within a half-inch tape cartridge format, the Fujifilm Tape Tracker is a GPS receiver and cellular transmitter that fits inside almost any tape media case and can be included in any or all tape shipments leaving from the data center in order to monitor tapes in transit. Combined with the Fujifind Interactive web application, based upon the *LoJack Intransit* software platform, Tape Tracker can track and monitor all tape cartridge movement, enabling the data center to maintain a viable chain of custody with a history report, even after the media has left the physical control of the

data center staff. An IT manager can log onto the Fujifind website using a secure ID/password and compile GPS data from the Tape Tracker to create a real-time map of tape movement. Tape Tracker can continue to report location status for up to 30 days on a single charge.

The Fujifind application provides the enterprise with the capability for geo-mapping location with satellite imagery and online mapping. It also provides a geo-fencing capability for perimeter entry/exit notifications for pre-defined locations, along with in transit route discrepancy alerts. The cost of a single Tape Tracker unit and 24 hour/7 days support and service is estimated to be about $150/month.

The LoJack InTransit software uses the largest law enforcement protocol and dispatch network in the cargo security industry and SCI's Communication Command Center to dispatch the appropriate authorities to recover any stolen property. Tape Tracker has 24x7x365 customer service with technical support.

Conclusion

Because of the rapid and continuing growth of mission-critical enterprise data and the excessive costs associated with its long-term storage on disk, tape is experiencing a renewed interest within the data center. If you want peace of mind whenever those tapes leave the data center, then Fujifilm's Tape Tracker solution may be the answer. If you want to protect your enterprise from the embarrassment of front page headlines and possible litigation leading to millions of dollars in settlements, than Tape Tracker may provide the additional security that you require. If you weigh the cost of Tape Tracker against the potential risk of making your next tape shipment without it, you will be calling your Fujifilm sales rep before the day is done.

---

[1] See the issue of Clipper Notes dated February 13, 2008, entitled *Disk and Tape Square Off Again - Tape Remains King of the Hill with LTO-4,* and available at http://www.clipper.com/research/TCG2008009.pdf
[2] Chief Information Officer and Chief Security Officer.

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.