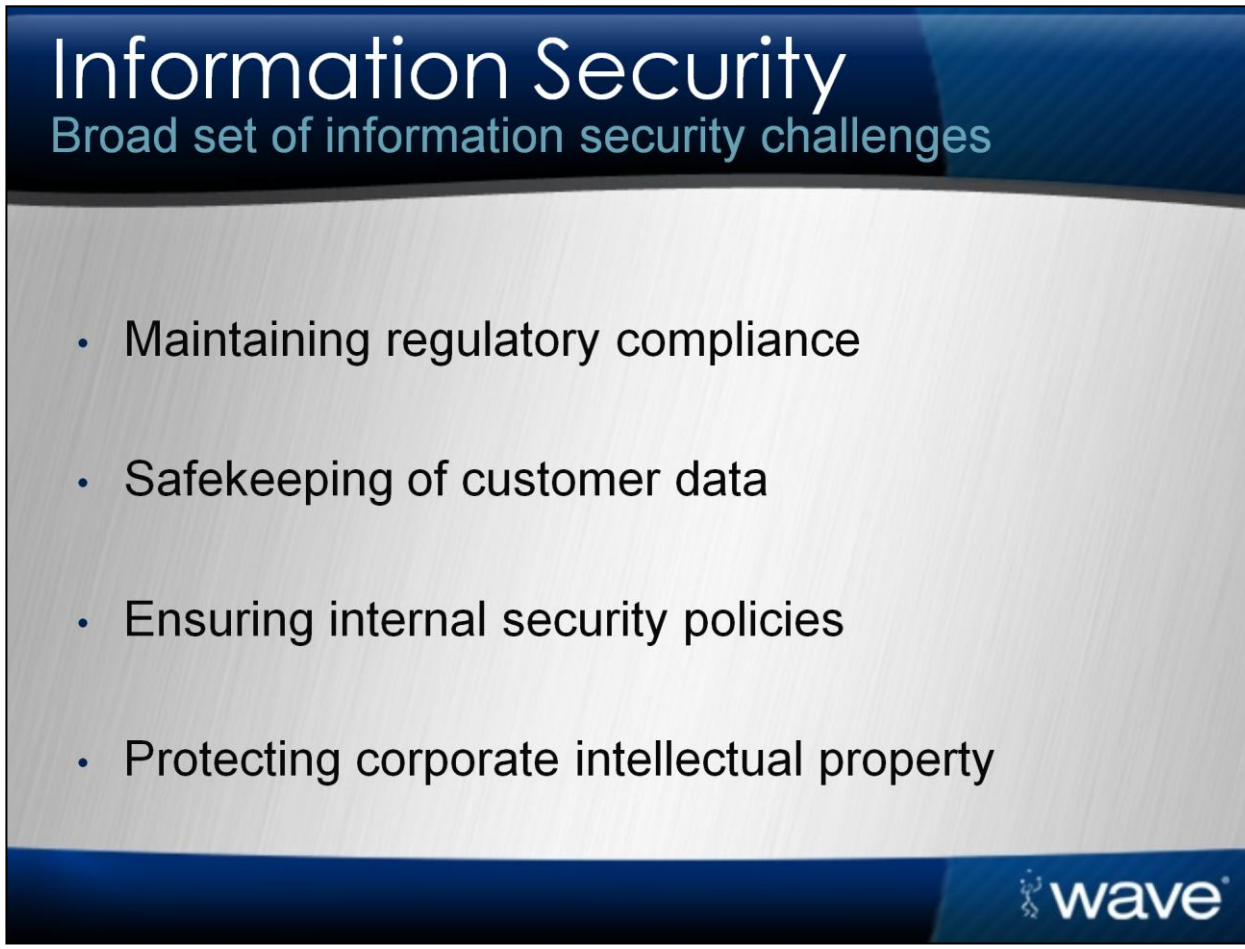
Presented to Central Plains ISSA on 5/7/2010



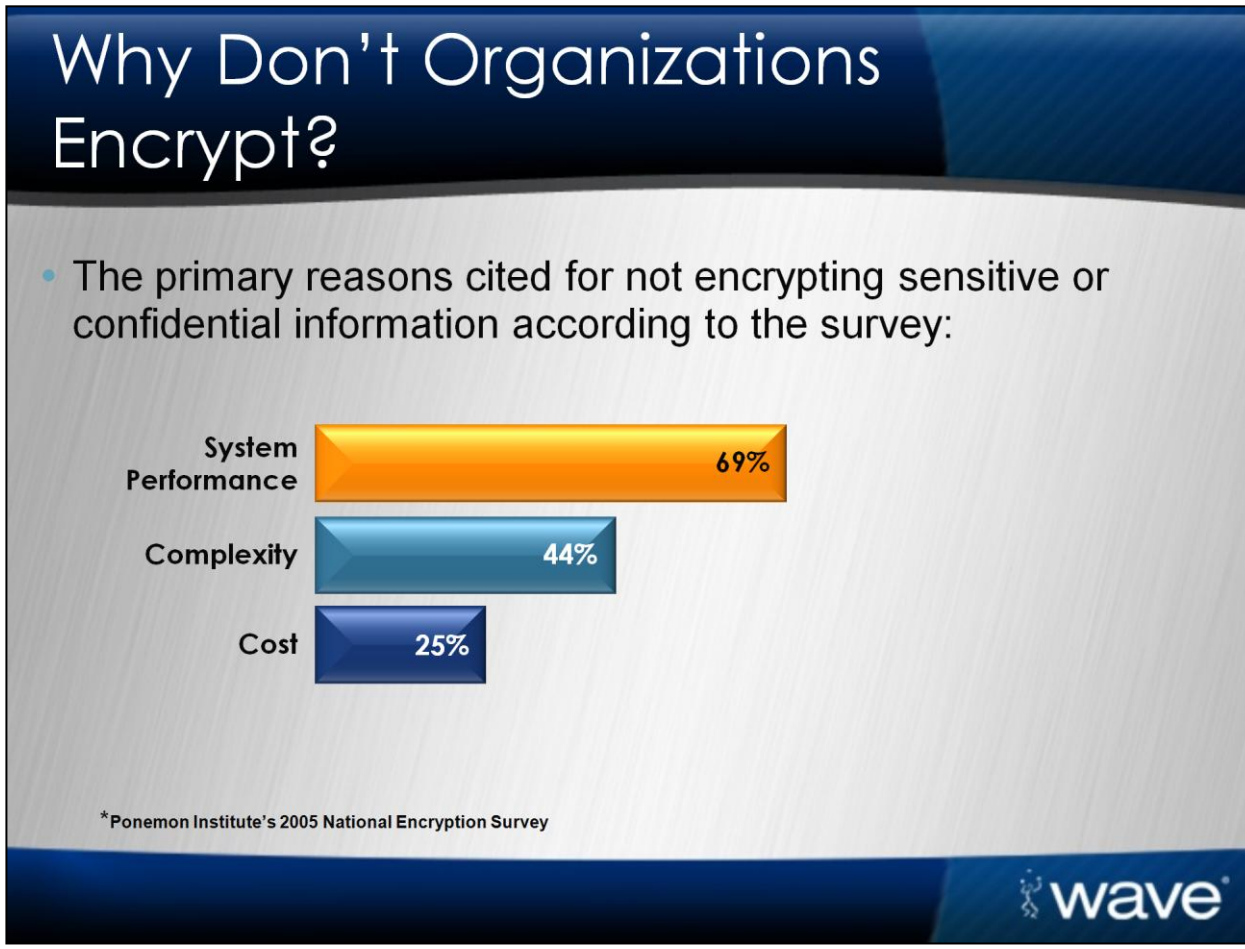
Where the buck stops on a lot of these threats is at the CEO's desk. However, every IT Security person I speak with tells me that there are four demands:

The first is Regulatory compliance—It has become a mandate, whether companies want to do it or not.

The second is the Safekeeping of customer data—This is critical, particularly in the case of any enterprise that talks to or takes care of individuals. Example: The personal information, be it health, financial or other information is clearly data that you do not want out in the hands of unauthorized people. This data could be mis-used from the perspective of your Enterprise itself, as well as being used in a harmful way against the individuals themselves. Neither of these is a risk worth taking.

CEOs also have to worry about abiding by their organization's own Internal Security Policies—many times this is the fundamental check and balance against maintaining compliance to external regulations. Additionally, no operating or financial data that is proprietary to your organization should be at risk of getting into the hands of unauthorized individuals.

Protecting Corporate Intellectual Property which is a fundamental requirement in any corporation.



Companies know they need to encrypt.

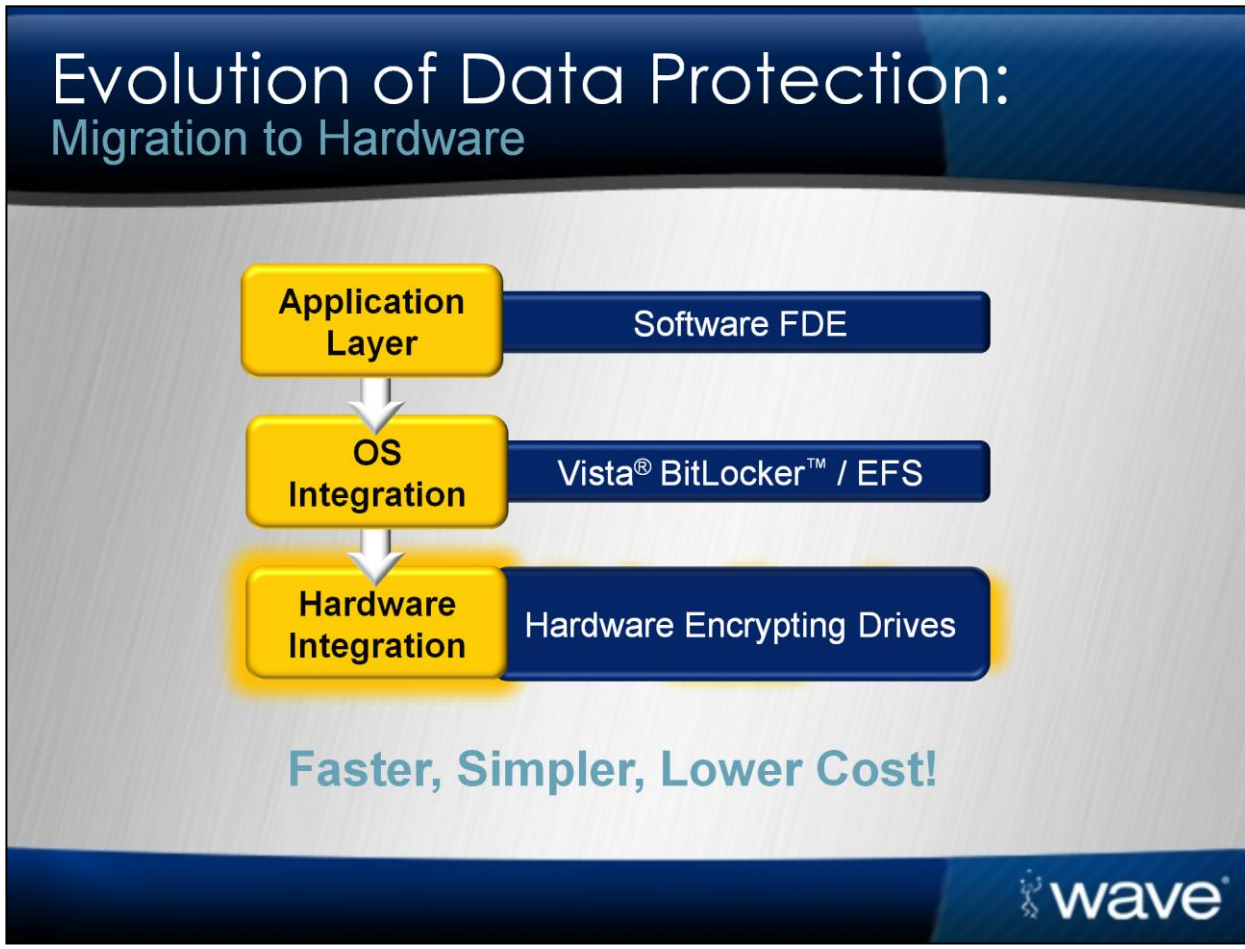
Why are they not doing it? Or doing only a limited amount?

Because:

1. System Performance - most full disk encryption software hits the hard drive and CPU pretty hard. Every time a bit has to get written back and forth to the drive, the CPU has to spend cycles there to crypt and decrypt . As applications and OS's have gotten more complex the hard drives gets hit a lot and that can slow system performance to a crawl.

2. Complexity – installation can be a complex and lengthy process. Turning on a full disk encryption software package can take many hours as it goes through existing data and encrypts every bit back and forth to the drive. Maintaining these systems can be time consuming.

3. Cost - encryption is not free, it costs something to do this. And much more than the modest cost of the software, is the cost of maintaining it. It's the IT person having to touch every machine – every time something has to be changed; or every time you install an application that doesn't play nice with the encryption software; or when an employee loses their password, or leaves the organization and they have to re-provision the machine



We are all in the middle of a natural migration to using hardware solutions for data protection. In the past the only solutions out there for Encryption were SOFTWARE at the application layer, file and folder encryption and then, Full Disk Encryption powered by the operating system. (Vista's BitLocker is an example of this.)

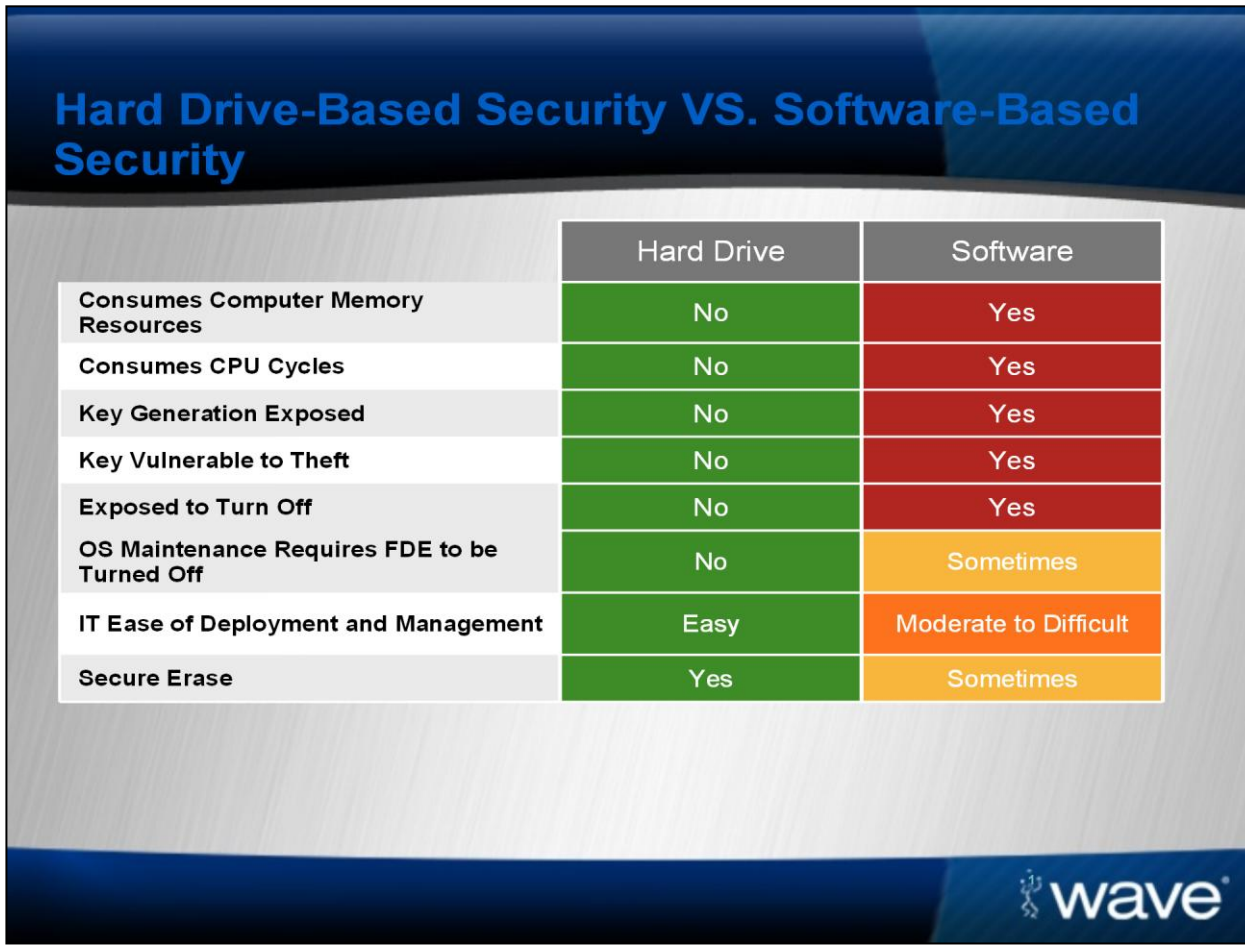
Now Data Protection has evolved to a deeper level. More basic level. It is now baked into the drives.

Over three years ago at the RSA Conference in San Francisco, Feb 2007 Seagate and Wave Systems, unveiled the Momentus 5400 Full Disk Encrypting drive. A few months later, Dell announced availability with new Latitude Notebooks and the Precision machines with Wave and Seagate.

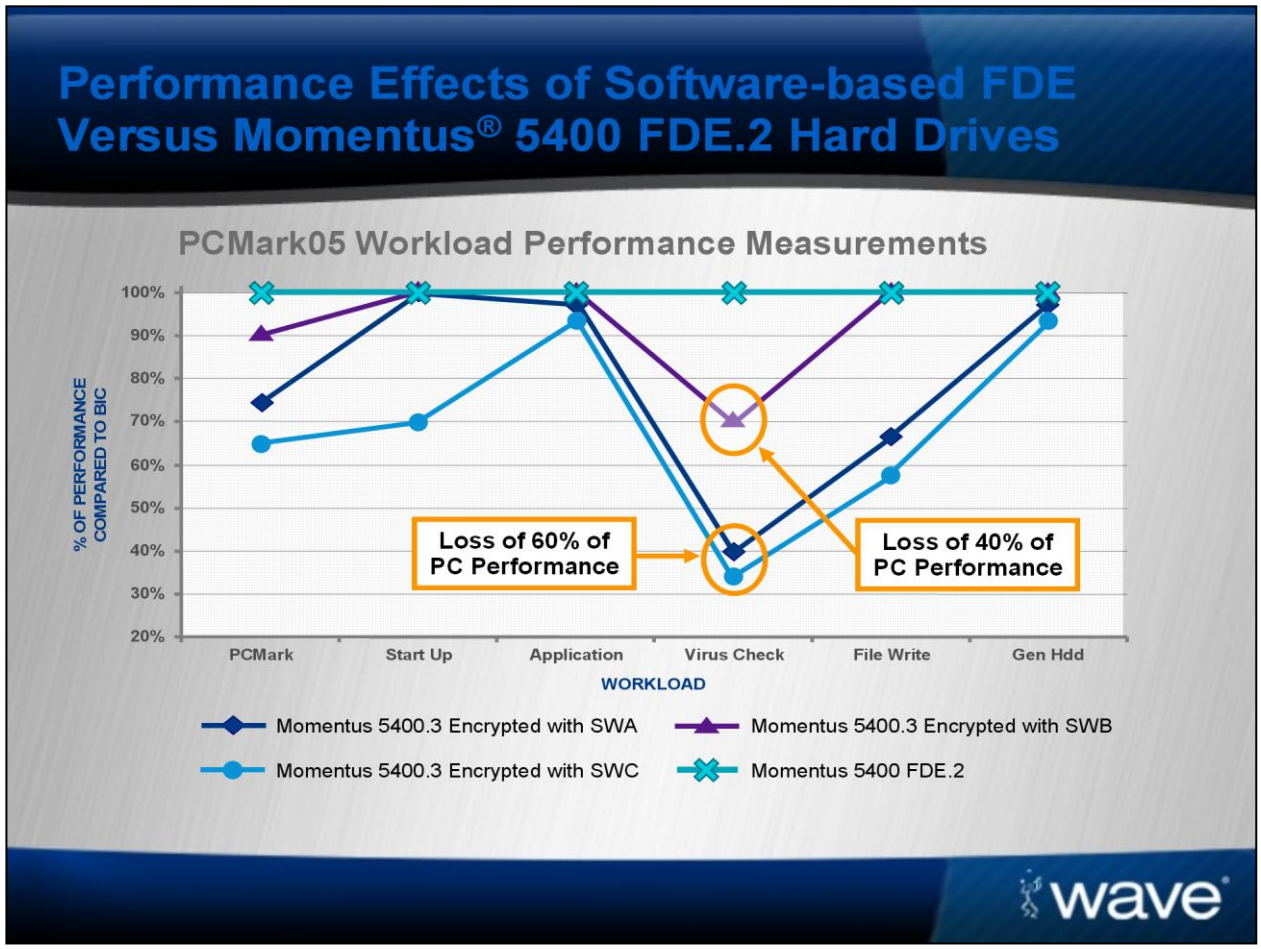
With this new drive, Authentication and Encryption became STANDARD FEATURES. Now Dell and HP ship machines with this drive installed!

Seagate put all security keys and cryptographic operations WITHIN THE DRIVE, separating them from the operating system in order to provide greater protection against hacking and tampering than traditional software alternatives, which can give thieves backdoor access to encryption keys and are more vulnerable to viruses. With today's solution, you have uses industry standard software that enables easy to deploy notebook PCs with strong hardware encryption and software infrastructure needed to manage your data and protect access to it.

Presented to Central Plains ISSA on 5/7/2010



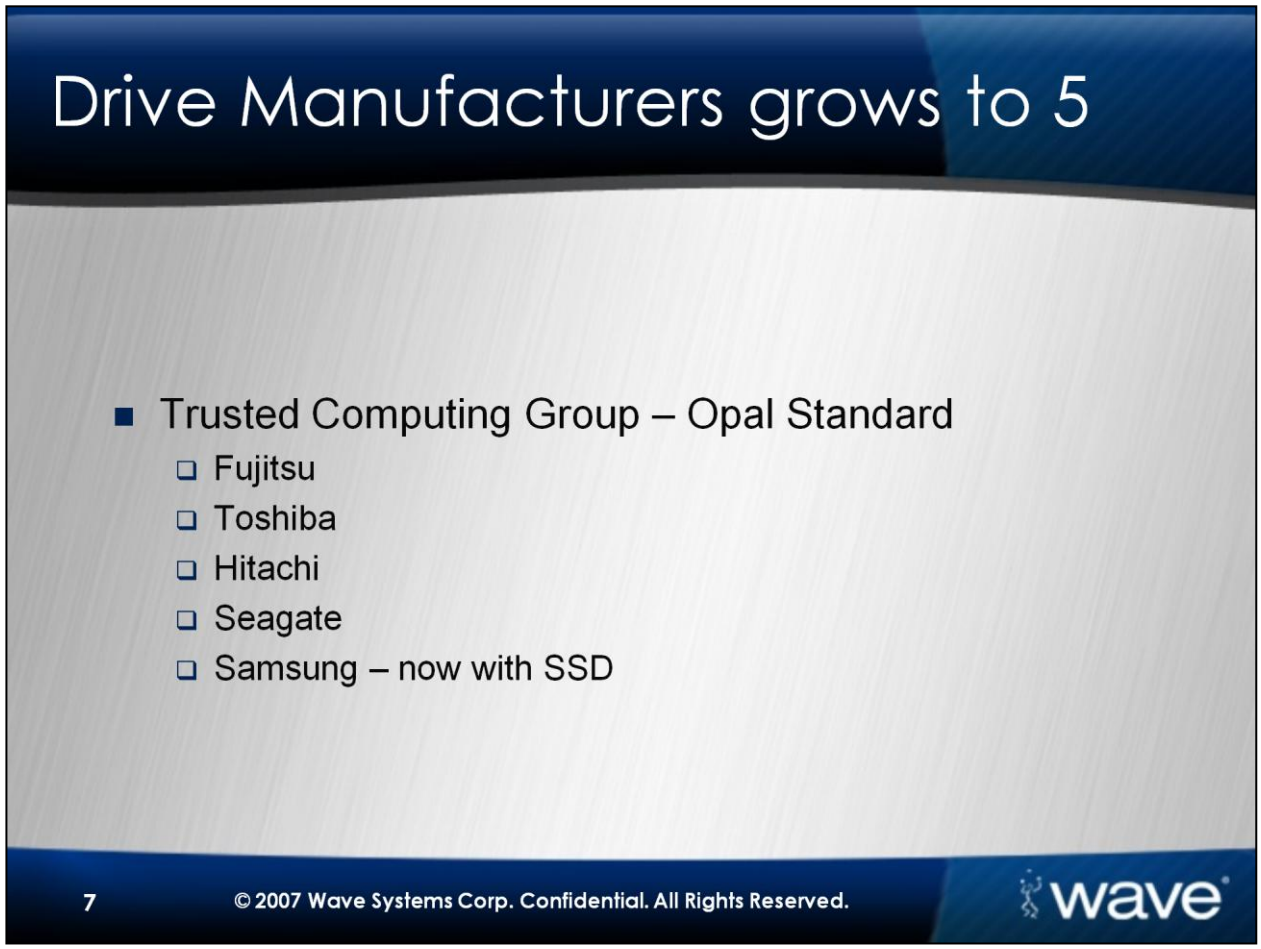
Here for more technical details, please get in touch with Wave (Frances Rivoire) to help you articulate the issues. This is a generic slide and could be used more accurately when a specific software solution is the basis for comparison. The Wave Engineer can speak to you about the key being encrypted and hidden on the drive itself. It is not exposed in memory. Memory has been hacked. The attached graph shows you the "CPU cycle" lab test by Seagate. I will discuss Secure Erase for you (saves you wiping 3 times, etc, at the end of life or re-provisioning) and how that is worth $100 every time you press the key. Of course, it is a protected function, only to be used by an authorized user. Oh, and can be done remotely. Very powerful.



What this slide shows is (SWA, SWB, SWC are Software Encryption Products) the loss of performance is indicated.

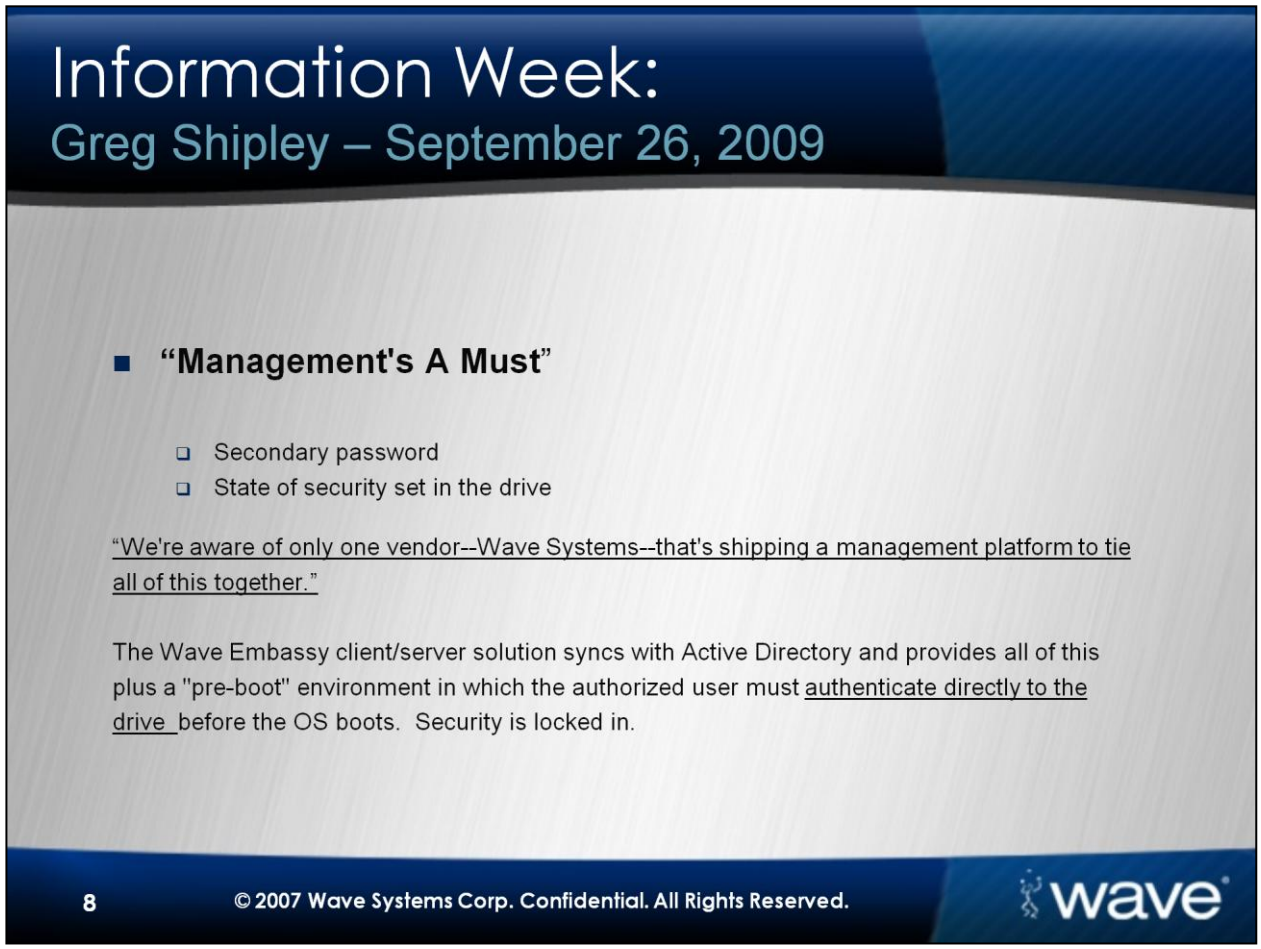
I use this slide as an example of the "consumes CPU cycles" on the previous slide.

The blue X shows you performance when Hardware Encryption, now known as Self Encrypting Drives are used. In other words, a straight line NO PERFORMANCE HIT AT ALL!!!



Five drive manufacturers are making these drives now. This is not a "niche" or a flash in the pan. This is an evolution in drive design and you will see it become ubiquitous.

Note there is standard now, for Hardware Encrypting Drives. It is called OPAL. Anyone can manufacture to this standard. This drives price down.

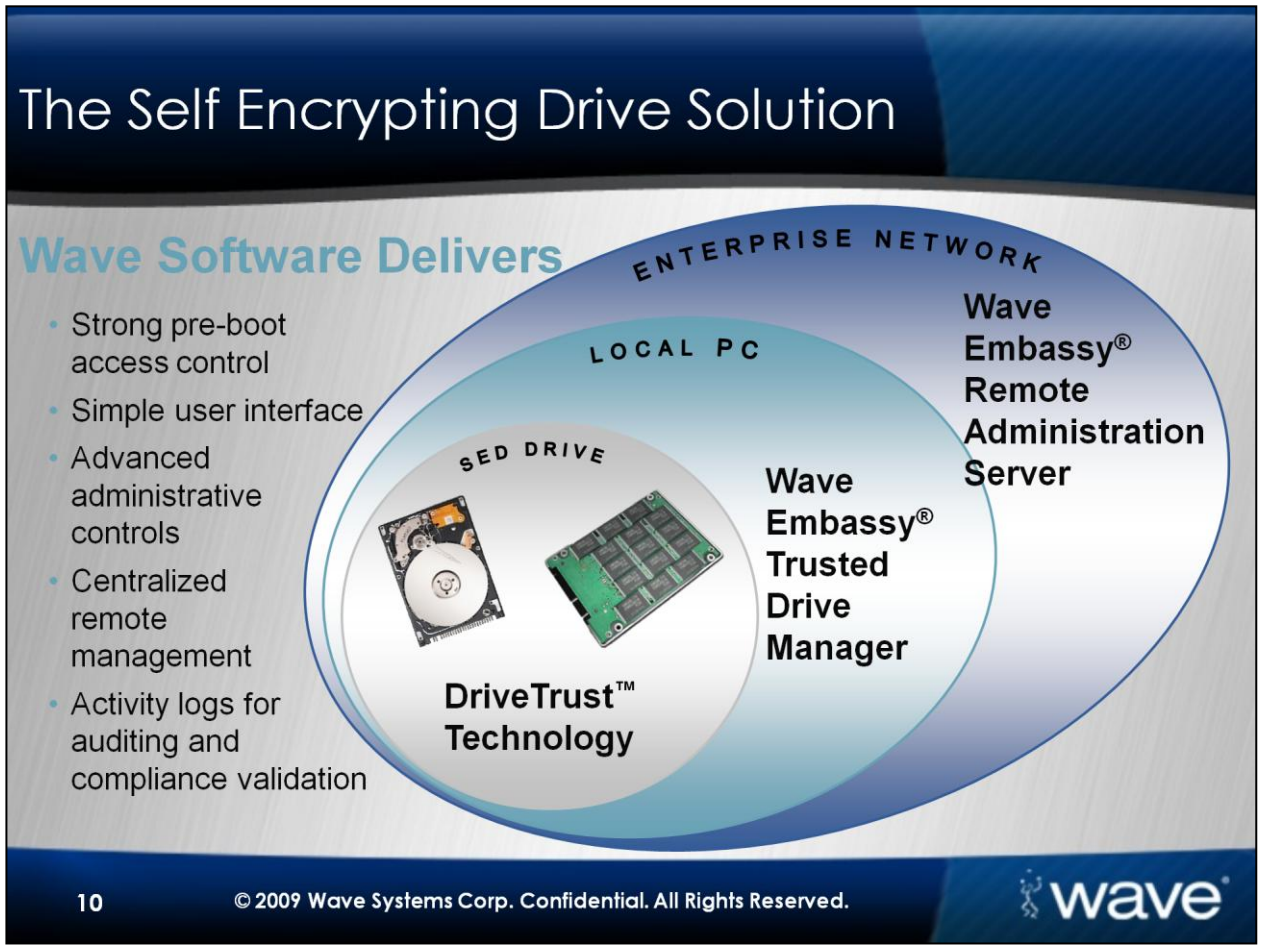


This a direct quote from Information Week

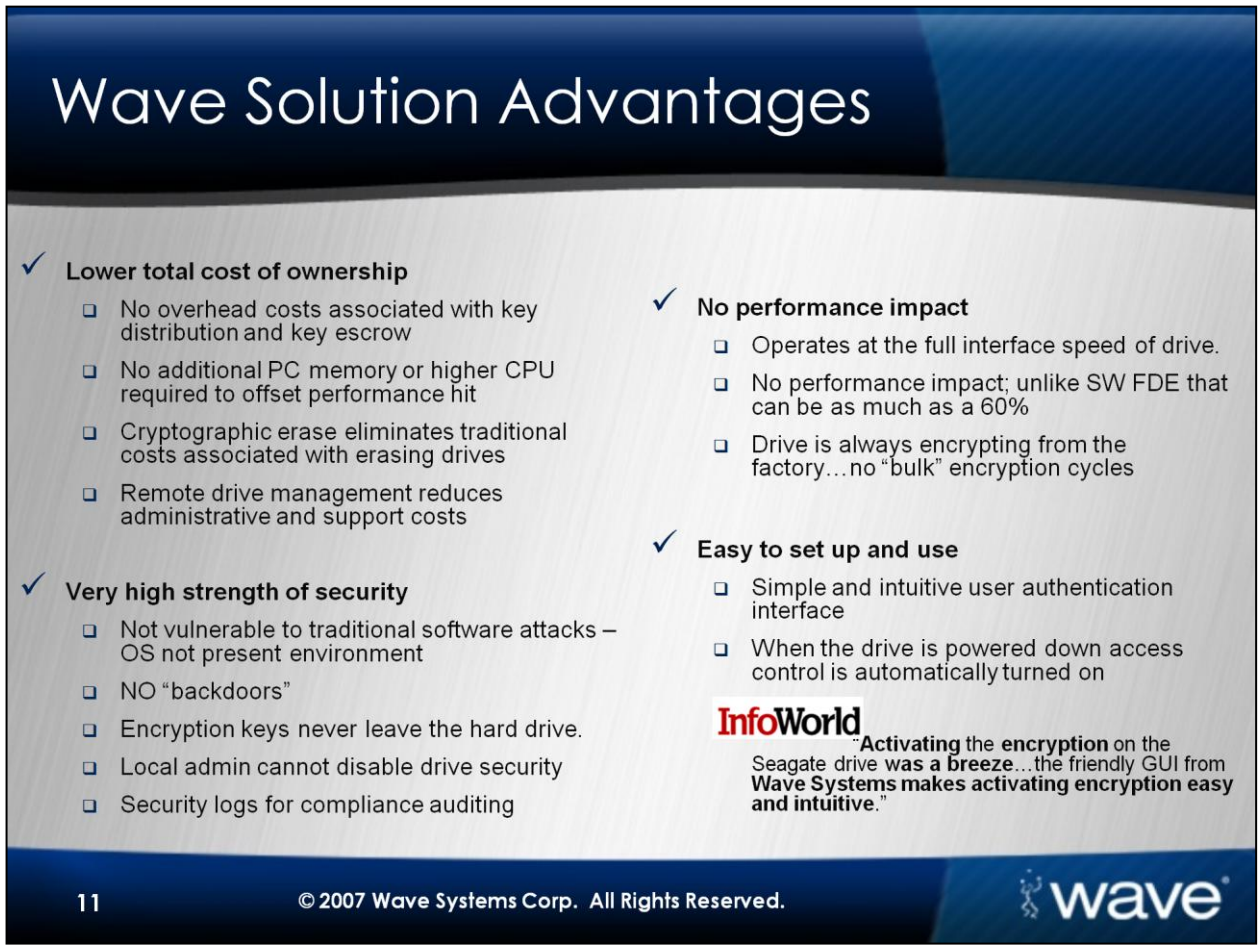
This technology has been around over 3 years now. You are not the first. Two generations of Dell Computers have shipped from the factory with hardware encrypting drives as a standard option. HP announced the availability of the same technology and is providing that in early 2010. Wave ERAS manages all of them.

This slide illustrates two key points:

1. All verticals have adopted hardware based encryption because data protection is important to all.
2. A lot of different companies/universities and government agencies have adopted Wave ERAS and hardware based encryption. More than will fit on this slide.. There are many others you can speak with.



This slide shows the hardware and Wave software components at the Enterprise Level and the Local PC Level. This explains the architecture, with hardware at the heart of it. The bullets describe several features that are very critical to any kind of enterprise deployment.



Wave Systems and Seagate originally teamed up and developed the premier mobile data encryption solution for organizations of every size and stature.

Today it is available for all manufacturers who are delivering hardware encrypting drives that can be managed.

Because this solution is hardware based and embedded within a PC it offers unparalleled performance and security benefits. The data encryption key and the pre-boot authentication policy are executed in the drive controller and therefore are not susceptible to traditional software attacks. Wave's EMBASSY Trusted Drive Manager and Remote Administration Server makes the activation, use and management of these Seagate drives easy and intuitive…which in turn provides a lower cost of ownership as associated deployment and ongoing management costs will be minimized.

Thank you!

Questions?

Frances Rivoire
Wave RSM – N. Central
815-858-3437