

BACKUP ■ ARCHIVAL ■ RETRIEVAL ■ STORAGE ■ DATA PROTECTION

# Are You Prepared for Data Terrorism?



**QUALSTAR®**  
The Tape Library Experts..

Qualstar 800-468-0680 / 805-583-7744 [www.qualstar.com](http://www.qualstar.com)

**SIMPLY RELIABLE DATA STORAGE SOLUTIONS**

## Are You Prepared for Data Terrorism?

In January 2003 the Slammer worm infected more than 160,000 computer systems worldwide, disrupting airline traffic, interfering with an election and preventing 13,000 Bank of America ATMs from processing customer transactions for a full day. The original Code Red virus in 2001 infected more than 250,000 systems in just the first nine hours and at the time was deemed the most expensive Internet attack in history. Business losses in the United States alone were estimated at more than \$2 billion in down time and transaction losses.

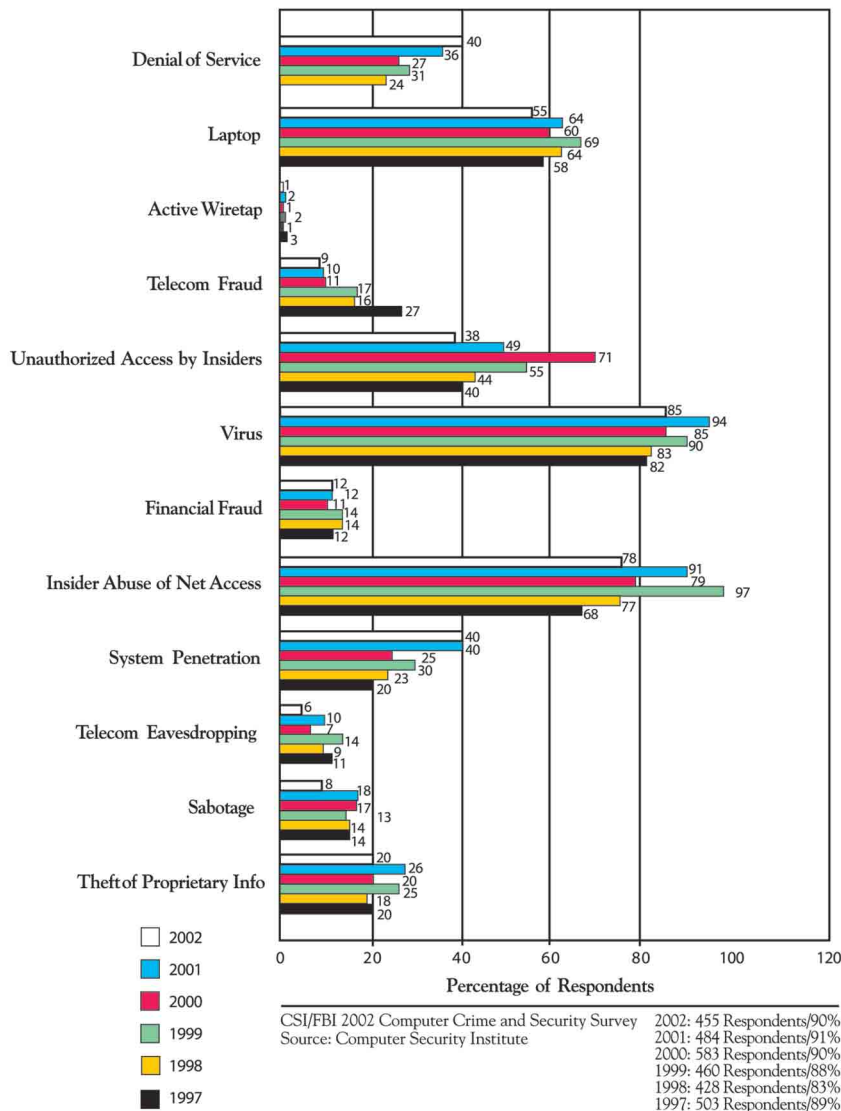
These are just two examples of the growing threat of data terrorism. This new security hazard is a much more common and more dangerous threat to a business's health and survival than the potential damage to IT infrastructure from the physical acts of terrorism that have received much more public attention, post 9/11.

According to the Computer Security Institute/FBI 2002 Computer Crime and Security Survey, 90 percent of the businesses and government agencies that responded had detected security breaches, and 80 percent acknowledged some financial loss. The CSI/FBI findings note that the perceived value of information that is vulnerable to attack by data terrorists is increasing, as is the frequency of attacks. In just the first five months of 2003, more data terrorism attacks were recorded than in all of 2002. Not all of those attacks were successful, but it illustrates the growing threat to the vast amounts of invaluable data that reside on networks.

Data terrorism takes many forms, all involving the disruption or disabling of a company's IT functionality, causing loss of productivity and disrupting access to the data necessary to conduct normal business. Data terrorism can strike at an IT infrastructure from many angles including disabling access (denial of service), corrupting data, stealing data, or even permanently erasing data. This threat is even greater to companies that are increasingly dependent on electronic transactions to perform even the simplest business operations. If access to their online systems is interrupted they are effectively shut down; they no longer have "paper-based" processes in place to support ongoing business operations in the case of an electronic attack.

Modern data protection and disaster recovery plans have increasingly focused on business continuity, ensuring that copies of critical data are readily available in the event of the failure of a primary storage device or site. Local data mirroring and remote data replication are the key components of this strategy. However, while these schemes to create multiple copies of data address some vulnerabilities, they ignore the fundamental flaw that data terrorists rely on: as long as data is online, it is vulnerable to attack. The only sure way to protect against data terrorism is to create a tape-based copy of the data and to secure that copy off-line, but in a still readily accessible manner.

**Types of Attack or Misuse Detected in the Last 12 Months (by percent)**



©2002 by Computer Security Institute. All rights reserved.

## **Analyzing the Risk: Data Terrorism Defined**

Data terrorism can take numerous forms. In the broad sense, any action that steals, alters, destroys or interrupts access to critical data – whether to satisfy the ego of a hacker or for financial or political reasons – can be deemed to be an act of data terrorism. Recent trends in data terrorism have centered around three types of attacks: worms and viruses, distributed denial of service, and unauthorized intrusions.

Attacks from worms such as the Code Red and Blaster strains, which infect computer systems and then rapidly replicate around the world via email, are becoming increasingly common and costly problems. Damage caused by the viruses left behind by these worms can range from destruction of data to opening back door access routes that allow data terrorists to later exploit that access to destroy or modify corporate data.

These types of attacks are not about to abate any time soon. According to the National Computer Security Association, electronic attacks are now the preferred method by criminals looking to harm businesses. These attacks are not just the province of lone hackers any longer; law enforcement officials point to the growing use of increasingly sophisticated electronic attacks by organized crime groups on a global basis and the damage can be devastating. To put the cost of these attacks in perspective, hurricane Andrew, the most expensive natural disaster in U.S. history, caused \$25 billion dollars in damage and the average annual cost from tornadoes, hurricanes, and flood damage in the U.S. is estimated to be \$11 billion. In contrast, the Love Bug virus alone is estimated to have cost computer users around the world between \$3 billion and \$15 billion.

## **Conventional Data Protection Plans & Their Limits**

To minimize the damage of data terrorists and provide a high level of continuous data access, many businesses are focusing less on traditional tape-based backup and utilizing a series of applications that center around creating multiple disk-based copies of primary data. Disk mirroring writes two simultaneous copies of all data, protecting against a hardware failure, but offering no protection against data terrorism. Data replication creates a copy of the primary disk storage onto secondary disks – either

locally or to a remote disaster recovery site – and then periodically updates the replica copy based on incremental changes to the primary data set. This can be a valuable option in the case of a catastrophic loss of a primary site, but as the data are still available online, it again offers no protection against a data terrorist.

Disk-to-disk backup – also referred to as “enhanced” backup and D2D – is being touted as a replacement for traditional tape backup solutions. In this application, primary data is backed up to a lower-performance disk array. In many cases the D2D array provides tape emulation functionality so it appears to existing tape backup software as an actual tape loader or library. Again, since the data is still available online D2D offers no protection against the data terrorists.

While each of these options has a niche in an overall data protection hierarchy, none addresses the fundamental vulnerability: that all of the critical data are still available online and subject to an attack by data terrorists. Additionally, data mirroring, local replication and D2D backup offer no protection against data loss in the case of natural or man-made disasters, ranging from the East Coast blackout to the devastating fires and earthquakes that plague California. The effects of deploying these techniques without adding tape-based backup to the data protection hierarchy can be devastating to a business. Consider these statistics:

- 60% of businesses affected in the 1993 World Trade Center terrorist bombing were out of business within two years. *(Canadian Insurance Company)*
- 43 percent of US companies never reopen after a disaster, and 29% more close within 3 years. *(U.S. National Fire Protection Agency)*
- 20 percent of small to medium sized businesses suffer a major disaster resulting in the loss of business-critical data every five years. *(Richmond House Group, a UK-based insurance provider for medium to large businesses)*
- The 1992 flood in downtown Chicago left 230 buildings without power for more than a week, affecting 8,000 to 10,000 businesses with estimated losses in excess of \$1.5 billion. *(Disaster Recovery Journal, Spring 1998)*

## Computer Virus Talley

### Viruses that Target Files on Primary Storage

TYPE OF INFECTION	DEFINITION	NUMBER OF IDENTIFIED VIRUS SIGNATURES
<b>Boot Sector Infector</b>	A virus which affects the original boot sector on a floppy diskette. These viruses are particularly serious because information in the boot sector is loaded in memory first before virus protection code can be executed.	106
<b>Denial of Service</b>	A means of attack against a computer, server, or network; the attack is either intentional or an accidental by-product of instruction code, which is either launched from a separate network or Internet connected system directly at the host. The attack is designed to disable or shutdown the target of the attack.	116
<b>File Infector</b>	A virus that attaches itself to, or associates itself with, a file. File infectors usually append or prepend themselves to regular program files or overwrite program code. The file-infector class is also used to refer to programs that do not physically attach to files but associate themselves with program filenames.	240
<b>Master Boot Record(MBR)/ Boot Sector Infector</b>	A virus that infects the systems Master Boot Record on hard drives and the boot sector on floppy diskettes. This type of virus takes control of the system at a low level by activating between the system hardware and the operating system. An MBR virus loads into memory before virus detection code can be executed.	1
<b>Macro Virus</b>	A saved set of instructions that users may create or edit to automate tasks with certain applications and systems. A Macro Virus is a malicious macro that a user may execute inadvertently and that may cause damage or replicate itself.	3000+
<b>Multi-partite Virus</b>	A virus that infects Master Boot Records, Boot Sectors, and Files	58
<b>Overwriting Virus</b>	A virus that overwrites files with its own viral code	84
<b>Trojan Horse</b>	A program that either pretends to have or is described as having a set of useful or desirable features but actually contains a damaging payload.	18
<b>Tunneling</b>	A virus that avoids standard interfaces to infect files. This allows the virus to infect files without being noticed by a behavior blocker	6
<b>Worm</b>	A virus that spreads by creating duplicates of itself on other drives, systems, or networks	3000+
	<b>Total</b>	<b>6,629+</b>

Source: Networkassociates.com McAfee virus database search and glossary

## De-coupling the Data from the Terrorist: The Role for Tape

In spite of the growing use of disk-based products in data protection and business continuity applications, there is still only one sure way to isolate and protect critical enterprise data from attack by data terrorists: backup the information to magnetic tape and secure the data offline.

The ability to remove the media to secure the data from online attacks is the fundamental advantage offered by tape-based backup that is lacking with any disk-based data protection methodology. Additionally, disk-only products offer no simple method to transport data to a secure offsite location to ensure against a catastrophic data loss incident. While remote data replication provides a measure of protection against a localized disaster, this model still leaves data online and vulnerable against hackers and other data terrorists. D2D “backup” solutions are hampered by the fixed capacity, requiring that at some point, the data must be deleted or archived to support new backup sessions. These limitations will come into play with new government regulations for financial records that mandate redundant copies of specified data must be stored at least 300 miles from primary storage, or the new Health Insurance Portability and Accountability Act that demands specific medical records and documentation be retained for at least six years.

D2D backup has become one of the hot button issues regarding data protection and business continuity. Much of the debate has been framed as an “either/or” issue. But in an overall data protection strategy D2D can play an important role, but only if it is combined with tape-based backup in a D2D2T architecture.

In today’s 24/7/365 business environments, a D2D2T backup architecture provides the solution to virtually every common data backup and restoration problem. An increasingly popular form of D2D2T backup is tape virtualization, combining the performance benefits of D2D with the cost, reliability, scalability and archiving advantages of tape libraries based on super high capacity, cost-effective tape technology. A virtual tape solution is composed of a D2D array essentially operating as a front-end cache for the tape library. The D2D array emulates the tape library and allows existing backup software to write data to virtual tapes on the disk array, just as it would to

physical tapes located in the tape library. The data is then sent to the tape library in an off-line, high speed transfer that is transparent to other operations. A key advantage of this approach is that it allows enterprises to deploy accelerated D2D backups without changing their current backup infrastructure, policies and procedures.

The D2D2T backup model offers several advantages for storage administrators. First, it eliminates the issue of the backup window for the tape library as the backup to tape is not being performed on active data and does not impact application servers. Second, it provides an opportunity for the data stored on the D2D array to be scanned for viruses prior to being sent to the tape library, ensuring that the tape backups will not be corrupted. D2D data can also be “groomed”, with duplicate files eliminated and data organized more efficiently to support faster restoration if needed. Finally, it enables storage administrators to achieve better utilization of tape media. Current backup practices typically put one backup session per tape cartridge, leaving large amounts of unused capacity on individual tapes. Low utilization is sometimes deliberate – driven by legal requirements – but it can severely impact the capacity potential of a tape library. D2D2T offers a better backup solution.

### **Choosing the Right Tape: the SuperAIT Advantage**

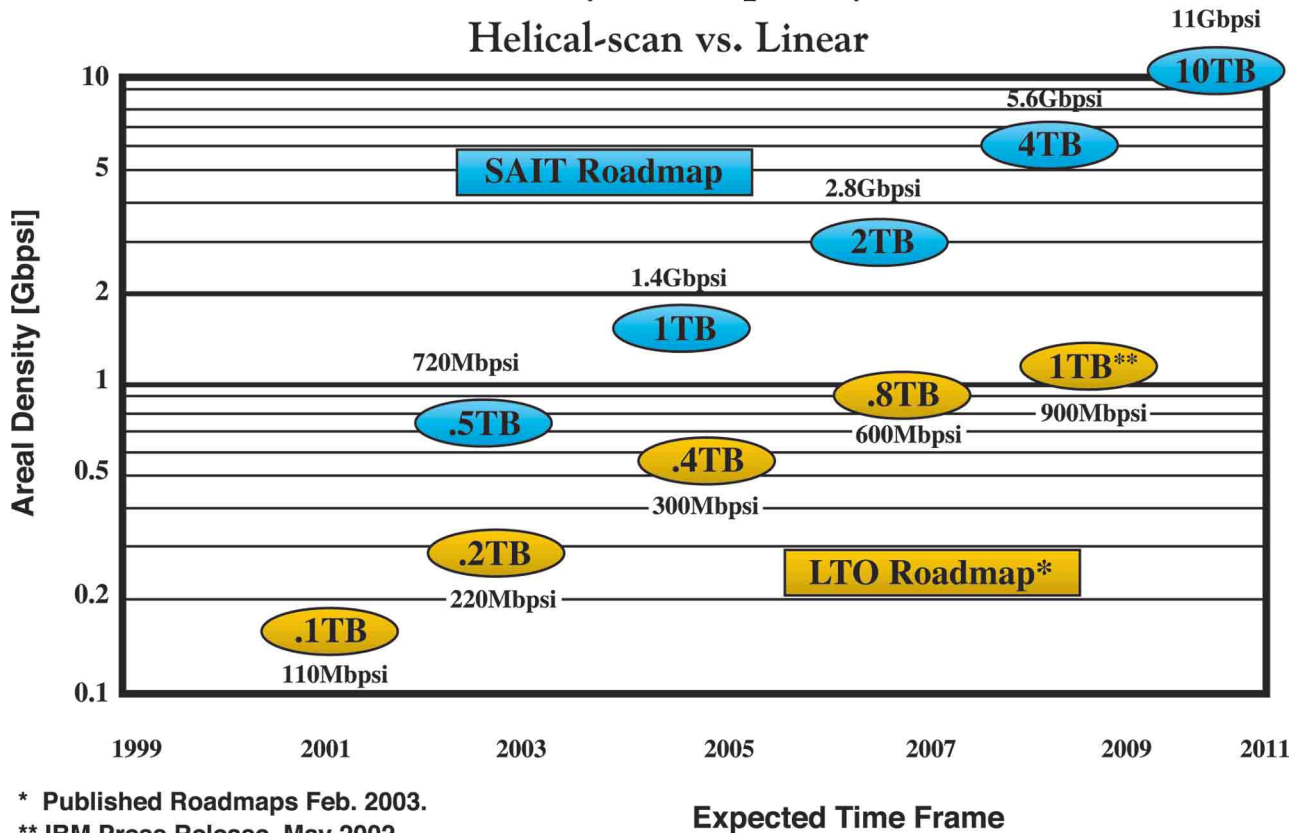
It is impossible to provide complete protection against data terrorism attacks without a tape-based backup component in an enterprise data protection plan. The challenge for endusers is selecting the best tape technology platform for the job. In the open systems high-capacity market, this choice really comes down to three options: LTO, Super DLT (SDLT) or Sony’s SuperAIT (SAIT). The key criteria for evaluating tape are capacity, performance, automation support and a compatible growth path with a future roadmap. When analyzing LTO, SDLT and SAIT on these core criteria, SAIT emerges as a clear winner.

Two years ago a group of tape drive manufacturers, tape media suppliers and researchers from the leading universities collaborated as part of the Information Storage Industry Consortium (INSIC), to analyze enterprise tape market requirements. This elite group concluded that in order to keep pace with the growth in disk drive capacities, the tape industry needs to follow a roadmap to achieve a single cartridge

capacity of 10 terabytes(TB) uncompressed by 2011, with an interim target of 1 terabyte uncompressed per cartridge by 2006. Given the current technology trends, linear tape formats – LTO and SDLT – based on metal particle media will barely exceed the 1 TB level until the end of this decade.

Conversely, the first generation of SAIT technology, based on high-output Advanced Metal Evaporative media formulation, is already at 500 gigabytes (GB) native (uncompressed), with a multi-generational roadmap in place to take it to the 10 TB target.

## Areal Density & Capacity Trends Helical-scan vs. Linear



The SAIT platform leverages the proven AIT helical scan tape technology, while adding a new single-reel cartridge design housing half-inch wide tape. A key feature of AIT technology is its more than four-fold areal density advantage over linear tape formats. The longer and wider tape used in the new SAIT cartridge leverages this advantage, giving SAIT five times the capacity for any given areal density design point, and a decided capacity boost over the linear tape formats which are currently in the 200-300 GB (native) per-cartridge range.

This new tape technology delivers high capacity and high performance using a half-inch, single-reel tape, dramatically improving the value proposition between conventional tape roadmaps and future hard disk drive capacity trends. As a new class of tape solution, SAIT technology leapfrogs conventional linear solutions, offering significant advantages in capacity, reliability and scalability.

SAIT's native data transfer rate starts at 30 megabytes per second for the first generation and is expected to double with each subsequent generation. SAIT also optimizes application performance over a wide range of host data rates by intelligent buffering to compensate for speed mismatches between the SAIT drive and the host system. This high data transfer speed, together with fast media load and fast search capability provide a total performance solution for today's enterprise applications.

The incorporation of a Memory-in-Cassette (MIC) flash memory chip embedded in all SAIT media allows the local storage of key media information and statistics. These include such parameters as media type and serial number, media usage and error recovery information together with a search-map to provide high-speed access to any file on tape.

### **Automating the Data Protection Solution: the Case for Qualstar**

The 500 GB per cartridge capacity of first-generation SAIT technology is a substantial improvement over competitive linear recording formats, but it is still only a piece of the overall data protection solution. For even modest-sized enterprises today, automated tape libraries are a requirement to handle the massive data loads. SAIT drives and media were designed with automated library applications in mind,

with the inherent capacity advantage translating into Total Cost of Ownership (TCO) savings by enabling companies to store substantially more information in a significantly smaller footprint.

Once again, customers are faced with making the right choice among multiple tape library vendors. However, an intelligent place to start would be with the company that has consistently been the market leader in AIT-based libraries: Qualstar. Not only is Qualstar the world's leading supplier of AIT libraries, the company was also the first to introduce a tape library based on the new SAIT technology. Qualstar's TLS-5000 Series offers configurations with up to eight SAIT drives and 132 TBs of native storage capacity in less than eight square feet of IT floor space.

The TLS-5000 Series – and all Qualstar *Simply Reliable* tape libraries – incorporate a number of innovations that improve reliability and performance, including Q-Link, the web browser-based remote library manager that enables administrators to configure, upgrade, and monitor any library via a company intranet or over the Internet from anywhere in the world. Q-Link extends the library's comprehensive front panel menu system and adds additional functionality such as automatic e-mail notification based on rules set by the administrator, and firmware updates can be implemented remotely. Qualstar also offers Fibre Channel Option, making any model ready for deployment on Storage Area Networks.

SAIT will shortly incorporate Write-Once Read Many (WORM) functionality, making all SAIT drives able to perform dual roles. This unique capability is made possible through the use of the MIC chip-in-cartridge technology together with special drive firmware that prevents data overwrite on media that is designated and created as WORM media. Any SAIT drive can operate in either read/write mode or in WORM mode. Qualstar has previously teamed with Sony to create AIT WORM-based libraries built around AIT-3 drives and media.

WORM tape functionality will become highly desirable as the most cost-effective method of meeting the new government records retention requirements for health care, the securities industry and corporate governance. Recent regulations such as

SEC 17a-3 and 17a-4, HIPPA and the Sarbanes-Oxley Act require that any records that are stored electronically must be stored on media that are non-erasable and non-alterable. WORM tape has already been certified to meet these new standards. According to the Enterprise Storage Group, these latest government regulations will boost the worldwide capacity for record compliance from 376 petabytes this year to 1644 petabytes by 2006. WORM tape is ideally positioned to meet this demand, with a solution that provides an unmatched value proposition for endusers with a need to comply with these new government standards, and a potential goldmine for resellers with the vision to tap into this market.

### **Summary**

The threat of data terrorism is real and growing. IT managers are battling this threat by employing a variety of network security features to prevent data terrorists from getting in. But the terrorists are succeeding at this cat-and-mouse game, constantly devising new ways to defeat even the latest security measures. As long as critical data is online, it is available to a data terrorist. The simple reality is that firewalls alone don't protect your data. Even if the data terrorist succeeds in getting access, the damage can be contained if enterprises employ data protection strategies that de-couple the data from the terrorist. The only sure way to achieve this de-coupling is to backup and archive all critical data to a Qualstar automated tape library and secure it offline where it is beyond the reach of even the most clever data terrorist.