Technology Paper

Seagate Secure™ Technology Enables Robust Security Within the Hard Drive

The Rising Value and Vulnerability of Digital Content

Stolen trade secrets and intellectual property can mean millions of dollars in lost business. The proliferation of valuable, business-critical data on mobile devices increases the risks. Consumers face the high cost of identity theft when Social Security numbers, account data, addresses and other personal information is stolen. Irreplaceable family photos and media downloads, stored in increasing numbers on consumer devices, have their own inestimable value.

For many organizations, compliance with data security and privacy legislation, such as the Sarbanes-Oxley Act and the Health Insurance Portability and Accountability Act (HIPAA), has become an urgent priority. At the same time, the security of critical digital content—including the secure disposal of electronic files at the end of the data lifecycle—is a critical requirement in many areas of business. Meanwhile, content owners and service providers engaged in the distribution of media, entertainment, gaming and other content need stronger security to protect digital assets and enable new business models to meet evolving consumer demand.

Seagate is working to deliver the highest levels of data security with innovative Seagate Secure™ technology[1], a fundamental evolution in data security with the advent of self-encrypting hard drives that automatically and transparently protect confidential information on all hardware platforms. Seagate Secure technology ends the traditional conflict between the desire to empower users with the information and exercising robust and compliant data security measures. Among other safeguards, Seagate Secure technology delivers powerful disk encryption, scrambling data to prevent unauthorized access to hard drives in notebook computers, consumer electronics or other devices.

The Cost of Security Breaches

News of security breaches frequently appears in national media, and the costs associated with compromised data continue to rise. According to the Ponemon Institute, a single data breach will cost a company on average US$4.8[2] million in direct costs (legal expenses, customer notification and other remedies),

Seagate Secure™

[1] Previously referred to as DriveTrust technology
[2] The Ponemon Institute, "2006 Annual Study: Cost of a Data Breach," October 2006

indirect costs (lost productivity), and opportunity costs (customer loss and customer recruitment). Organizations dealing with lost or stolen personal information face dwindling public trust, especially as more laws and regulations mandate the public disclosure of security breaches.

In a study conducted by global IT service provider Computer Sciences, chief financial officers rated information security as their top priority.[3] The need for tighter security has increased as technology matures, becomes more complex, and reveals additional vulnerabilities. What's more, the need for security escalates with the proliferation of critical data on mobile devices and notebook computers, which are easy targets for theft and are easily lost. Compounding the risk, compromising the passwords and authentication schemes for these devices is by no means a challenging task for the technically savvy.

In recent years, the U.S. government has enacted security and privacy legislation aimed at protecting personal data. Compliance is mandatory and requires organizations to secure access to data and to securely dispose of electronic files at the end of the data lifecycle. Meeting expectations of the public—and complying with government legislation—requires organizations to scrutinize current security infrastructures and policies. Remarkably, only 20 percent of the chief financial officers interviewed in the Computer Sciences study claimed to be "highly satisfied" with their security technologies.

One well-publicized case of compromised security was that of the U.S. Veterans Administration, which experienced the theft of a laptop computer with extensive, confidential records of veteran's personal information. Although the computer was recovered, the risk was deemed high enough for the Veterans Administration to request US$160 million in funding for credit monitoring necessitated by compromised information—an extremely high cost incurred by a single incident.

Traditional Security Options

Organizations have many options for deploying information security on desktop computers, at the server, inside the corporate network and on the Internet. The cost of implementing security extends beyond purchase and installation to include maintenance, upgrades, support and testing costs. For organizations with limited resources, these direct and indirect costs, and the logistics of deploying security, can be daunting.

Other common concerns related to security implementation include:

- Multiple, unintegrated point solutions. Organizations must choose various safety measures to protect their incoming, outgoing and stored data. These solutions can be highly complicated to implement, lack integration, and impose significant resource requirements. The combination of these factors can result in vulnerabilities that may be unknown until a failure or security breach occurs.
- Performance impact. Some security software applications consume system resources such as processing power and system memory to perform encryption or to manage data. This resource draw can slow overall system performance.
- Lack of extended data access controls. Once software-based security, such as a password, has been breached, there's typically a clear path to data on the hard drive. Most solutions don't secure the data where the data resides, on the drive.

Benefits of Seagate Secure Technology

Seagate redefines the role of the hard drive through Seagate Secure technology. With hardware-based full disk encryption built in, Seagate Secure hard drives automatically and transparently protect confidential information. Self-encrypting hard drives provide the robust security needed to comply with data security measures. In addition, Seagate Secure technology provides a development platform for independent software vendors (ISVs) to create more robust applications that can manage security functions or interoperate with secure storage.

Hard drives provide the perfect infrastructure for data security:

- **Secure computing environment.** A hard drive's CPU, storage and firmware manage

[3] http://www.eweek.com/article2/0,1895,1988728,00.asp

drive operations independently of other system resources, making it difficult to compromise or attack the drive. Seagate Secure technology further strengthens the security of a drive through authentication and a secure communication infrastructure.

- **Independent data processing unit.** Hard drives include powerful processors, high-speed memory and multiple data ports. Seagate Secure technology has very little, if any, impact on the overall performance and speed of drives or systems.
- **Private code execution.** Drive-level firmware runs in isolation from other system resources and cannot be manipulated or modified by malicious code. Strong access control and trusted communications ensure that only authorized applications have access to security functions for designated storage resources.

By protecting critical information where it lives, Seagate Secure technology automatically and transparently enables powerful data security. Without any need for user intervention, all data stored on the drive is protected at all times. For example, if a system's operating system is compromised, the security functions are not affected and will continue to protect the data.

The Seagate Secure platform gives organizations a comprehensive data protection solution that is easy to deploy and manage. Drives protected with Seagate Secure technology reduce the overall complexity of the IT security environment by supporting complementary security applications. Drive-level security operates transparently and has few requirements for installation, configuration and setup. Organizations can use self-encrypting drives to create a standardized, secure storage platform and streamline the deployment process for data security regardless of applications, operating system or hardware.

By facilitating the security of digital data where it is stored, Seagate Secure technology becomes a solid foundation for a secure IT environment. Seagate Secure technology enables the secure access, distribution and storage of critical information through strong access and authentication control, secure content and application delivery, cryptographic functions, protected storage, and secure erase and disposal. Some of the solutions and benefits provided by Seagate Secure technology include:

- **Full disk encryption (FDE).** This solution automatically encrypts and decrypts all the data that travels in and out of the drive. Unlike other data encryption applications, Seagate Secure encryption keys are password-protected and never appear in the clear or in any readable format on the drive.
- **Drive pairing.** Seagate Secure technology allows users to "lock" a drive to a specific system or host. This solution prevents the illicit copying and distribution of the data if the drive is removed and installed in another system.
- **Secure partitions.** Hidden storage, accessible only by Seagate Secure-enabled software applications, provides a secure environment for additional drive-level security solutions, including access control, ID and authentication, anti-virus protection and token-free security.
- **Secure erase and disposal.** Encryption combined with strong authentication simplifies and secures hard drive disposal and reuse. Data on an encrypted drive is only accessible when the encryption key is enabled through a valid password. If the encryption key is changed or eliminated, all of the data is instantly rendered inaccessible. Technicians can then safely repurpose or dispose of the drive, without compromising sensitive information.

Seagate Secure Technology Fundamentals

Seagate Secure technology comprises four technologies: enhanced firmware, trusted send/receive, secure partitions and issuance protocol. Together these elements create a secure storage solution. In addition, a software development kit is available to help ISVs develop Seagate Secure-enabled applications.

Enhanced Firmware

Firmware is the software that runs on the drive's internal computer; it is normally used to manage extremely complex drive functions such as moving the read/write heads, tracking bad sectors on the disc and storing bitmaps of where data is located. Seagate Secure technology extends a drive's capabilities with additional security code optimized on the drive's computing resources. Seagate Secure technology implements a cryptographic service provider on the drive,

including encryption, hashing, secure storage, decryption, digital signature and random number generating functions.

Trusted Send/Receive Command Set

Extending trust to storage requires a secure communication infrastructure. For that reason, another critical element of Seagate Secure technology is the trusted send/receive (in/out) command set specification, designed in collaboration with the standards bodies that define ATA and SCSI interfaces.

Secure Partitions

A 200-GB hard drive reserves roughly 200 MB for internal system memory. Seagate Secure technology uses this space to create secure partitions that are both logically and physically separated from the rest of the drive memory, with strong conditional access controls—providing an excellent place to store cryptographic keys. Seagate Secure-equipped drives can make these secure partitions exclusively available to applications that present the proper credentials. ISVs can make use of this capability to build strong authentication functions into their applications.

Issuance Protocol

Software applications, basic input/output systems and other programs interoperate with a Seagate Secure-equipped drive through strictly controlled communication channels. ISVs and developers can write applications and have them assigned to a secure partition in the drive through the issuance protocol. Anytime the application attempts to access those secure resources, it must present its credentials—given under the issuance protocol—to the administrator function in the drive. The administrator function authenticates the application, activates the appropriate secure partition, and thus allows the application to interact with the secure partition through the trusted send/receive command set specification.

Meeting Compliance Needs

In recent years, government regulations have emerged that set strict requirements for the ways in which organizations manage and protect business and personal information. Seagate Secure technology helps companies address compliance issues by providing a simple, effective way to secure stored data through strong encryption and authentication. Encryption is recognized as a best practice against theft or loss of private data. In the United States, implementing effective data encryption can provide safe harbor from state and federal requirements for public disclosure of a data breach.

The Trusted Computing Group

The Trusted Computing Group (TCG) is a not-for-profit industry organization formed to develop, define and promote open standards for hardware-enabled trusted computing and security technologies. Seagate presented the Seagate Secure technology to TCG as the basis for extending trust and security to storage devices. This led to the formation of the Storage Work Group that includes all leading disk drive manufacturers as well as vendors of flash storage, storage management and storage integration.

The Storage Work Group is developing the Core Storage Specification that will enable secure storage solutions to protect data and interoperate with trusted systems. The primary goal is to help users protect information assets such as data, passwords, and encryption keys from attack and theft. The Core Storage Specification is currently being finalized for publication and future Seagate Secure-enabled products will comply with the open standard. Seagate chairs the Storage Work Group is actively contributing to the standardization effort.

Seagate Secure-Enabled Products

As the world's largest hard drive supplier, Seagate can deliver a broad range of Seagate Secure security solutions through original equipment manufacturers (OEMs), system builders, integrators and software partners.

Today, Seagate offers two product lines that feature Seagate Secure technology: the Momentus 5400 FDE drive for notebook computers, the first hard drive with full disk encryption, and the DB35 Series drive for digital video recorders (see Figure

Seagate Secure™ Technology Enables Robust Security Within the Hard Drive

1). The second generation of each line is being prepared for production, and Seagate continues to explore other applications to fulfill the promise of the technology.

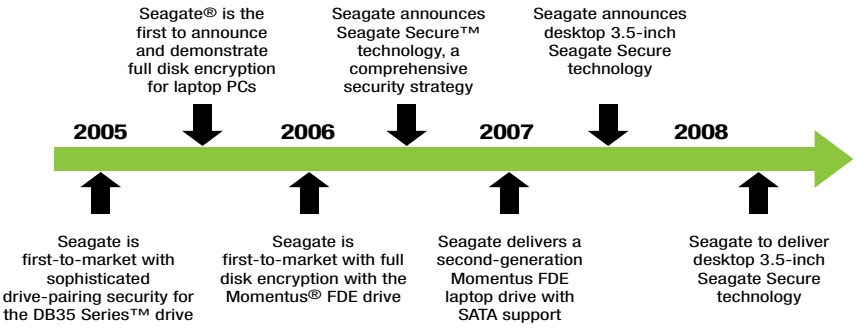

Figure 1: History and immediate future of Seagate Secure technology

Conclusion

Seagate Secure technology is meeting the growing need for data security by protecting digital information where it is stored—on the hard drive. The tools and safeguards provided by Seagate Secure technology are ushering in a new era of safe computing, giving businesses, government agencies and individuals the highest levels of protection for their digital assets.

Resources

Learn more about Seagate Secure technology:

- Visit www.seagate.com/security
- Trusted Computing Group: www.trustedcomputinggroup.org/home
- TCG Storage Work Group: www.trustedcomputinggroup.org/groups/storage/

AMERICAS Seagate Technology LLC 920 Disc Drive, Scotts Valley, California 95066, United States, 831-438-6550
ASIA/PACIFIC Seagate Technology International Ltd. 7000 Ang Mo Kio Avenue 5, Singapore 569877, 65-6485-3888
EUROPE, MIDDLE EAST AND AFRICA Seagate Technology SAS 130–136, rue de Silly, 92773, Boulogne-Billancourt Cedex, France 33 1-4186 10 00