Seagate and Dell: Bringing Hardware-based PC Encryption to the Masses

Date: January, 2009

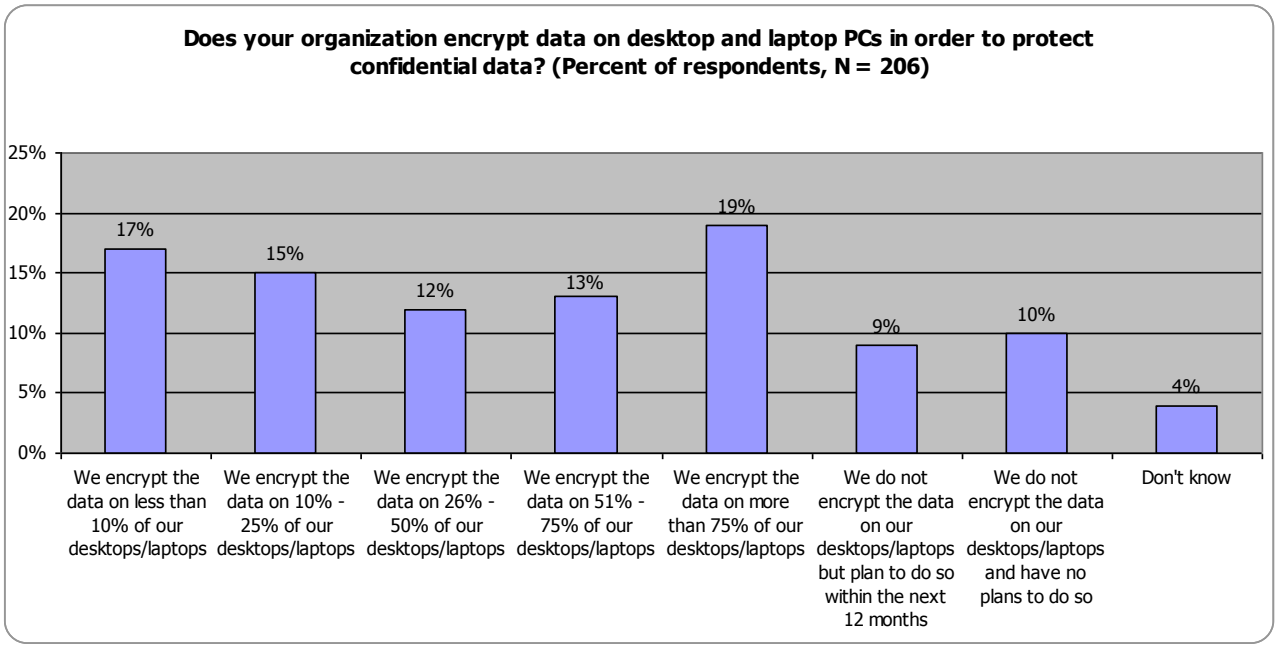
Author: Jon Oltsik, Senior Analyst

Abstract: Facing a combination of regulatory compliance, malicious threats, and publicly-disclosed breaches, PC encryption has become a requirement for most businesses. Historically, that meant encryption software, but this model will likely become obsolete as more PCs integrate self-encrypting hard drives. Why? Hard drive-based encryption offers ease-of-use, performance, and security advantages that are too attractive to pass up. This conversion is gaining tremendous momentum thanks to the activities of leading technology companies like Seagate and Dell.

Overview

In the early part of this decade, few organizations believed that PC encryption was necessary. If a laptop was lost or stolen, IT managers were actually more concerned about backing up and recovering sensitive PC-based data than were about protecting it from falling into the wrong hands. Fast forward to today—attitudes have radically changed. Driven by visible data breaches, embarrassing headlines, and regulatory compliance mandates, large and small organizations are demanding Full-Disk Encryption (FDE) as a standard for laptops. In fact, according to ESG research, nearly 90% of large organizations use FDE on their PCs today and nearly one-third of enterprise firms have implemented encryption on more than half of their PC portfolio (see Figure 1).

FIGURE 1. PC ENCRYPTION IS BECOMING UBIQUITOUS



Source: Enterprise Strategy Group, 2009

PC Encryption Can Lead to Software Headaches

As executive management and CIOs mandated PC encryption, IT managers scrambled to find adequate solutions. Typically, this meant purchasing and installing add-on encryption software available from a plethora of

vendors. This certainly seemed like a straightforward proposition—simply purchase software, install it on sensitive systems, and voila: instant encryption. Unfortunately, things are never as easy as they seem. Software-based encryption can be difficult because:

- **Software encryption can create security vulnerabilities and operations.** Ironically, encryption software often leads to new types of security risks. For example, encryption software relies on the security of a general purpose operating system and PC hardware to store user credentials and encryption keys. Industry tests have revealed lots of weaknesses here. For example, some encryption software tools store this information (i.e., user name, password, encryption keys, etc.) in main memory as cleartext. Encryption software with this vulnerability may protect data confidentiality against a common thief, but would be no match for a skilled and motivated hacker. In addition to vulnerable software, IT managers must also marry software encryption tools to centralized services for key management, password reset, and auditing.

- **Software encryption may mandate changes in user behavior.** Some desktop encryption software may require users to install software and input their user name and password multiple times (i.e., pre-boot authentication and then network authentication). Other encryption software may also interfere with system sleep, hibernation, or undock functions. Additionally, software encryption can seriously impact system performance, impacting user productivity. Users need to be aware of which data is and is not encrypted. Lastly, users have to decrypt and re-encrypt the hard drive for certain kinds of software OS updates. These issues can become a major nuisance across an enterprise of thousands of users. When employees complain about encryption-related production bottlenecks, angry business managers will certainly place the blame squarely on IT.

- **PCs come in many flavors.** Users with multiple operating systems, various PC hardware platforms, and lots of system configurations often struggle with finicky encryption software. Overcoming these idiosyncrasies demands long testing periods, multiple configuration changes, custom installation scripting, and lots of help desk training for end-user support. To avoid implementation problems, many organizations will actually deploy encryption software as multiple unique test and deployment projects rather than one enterprise rollout.

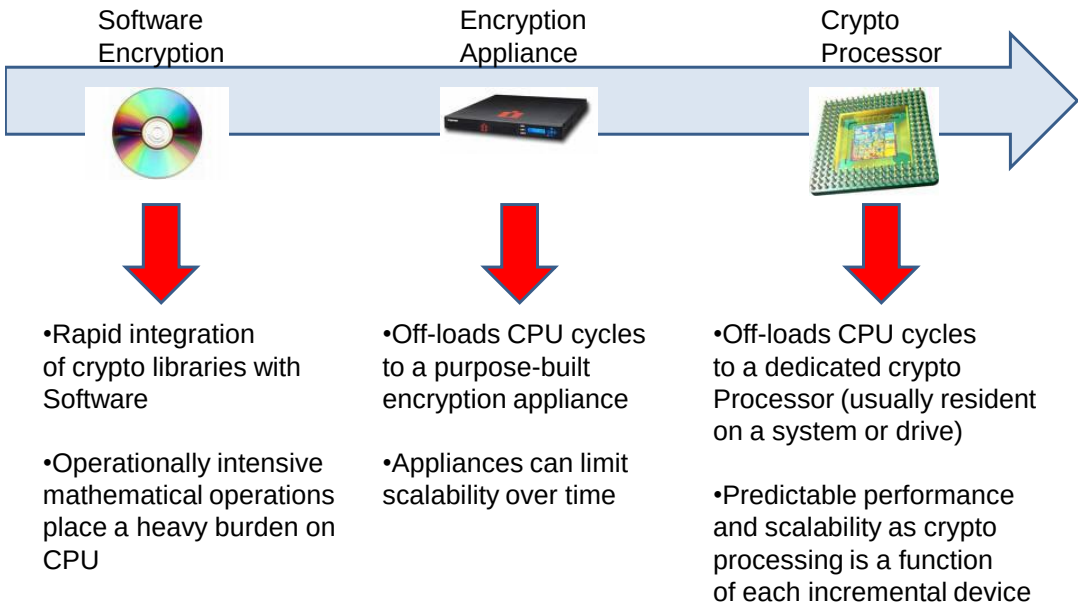
Ultimately, these shortcomings can make software encryption far more complex, time consuming, and costly than originally thought. Large, distributed enterprises with lots of PC variation tend to feel the most pain.

PC Encryption 2.0: Hardware-based Encryption Comes of Age

Encryption technologies tend to follow a predictable evolutionary cycle. Since cryptographic libraries can be added to source code fairly easily, software-based encryption is normally introduced first for data confidentiality. While this approach is the most straightforward, it also carries a high performance price. Since cryptographic operations require lots of CPU horsepower, software-based encryption is often replaced with more efficient hardware appliances or microprocessors dedicated specifically to cryptographic processing (see Figure 2). This progression is evident in many types of IT technologies. A few years ago, backup encryption was only offered as an extra feature in backup servers that most users eschewed because of its high cost and performance impact. Today, many users encrypt their backup jobs by using more efficient network encryption appliances or relying on embedded crypto processors resident in tape drives. IBM mainframes went through a similar cycle, replacing encryption software with a dedicated cryptographic co-processor in its System z.

This same evolutionary cycle is now gaining momentum with PCs—FDE software is being replaced by self-encrypting hard drives built with onboard cryptographic processors. This trend started with the Trusted Computing Group (TCG) storage specification effort and came to fruition with the announcement of the Seagate Momentus 5400 self encrypting drive and its DriveTrust initiative in 2006. What was once a trickle of products is now a flood—all major disk drive vendors are either shipping encrypted drives or have announced their intention to do so.

FIGURE 2. TYPICAL ENCRYPTION EVOLUTION



Source: Enterprise Strategy Group, 2009

The onset of self-encrypting drives represents an industry tipping point. Hard drive-based encryption will soon become the default PC encryption technology, replacing software alternatives. ESG believes this will take place over the next 12-18 months because:

- **Hardware-based encryption is easier to deploy, manage, and recover.** Since self-encrypting hard drives are 100% transparent to operating systems and applications, they can help IT eliminate complex compatibility testing procedures and expensive end-user training. This is especially attractive in light of the global recession, with IT managers operating under tight budgets and hiring restrictions. Self-encrypting drives streamline the data erasure process**.** An often overlooked benefit of hard drive-based encryption is that drives can be easily repurposed or retired without manual data erasure processes. When a drive needs to be moved offsite, security administrators simply delete the encryption key resident on the actual disk, rendering the data unreadable. By automating this process using cryptographic sanitation, IT can avoid the time and expense associated with traditional data erasure methods like physical destruction, degaussing, and software overwriting

- **CISOs will opt for hardware-based encryption because it is more secure.** FDE was once thought of as a "check-off box" security technology where any encryption option was deemed "good enough." This is no longer true—the Princeton "cold boot" attack on encryption software taught IT professionals that there are qualitative differences with encryption technology security. As CISOs realize these security advantages, they will recommend hardware-based encryption as part of all new PC purchases.

- **Hardware-based encryption provides better system performance**. According to performance tests conducted by the SANS Institute, software-based encryption runs approximately 30% slower than hardware-based options on average. This difference is significant enough to tilt the scale toward self-encrypting drives. Why? IT managers always opt for high performance technologies while business managers will extrapolate the 30% performance penalty as a potential productivity drain.

- **Hardware-based encryption delivers a better TCO**. Companies that deploy Seagate self-encrypting drives can see an immediate lower TCO based on the fact that these drives are 100% recyclable and reusable. However, the savings extend to the IT time it takes to manage this solution as it is quicker and simpler to deploy than software, requiring less than ten minutes for the initial encryption and laptop

repurposing versus approximately seven hours to do the same for software-based encryption solutions.

- **Self-encrypting drives will become part of every PC.** To drive down manufacturing and product costs, disk drive manufacturers like Seagate will likely add cryptographic processors into every drive they ship. As this occurs, it should: 1) reduce the actual price of encrypting PCs, making hardware-based encryption more attractive and 2) become a standard part of all new business PCs. In 2 to 3 years, it may be difficult to find a business PC without a self-encrypting drive.

These factors make hardware-based encryption an easy decision for CIOs, security professionals, and purchasing managers. As PCs with self-encrypting drives proliferate, IT operations will realize benefits as well because management software options continue to grow. Managing a mixed environment of PCs with software and hardware-based encryption will become increasingly easier as encryption management software vendors such as Wave Systems and WinMagic, who already provide support, are joined by other companies supporting Seagate self-encrypting drives. As this happens, enterprise organizations can gracefully transition from software encryption to self-encrypting drives as they purchase new PCs in their regular replacement cycles.

Dell is Leading the Transition

While most PC companies are slowly recognizing the conversion from software- to hardware-based encryption, Dell has been an aggressive supporter of the actual transition. With its long standing relationship with Seagate and early enthusiasm around the DriveTrust initiative, Dell is leading the way with:

- **The largest portfolio of PCs with self-encrypting drives**. Dell offers over a dozen different systems with hard drive-based encryption—from affordable notebooks to high-end PC workstations. This wide variety helps Dell marry strong security to user profiles and customer needs.

- **Implementation options.** Dell hardware-based encrypting PCs leave the factory with all the hardware and software needed to deploy the systems. For simple installations, Dell provides configuration software suitable for end-user management of drive encryption. For larger organizations, Dell PCs can be set up in DriveTrust mode to run with encryption management software, enabling centralized command-and-control for configuration and key management.

- **ISV partners.** Dell Latitude and Optiplex systems with encrypting drives come with factory-installed software for client management and optional server software for centralized IT management. A variety of encryption providers are also currently qualifying drive support within their software management tools.

The Bottom Line

Gordon Moore's famous law states that chip density doubles every 18 months, making microprocessors ever faster and cheaper. This phenomenon is now influencing PC encryption—henceforth, self-encrypting hard drives will become cheaper and more ubiquitous. Seagate and Dell are leading this foreseeable transition.

Given this inevitable trend, CIOs should prepare accordingly by adopting a transition plan. This should include policies, processes, and technologies for configuration management, end-user support, key management, and data destruction. Smart IT managers will begin this process immediately so they can begin their transition to hardware-based encryption ASAP.