Self-Encrypting Drive
Market & Technology Report

Thomas M. Coughlin
Coughlin Associates, Inc.

August 2011
Table of Contents

Executive Summary ........................................................................................................ 4
Introduction ..................................................................................................................... 4
Technology Options for Data at Rest ........................................................................... 5
Factors That Led to Slow Market Adoption of Self-Encrypted Storage Devices .......... 6
Factors Favoring Future Growth of Self-Encrypted Storage Devices ......................... 8
Some Additional Benefits with SEDs........................................................................... 14
Market Projection Methodology for Self-Encrypted HDDs and SSDs ......................... 14
Market Projections for Self-Encrypted HDDs ............................................................... 16
Market Projections for Self-Encrypting SSDs .............................................................. 22
Summary....................................................................................................................... 25
Appendix: A Discussion of Growth Modeling.............................................................. 26
About the Author: ......................................................................................................... 30
Sources and References............................................................................................... 30

Table of Figures

Figure 1. Banded Hard Drive Volume Projections......................................................... 16
Figure 2. Projection of Drives by Market Niches (in 1,000’s of units) ......................... 17
Figure 3. Security Adoption for Laptop HDDs ............................................................. 18
Figure 4. Security Adoption for Enterprise HDDs ....................................................... 19
Figure 5. Security Adoption for Desktop HDDs ......................................................... 19
Figure 6. Security Adoption for Consumer Electronics HDDs .................................. 20
Figure 7. Security Adoption for all HDDs Market Segments ....................................... 21
Figure 8. Security Adoption SED HDD Estimates (high, median and Low) ............... 22
Figure 9. SSD Annual Shipped Unit Projections ......................................................... 23
Figure 10. High/median/low SSD Estimates............................................................... 23
Figure 11. SSD Security Adoption Projections ......................................................... 25
Figure 12. External Resistance Model Growth Curve ............................................... 27
Figure 13. Internal Social Model Growth Curve ....................................................... 29

List of Tables

Table 1. HDD Encryption Throughput Test Results (extracted from 2010 Trusted Strategies Report) ......................................................................................................................... 10
Table 2. SSD Encryption Throughput Test Results (extracted from 2010 Trusted Strategies Report) ......................................................................................................................... 11
Executive Summary
The major conclusions from this report are:

- **It is likely that by about 2017 all HDDs will shift to SED capable units, although estimated security adoption units by 2016 (SED capable HDDs actually used or intended for data security) are only 25% of all HDDs shipped.**

- **By 2016 the high, median and low estimates for security adoption for SED HDDs are 411 M, 315 M and 122 M units.**

- **We project that within 2 years (by 2013) SED capability will be in over 80% of SSDs and likely in almost all SSDs within 3 years (2014).**

- **Although actual SSD SED feature implementation in 2016 is likely to 100% in about 122 M SSDs, the projected actual SSDs from that year used for security and data protection purposes is estimated at less than 18 M units.**

Introduction
In July and August 2011, in cooperation with members of the Trusted Computing Group storage working group, Coughlin Associates conducted a survey of a number of interested parties to the use of encryption to provide security in various types of electronic equipment that use storage devices. Those interviewed included storage device suppliers (hard disk drives and solid state drives), systems OEMs, security software companies, storage controller suppliers and others.

Based upon input from the interviews we created a list of drivers for the use of self-encrypting drives (SEDs) as well as factors that limit their use in the market, both historically as well as in the near future. In this report we examine each of these positive and negative factors and look at their historical impact on the SED market and the implications of these factors in the future growth of SEDs, both HDDs and SSDs.

In addition to input from the interviews we also used public information such as press releases, reports and presentations to look at both past projections and factors driving or moderating future growth. We include references and material from these sources as appropriate in this report.

In the course of our analysis we came to realize that there was more than one type of metric for the growth of SED devices. The first metric is the growth of SED capable devices or SED adoption. SED capable devices have self-encryption built into the
basic architecture of the device. Data coming into and out of the device are encrypted or can be encrypted if this feature is enabled. The second metric is the growth of **security adoption** using SEDs. The first metric enables the second metric but not all SED capable devices will actually be or are intended to be used for protecting the privacy of data. Thus security adoption will by its nature be slower than SED capability growth.

We base our projections upon a simplified version of the Bass Diffusion Model\(^9\). This model is a mathematical model that projects growth of a market based upon accelerating and resisting factors. As a result of the interaction of these factors the resulting growth curve has a familiar s-shape. An analysis of the factors leading to s-curve growth is given in the report appendix. In our projection for security adoption we assume that all the SED capable devices sold to date are actually used for or intended to be used for the protection of data. We use historical data on SED HDDs and appropriate growth factors for several HDD markets to project security adoption in each of these markets and by aggregating these projections get a projection of security adoption growth for HDDs. High, median and low estimates for security adoption are based upon high, median and low estimates for total HDD shipments.

Separately we make projections for the growth of SED capable storage devices, arguing that once the demand for these devices in a given market exceeds some threshold value that all HDDs intended for that market will become SED capable devices within some reasonable period of time.

Although the available historical data for SED SSDs is less available we have created a model based upon analogy to the HDD model for both security adoption as well as SED capable storage devices. Note that due to the importance of crypto-erase for making data inaccessible on a SSD, we expect SED capable SSDs to become widespread more quickly than we project for HDDs.

**Technology Options for Data at Rest**

Self-encrypting hard disk drives were initially introduced by Seagate Technology in 2007. These initial products were called Full Disk Encryption (FDE) drives under the brand name DriveTrust. FDE drives were introduced by Seagate in advance of a SED standard from the Trusted Computing Group (TCG), a consortium of HDD, SDD, electronics, OEM, software and other interested companies whose Storage Working Group was tasked with creating universal standards for storage devices with internal hardware based encryption—often called Hardware (HW) Encryption. Storage devices with HW encryption, where the encryption key never leaves the storage devices and
where encryption and decryption of data are handled by the storage device electronics independently of the host, are called Self-Encrypting Drives or Devices (SEDs).

Hardware encryption is contrasted with Software (SW) encryption which runs the encryption software and accesses the encryption keys off of the storage devices. HW encryption runs entirely on the digital storage device and the encryption key never leaves the storage device.

All sorts of storage devices can be SEDs. The Trusted Computing Group has standards for internal encryption of hard disk drives, optical disc storage, as well as NAND flash storage devices such as Solid-State Drives (SSDs). It should be noted that popular magnetic tape standards also include encryption but this is independent of the TCG standards.

**Factors That Led to Slow Market Adoption of Self-Encrypted Storage Devices**

As will be shown in the following section the widespread adoption of SEDs has been rather gradual and far below earlier projections. There are various factors behind the slow market adoption of the technology in its early history; which include:

- higher costs/prices for initial SEDs,
- slow corporate IT spending due to economic disruptions and uncertainty in the last few years,
- lack of knowledge about the difference between HW based encrypted SEDs and SW encrypted solutions,
- lack of training of OEMs and integrators on the use and advantages of SEDs limits their growth
- issues limiting the use of encrypted drives in some countries,
- a limited initial market mainly driven by government mandates and,
- until recently, a lack of common standards and a continuing lack of product certification.

We will examine each of these factors.

The initial HDD SED products (in the 2007 and 2008 time frame) had a significant cost premium vs. similar drives that did not include internal encryption. OEMs indicate that the initial SED HDDs had a premium of about $100 vs. non-SED HDDs. This created an issue in take up of the initial products from Seagate. Today the premium that OEMs report is about $10 for an SED HDD compared to a non-SED HDD and it appears that this could be reduced to a much lower number with an additional growth in volume and
continued integration of encryption into the HDD controller chip (this is also becoming common for SSD controllers).

The economic slowdown in 2008 and 2009 impacted the purchase of enterprise storage systems and computers by many government and corporate users. That slowdown also impacted overall adoption of SED HDDs and HDDs in general during the last quarter of 2008 and through the first half of 2009. The higher costs of the SED HDDs, combined with economic uncertainty through 2010 also impacted the sales and adoption of SED HDDs. As in other aspects of the data storage industry, additional costs create a significant obstacle to wide-spread adoption of a new storage technology such as SEDs, particularly in a period of economic uncertainty.

While many larger IT departments know about the benefits of data encryption and the advantages of HW encryption vs. SW encryption, this awareness generally diminishes as the size of an organization declines. According to a recent survey of IT-savvy individuals from mostly larger organizations (only 9% had less than 500 employees) about 88% of the survey participants knew about SEDs. In the same survey only 14% had mostly HW encryption and 41% had a combination of SW and HW encryption in their facilities. Smaller organizations are less likely to have dedicated IT people and depend upon consultants and integrators to set up their IT operations, including encryption.

While larger IT houses appear to be relatively familiar with the need for encryption and the differences between HW and SW encryption, this is not the case with many system integrators and even OEMs who sell storage solutions to smaller organizations through consultants and their own sales channel. Until OEM representatives and system integrators are aware of and buy into the advantages of SEDs, it will be difficult for these products to grow in the smaller business and organization market. Since the number of companies in the USA with greater than 500 employees is only 0.8% of the number of all the companies with greater than 5 employees there is probably a large part of the market that doesn’t know much about the benefits of SEDs. Note that the total number of employees working for companies with less than 500 employees is almost the same as the total number of employees working for companies with greater than 500 employees.

Some countries limit the use of encryption in order to prevent individuals and companies from having private information. Such countries have been and will continue to be difficult markets for encrypted SEDs to find a foot-hold (at least, legally). This limits the potential growth of SEDs in some large markets (like China).
SEDs were initially championed by US government organizations, such as the NSA, and government regulations say that any US government IT equipment must meet NIST FIPS 140 certification, including storage devices and systems. That is why the largest percentage of sales up through 2010 for SEDs were to the US government and US government contractors that are subject to rules requiring them to use FIPS 140 certified devices and systems.

The second largest driver for SEDs to date is regulatory compliance. An SED that is lost or stolen without the password to access the SED encryption key is considered secure. Thus companies experiencing this loss don’t need to report a data breach and all the additional costs and bad public relations that such announcements create. Thus, laws such as Sarbanes-Oxley have helped drive the use of SEDs, particularly for corporate legal and financial data. However use outside of these applications has not been as widespread.

The original HDD SEDs introduced in 2007 were not compliant with any standard. Now that the Opal standard for client computer SEDs has been released by the Trusted Computing Group, SEDs should be interoperable and, in principal at least, should be capable of FIPS 140 certification. Unfortunately, only one SED vendor has FIPS 140 certification as yet and in general Opal SED certification does not yet exist. (Note that the Trusted Computing Group Storage Workgroup is currently working on a certification process). Lack of such certification is a barrier to more wide-spread SED deployment, since large system vendors and OEMs will feel more comfortable using SEDs in more applications once a solid certification program or programs are in place.

**Factors Favoring Future Growth of Self-Encrypted Storage Devices**

On the other hand there are various factors that favor the continued growth of SEDs, including:

- the approach to cost parity of SEDs to non-self-encrypting storage devices will make it easier to get these products adopted universally
- with SEDs there is no discernable encryption time like there is with SW encryption
- SEDs don’t have the performance overhead that SW encryption running on the host has, leading to better overall system performance
- SEDs may have a somewhat longer useful life than drives used in a software encrypted system, due to increased reads and writes with SW encryption
because the encryption key is stored on the storage device, it cannot be accessed through host hacking, like SW encryption can
- SEDs are less complex to implement in storage array encryption solutions
- government mandates and regulations are increasing the requirements for privacy and favor the use of SEDs, particularly those with FIPS 140 certification
- crypto-erase is the only effective way to make data on a SSD inaccessible

We will examine each of these growth factors.

Within the last year, the cost of adding SED functionality to HDDs has dropped to $10 or less (it started out in the $100 range). As in other markets, it is easier to sell a feature (especially one with an indirect ROI, like data security) if it is less expensive or ideally at no extra cost. The decrease in price combined with better education of at least larger IT groups has probably contributed to the significant increase (on a percentage basis) in the sales of SED HDDs in the last year. Larger production volume decreases the price further and it is expected that HDD encryption can be built into all HDD controllers and provide the capability at little or no additional cost to the HDD companies and thus their customers in the next few years. This would make HDD SEDs as common as SSD SEDs (which are likely to be 100% of SSDs within a couple of years, as discussed later).

Handling Stock Keeping Units (SKUs) of encrypted and non-encrypted HDDs has already created supply and inventory problems for OEMs. HDDs and other commodity microprocessor-containing electronic products have a long history of incorporating more and more functionality into the controller over time. It makes sense to do this with SED functionality. Incorporation of SED into the HDD controller eliminates the need (and cost) of an additional encryption chip (as has been the case in the past). We expect that unit volume increases, combined with inventory management, will drive HDDs to 100% SED built-in functionality within the next 3 years (similar to the 2 year projection for SSDs). As is also mentioned in the SSD SED adoption discussion, actual use of the SED encryption built into HDDs for data security is a different issue and will be addressed in the next section of this report.

Software encryption runs on the host processor rather than the storage device. This has implications on performance due to additional processor overhead in order to handle the encryption and decryption of data as well as the time it takes for initial encryption of a storage device. SW encryption performance penalties as high as 20-40% were reported by OEMs and storage device suppliers in the course of interviews leading to this report. In the Ponemon Survey in 2011, 53% of larger organization IT
participants indicted that SEDs would provide enhanced system performance because the encryption workload is moved off the host processor and onto the drive\(^3\).

In 2010, Trusted Strategies released a report comparing full disk encryption using a Seagate DriveTrust drive (an SED) vs. several popular software full disk encryption software\(^5\). The software packages that were tested and compared to the Seagate SED were McAfee Endpoint Encryption for PC, version 5.2.3; PGP Whole Disk Encryption for Windows, corporate desktop version, release 9.12; and Microsoft Bitlocker, Windows Vista Ultimate, SP2.

In the Trusted Strategies report the HW and SW encryption was tested using PCMark Vantage Professional edition mostly using the hard disk drive test suite. Identical 32 bit Dell Latitude E6400 laptops running Microsoft Windows Vista Ultimate, service pack 2, with Intel Core 2 Duo Processors and 2 GB of RAM were used for the comparison testing. The computers were re-imaged and restored for operating system and applications after every test to try and create common starting point for each test. Multiple tests of each encryption method were run and the optimum score for each product is given in Table 1 below. More details on the test and additional results are in the full report.

Table 1. HDD Encryption Throughput Test Results (extracted from 2010 Trusted Strategies Report\(^5\))

<table>
<thead>
<tr>
<th></th>
<th>No Encryption</th>
<th>Seagate SED HDD</th>
<th>SW Encryption Avg.</th>
<th>SW Encryption 1</th>
<th>SW Encryption 2</th>
<th>SW Encryption 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start-up Throughput (MB/s)</td>
<td>7.9</td>
<td>8.0</td>
<td>7.7</td>
<td>7.9</td>
<td>7.8</td>
<td>7.5</td>
</tr>
<tr>
<td>Application Loading (MB/s)</td>
<td>5.9</td>
<td>5.7</td>
<td>5.5</td>
<td>5.6</td>
<td>5.5</td>
<td>5.4</td>
</tr>
<tr>
<td>Modest Size File Test (MB/s)</td>
<td>5.4</td>
<td>5.3</td>
<td>5.1</td>
<td>5.1</td>
<td>5.2</td>
<td>5.1</td>
</tr>
<tr>
<td>Extensive Data Read (MB/s)</td>
<td>80.2</td>
<td>82.8</td>
<td>38.6</td>
<td>46.3</td>
<td>35.6</td>
<td>33.8</td>
</tr>
<tr>
<td>Extensive Data Write (MB/s)</td>
<td>50.7</td>
<td>50.3</td>
<td>35.2</td>
<td>39.1</td>
<td>31.4</td>
<td>34.9</td>
</tr>
</tbody>
</table>

Significantly faster throughput was seen for the HW encrypted SED vs the SW encryption products for extensive data reading and writing. From the table above the SED gave a 115% higher read throughput than the average of the SW encryption products and 43% higher write throughput.

Trusted Strategies did a follow on report looking at software vs. self-encrypted Samsung SSDs using a similar test set up as for the earlier HDD study. They also compared a
non-encrypted Samsung SSD vs an SED Samsung SSD\(^6\). Results from that report are give in Table 2 below.

There was no observable performance penalty for the SEDs, in fact they performed faster than the non-encrypted drives (for some reason). SED drives (as well as the non encrypted drives) had significantly higher performance than the SW encrypted SSDs.

SED storage devices have encryption built in so any data on the drive is automatically encrypted. In the case of initial deployment of SW encryption to encrypt a storage device, there can be a considerable time required for the initial encryption. For very high-capacity storage devices, the initial encryption time for SW encryption, can be a day or more. Thus, SEDs allow a quicker implement of an encrypted data solution than SW encryption. The lower performance overhead (and thus improved system performance) as well as elimination of any encryption time for a new storage device can offer considerable ROI advantages for SEDs (HW encryption) over SW encryption. These advantages would also scale from individual host systems to virtualization environments, making SEDs better storage devices for use in cloud storage environments where data security is important.

<table>
<thead>
<tr>
<th></th>
<th>Samsung SSD, No Encryption</th>
<th>Samsung SSD with SW Encryption</th>
<th>Samsung SED SSD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start-up Throughput (MB/s)</td>
<td>82.50</td>
<td>47.90</td>
<td>95.33</td>
</tr>
<tr>
<td>Application Loading (MB/s)</td>
<td>48.33</td>
<td>30.77</td>
<td>60.37</td>
</tr>
<tr>
<td>Modest Size File Test (MB/s)</td>
<td>41.13</td>
<td>26.77</td>
<td>50.40</td>
</tr>
<tr>
<td>Large Scale Data Read (MB/s)</td>
<td>178.00</td>
<td>70.23</td>
<td>169.33</td>
</tr>
<tr>
<td>Large Scale D Write (MB/s)</td>
<td>170.80</td>
<td>63.60</td>
<td>164.50</td>
</tr>
<tr>
<td>Random R/W (MB/s)</td>
<td>54.77</td>
<td>29.57</td>
<td>54.50</td>
</tr>
</tbody>
</table>

An additional related factor, although a secondary one, is that the additional write and read steps required for the initial encryption of a storage device using SW encryption and to some extent during actual use of SW-encrypted storage devices may lower the expected life expectancy of the storage devices. In my interviews with OEMs and suppliers, it was mentioned that a 10-15% loss in effective life of storage devices may be a result of SW encryption vs. SED HW encryption\(^8\).
In SEDs, the encryption key stays in a non-user accessible area in the storage device; it never leaves the drive. In the case of SW encryption, this is not the case. The encryption key will be in the host processor and memory while data is being accessed. This creates additional security vulnerabilities for SW encryption compared to HW encryption.

Since SED encryption is done within each drive, storage systems using many SED drives can include encryption with much less trouble than is the case for SW-based encryption. Thus, a storage array can do an escrow of drive security data, allowing access to each disk drive in the array without having access to the actual drive encryption keys. In addition, when drives are retired from storage systems (or for that matter, clients) they can be crypto-erased by erasing the key inside the SED to return the drive to a state where the drives can be reused by anyone without concern about access to the original data on the drive(s). This feature can be very important in virtualization environments where storage resources may have to be moved from client to client very quickly.

In addition, Opal standard enhancements will enable features such as secure bands of data in an SED drive. These bands could be quickly repurposed between customers in a virtualization environment by erasing the band encryption key.

The development of HW drive encryption has from its outset been promoted by agencies of the US government in order to provide more effective methods of protecting sensitive data. This has led to US government policies requiring digital technologies that can be certified to meet the security requirements of the 140 series Federal Information Processing Standards (FIPS 140, FIPS 140-2 is the latest version). The TCG SED standards were designed to create storage devices and systems that could meet these standards. The US government requires its IT encryption hardware and that of its contractors to use technologies that are FIPS-140-2 compliant.

As a consequence of its promotion of HW-based SED encryption that meet the FIPS-140-2 specification, government computer applications and those of government contractors have been the single biggest markets to date for SEDs. State and local governments also take their cues from the US government and so they also represent a significant part of the current USA SED market. In addition, US and European data privacy regulations favor the use of encrypted data in the commercial sector and thus represent another significant market for SEDs. These commercial uses have been concentrated in the storage of credit card and other financial data as well as medical and related data. To a large extent, the current market for SEDs has been created by government requirements and legislation.
Concerns with data privacy are expanding into other areas besides financial and medical information and it is likely that new regulations in North America, Europe, Japan and other countries will create a greater need for secure digital storage in the next few years. In addition to legal requirements, many organizations and individuals are becoming more conscious of their exposure to identity theft and other data privacy concerns. As a consequence, as knowledge of the ease of use of SEDs increases and their costs/prices decrease we should see a gradual increase in the adoption of SEDs for data security in the next few years.

HDDs can physically overwrite most prior data using built-in functions such as the security erase or sanitization functions built into HDDs with standard SATA or SAS command sets (as well as derivative FC HDDs). This is because there is a one-to-one correspondence between the logical mapping of data on a HDD and the physical location of the actual stored bits in the magnetic recording media.

In the case of a NAND flash-based storage device such as an SSD, wear-leveling and the consequent garbage collection do not allow for a one-to-one correspondence between the logical location of the data and the physical flash memory cells where the data may be stored. As a consequence, any attempt to physically overwrite data may not in fact erase old bits in reallocated cells. At the same time, SSDs and other flash devices are constantly moving data around and erasing de-allocated blocks of flash cells in the background so old and “erased” data may or may not be present in the flash memory device at any given point of time.

The ambiguity of the presence of old “deleted” data in a SSD leads to a security hole for SSD content. On the other hand, if the SSD or other flash memory device has a built-in encryption tightly coupled to the function of the flash memory controller (an SED SSD), then, if the internal encryption key on the SSD is erased, the data in no longer translatable from the ciphertext to data. This is called crypto-erase and it is very fast. Crypto-erase is very effective and it has been recognized by NIST and the government security standards as adequate for “secret” data. The 256-bit AES encryption currently used in both SED HDDs and SSDs is estimated to be beyond financially reasonable brute force decryption until after 2050.

Thus crypto-erase is the only really effective way to protect data on an SSD. As a consequence, many SSDs are now being built with SED encryption built into the controller function, making crypto-erase an increasingly common feature in modern SSDs. It is likely that all SSDs will have the encryption capabilities of SEDs within the next 2 years, making the basic SED capability available to all SSD users within a short period of time. Adoption and actual use of the SED encryption built into SSDs (or for
that matter HDDs) for data security is a different issue and will be addressed in a future section of this report.

**Some Additional Benefits with SEDs**

The non-user accessible area created to store the drive encryption key in an SED may also have other interesting uses for pre-OS boot application launches and storage of programs which cannot be damaged by viruses and other issues. These features have yet to be properly exploited but they may have enormous potential and could help drive the penetration of SED drives into the general market. These features have many positive uses and may also pose some dangers in certain situations.

If the size of the non-user accessible areas can be manipulated and used by system administrators, they could serve as a pre-boot area to store golden images of applications and special security credentials. Some companies are reported to be putting network management SW in the pre-boot area for use in tracking stolen storage hardware. Hypervisors and other useful SW could also potentially be run from the non-user accessible areas.

**Market Projection Methodology for Self-Encrypted HDDs and SSDs**

Based upon established demand for SEDs, it is unlikely that this technology will decline in market adoption. Therefore, we believe that there will be market growth over the next few years in units compliant to the TCG SED standards; the question is, how much growth and in what market segments and geographies.

In order to create a market projection, we need to look first at the expected overall growth in HDDs and SSDs unit shipments and determine what percentage of these will be used for drive encryption based security. We will do this by looking at the expected demand for drive encryption based security for different market segments for HDDs first and then SSDs. Based upon these estimates, we can create an aggregate estimate of HDDs and SSDs used for encryption based security.

In addition to creating an estimate and projection of drive based encryption use, we believe that at some point all HDDs and SSDs for given market segments will be created with SED functionality built in, whether or not the SED features are turned on or enabled for encryption based security. This will occur at some point for two reasons. First, trying to manage separate Stock Keeping Units (SKUs) of storage devices, some with the SED encryption and some without but otherwise identical products, becomes more difficult as demand grows for a special SED SKU.
Production and inventory control for manufactured storage devices is much simplified with a single SKU or at least if the hardware, including SED capability, is included with each HDD or SSD is common and the only difference between the SKUs is whether the SED capability is turned on to use for encryption based security. This approach may be a way to make a common SED-capable drive for an entire market and to create a special SKU that does not let the self-encryption functionality to be used in the field for encryption based security, in order to sell these products into markets such as China.

Second, as the volume of encryption based security using SEDs increases, the costs will go down and there will be additional pressure to include encryption within the storage device System on Chip (SoC) processor. This has been a common evolution of functions on storage devices over time, a feature initially enabled using a separate IC gets bundled with the device SoC controller. Since all drives use an SoC, the overall additional cost of including SED functionality in the drive is significantly reduced or eliminated (depending upon licensing terms for the encryption solution).

We estimate that it will be easier to include SED capability in all HDDs or SSDs for a given market segment, whether or not it is enabled or used by the customer for encryption based security, when the total demand for encryption based security for that segment is in the range of 10-20% of the total market. We will use a threshold value of 15% for the onset of very rapid adoption of SED functionality in a drive family (for most markets) independent of the use of encryption based security.

Thus, in the market projections given in this report we will make two types of projections for given market segments and for HDDs and SSDs as a whole. The first projection will be for the growth of SED- encryption-based security in terms of drive units. The second projection will be for the adoption of SED capability in drives for that market segment in terms of drive units. We call these two projections Security and SED adoption respectively.

The actual modeling methodology will assume that Security adoption (the use of SED drives for encryption based security) will follow an S-shaped adoption curve. Because of some intrinsic adoption issues for encryption-based security in some geographic regions, the maximum security adoption will not be 100% of all the drives produced.

We will use a common product growth estimate model based upon a derivative of the Bass model of technology diffusion9. In particular, we will use an equation for the cumulative fraction of adopters at time t, F(t), where p is the so-called innovation factor and q is the imitation factor. The equation for F(t) is given below10:
We will try to find values of \( p \) and \( q \) that allow us to approximately match the available historical data for SED sales. These values will then be used to create a projection of the adoption of SED based security for given markets. In the year where it looks like the SED security demand exceeds our arbitrary threshold of 15% of all the drives for that market segment, we project that there will be a rapid transition to making all the segment drives SED capable. This transition would be expected to occur over 1.5 years at a roughly exponential rate. 1.5 years is estimated to be the time for ramp of encryption in the controller and related hardware and firmware and introduction into all products in the market segment.

**Market Projections for Self-Encrypted HDDs**

Coughlin Associates estimates for high, median and low HDD shipments are shown in Figure 1 for historical data from 2001 through 2010 and projecting out to 2016. This is the total target population of disk drives for the projection period and the median model predicts that HDD shipments will exceed 1 B units by 2014.

![Figure 1. Banded Hard Drive Volume Projections](image)
Figure 2 shows median projections of HDDs shipped for various market niches. In particular we will focus on laptop and enterprise HDDs in our initial HDD Security adoption analysis.

**Figure 2. Projection of Drives by Market Niches (in 1,000’s of units)**

In February 2011, Seagate announced that it had shipped more than 1 M self-encrypting HDDs into the laptop and enterprise markets. Seagate introduced their laptop SEDs in 2007 and their enterprise SEDs in 2009. Other companies that have shipped SEDs include Hitachi (announced in 2007) and Fujitsu (announced in 2008, note that Fujitsu’s hard disk division is now part of Toshiba). Hitachi also announced 3.5-inch SED HDDs for desktop PCs in 2008. Toshiba announced and SED HDD and Samsung announced an SED SSD respectively in 2011. Western Digital has not announced shipping SED drives as of the date of this report. By the end of 2010, we estimate that a total of about 1.2 M SED HDDs shipped, mostly for laptop and some for desktop and enterprise applications.

Figure 3 shows our projections for **security adoption** using laptop (mobile) SED HDDs. Note in our earlier discussion we made the distinction that not all SEDs will actually be used for secure data protection of user data for various reasons, the capability is in the drive but it may not be turned on or used. Security adoption is our projection of the use of SEDs intended to be used for data security. For the laptop model p=0.00005 and q = 1.1. The high, median and low estimates in this figure are...
calculated from the high, median and low HDD models like those shown in Figure 1 (for the laptop market segment).

**Figure 3. Security Adoption for Laptop HDDs**

![Graph showing security adoption for laptop HDDs over years 2007 to 2016.](image)

**Figure 4** gives our projections for **security adoption** for enterprise HDDs. These include both traditional high performance enterprise drives as well as SATA drives used for enterprise applications (such as in drive arrays). For the laptop model $p=0.00003$ and $q = 1.35$. The high, median and low estimates in this figure are calculated from the high, median and low HDD models like those shown in Figure 1 (for the enterprise market segment).

**Figure 5** gives our projections for **security adoption** for desktop HDDs. For the desktop model $p=0.00003$ and $q = 1.15$. The high, median and low estimates in this figure are calculated from the high, median and low HDD models like those shown in Figure 1 (for the desktop market segment). Note that demand for desktop security adoption is slower than for laptop computers as would be expected since desktop computers aren't as liable to be lost or stolen as laptop computers are.
Figure 4. Security Adoption for Enterprise HDDs

Figure 5. Security Adoption for Desktop HDDs
Figure 6 gives our projections for security adoption for consumer electronics HDDs. We assume that consumer electronic HDDs will not experience nearly the demand for encryption as computer and enterprise drives. In fact, in our model we assume that the q parameter is about half of that for desktop HDDs. For CE HDDs p = 0.00003 and q = 0.7. The high, median and low estimates in this figure are calculated from the high, median and low HDD models like those shown in Figure 1 (for the consumer electronics market segment).

Figure 6. Security Adoption for Consumer Electronics HDDs

![Security Adoption for Consumer Electronics HDDs](image_url)

Figure 7 summarizes the median results from Figures 3-6 in one chart. This chart has a log scale on the vertical axis so the smaller unit trends between 2007 and 2012 are visible. By 2016 this median model shows a total of 315 M security adoption SED HDDs shipping annually. It is clear that laptop units vastly outnumber other market segments.

Figure 8 shows the resulting high, median and low estimates for security adoption SED HDDs. Note that these estimates show that by 2016 the high could be as many as 411 M security adoption SED HDDs while the low could be as low as 182 M security adoption SED HDDs.
Figure 7. Median Security Adoption for all HDDs Market Segments

Note that using the 15% security adoption criteria as the threshold where all the drives in that market segment would shift to SED capable units (although not necessarily turned on or used for data security purposes). We see that this threshold is reached in 2014 for laptop and enterprise HDDs and in 2016 for desktop computer HDDs. CE HDDs never reach that level of demand and so they would likely only shift to 100% SED capable if there is no economic cost and if doing so simplified the overall production of HDDs—which is likely if all other HDDs shift to SED capable units.

Thus, it is likely that by about 2017 all HDDs will shift to SED capable units, although estimated security adoption units by 2016 (SED capable HDDs actually used or intended for data security) are only 25% of all HDDs shipped.

Factors that could accelerate security adoption and SED capability in HDDs:

- if HDD controller makers move to incorporate SED capability into standard HDDs the shift to SED capable units could happen much quicker than this. If this happened it would also be part of a significant cost reduction for SEDs and would probably accelerate security adoption with SEDs as well.
- increased publicity to susceptible mid-market users, especially with increasing amounts of government privacy regulation could increase security adoption.
Market Projections for Self-Encrypting SSDs

Although market numbers for SED HDDs have been announced by some companies, there is less public information on SED SSDs. At least one major SSD company, Samsung, announced SED SSDs starting 2009 and major controller companies such as SandForce are incorporating SED capability into all SSD controllers. We have an expectation that incorporating SED capability into SSDs will become commonplace for many market segments and likely will become universal before this happens in HDDs.

There are two reasons why SED capability (whether it is needed or used by customers for data protection and security) is likely to become commonplace in SSDs. The first reason is that SSDs by their very architecture do not provide ways to effectively erase all the content in the device, unlike HDDs. Providing encrypted data on the SSD where the key is within the device allows erasing the encryption key and making the data unavailable to others—a crypto-erase. This feature will be popular for many users even if they don’t use the SED features on a day to day basis, since drives can be reused without fear that the data is available to a new user after the internal encryption key is erased.

The second reason is that, with relatively lower volumes and a great many SSD suppliers having SED capability, that capability is both easier to implement in controllers...
and propagate in the industry and at the same time a distinguishing product feature for those that have it and a potential negative purchase factor for those SSDs that don’t include it. This is because, by incorporating SED capability in controllers, customers don’t pay extra for the security features. This makes SED SSDs more attractive to customers even if they have no active plans to use the security features.

*Thus we project that within 2 years (by 2013) SED capability will be in over 80% of SSDs and likely in almost all SSDs within 3 years (2014).*

Regarding actual *security adoption* in SSDs, we must make some guesses and assumptions for particular markets where these features would be attractive. Figure 9 shows projections for SSD for various applications out to 2015. Objective Analysis estimated about 49 M SSDs shipped in 2011, rising to about 106 M units by 2015. If we take the Objective Analysis data, extrapolate to 2016 for the median shipments and apply rules for higher and lower SSD estimates similar to those for HDDs we get the chart shown in Figure 10.

*Figure 9. SSD Annual Shipped Unit Projections*¹²

![SSD Annual Shipped Unit Projections](image)

The markets where we would expect the greatest interest in SED SSDs include
Financial and POS, Servers, Notebook PCs, Desktop PCs, Military and Aerospace and NAS and SAN. Altogether these account for over 90% of all SSDs.

**Figure 10. High/median/low SSD Estimates**

Since we have no historical data for SED SSDs for any of these segments, we will use the p and q values from the HDD laptop adoption model ($p = 0.00005$, $q = 1.1$), extrapolate the SSD data out to 2016 and only consider adoption in the SSD markets that we have identified as most likely to find data protection security of interest. **Figure 11** gives our model of SED SSD *security adoption* (actual use of SED security features). High, media and low estimates are made for these based upon the projections in Figure 10. Although actual SSD SED feature implementation in 2016 is likely to be about 100% in about 122 M SSDs, the projected actual SSDs from that year used for security and data protection purposes is estimated at less than 18 M units (these are mean values only).
Summary

Following is a summary of the major conclusions of this report.

Various factors behind the slow market adoption of the technology in its early history:

- higher costs/prices for initial SEDs,
- slow corporate IT spending due to economic disruptions and uncertainty in the last few years,
- lack of knowledge about the difference between HW based encrypted SEDs and SW encrypted solutions,
- lack of training of OEMs and integrators on the use and advantages of SEDs limits their growth
- issues limiting the use of encrypted drives in some countries,
- a limited initial market mainly driven by government mandates and,
- until recently, a lack of common standards and a continuing lack of product certification.

Various factors that favor the continued growth of SEDs:
• the approach to cost parity of SEDs to non-self-encrypting storage devices will make it easier to get these products adopted universally
• with SEDs there is no discernable encryption time like there is with SW encryption
• SEDs don’t have the performance overhead that SW encryption running on the host has, leading to better overall system performance
• SEDs may have a somewhat longer useful life than drives used in a software encrypted system, due to increased reads and writes with SW encryption
• because the encryption key is stored on the storage device, it cannot be accessed through host hacking, like SW encryption can
• SEDs are less complex to implement in storage array encryption solutions
• government mandates and regulations are increasing the requirements for privacy and favor the use of SEDs, particularly those with FIPS 140 certification
• crypto-erase is the only effective way to make data on a SSD inaccessible

The major conclusions of this analysis are:

• **It is likely that by about 2017 all HDDs will shift to SED capable units, although estimated security adoption units by 2016 (SED capable HDDs actually used or intended for data security) are only 25% of all HDDs shipped.**

• **By 2016 the high, median and low estimates for security adoption for SED HDDs are 411 M, 315 M and 122 M units.**

• **We project that within 2 years (by 2013) SED capability will be in over 80% of SSDs and likely in almost all SSDs within 3 years (2014).**

• **Although actual SSD SED feature implementation in 2016 is likely to 100% in about 122 M SSDs, the projected actual SSDs from that year used for security and data protection purposes is estimated at less than 18 M units.**

**Appendix: A Discussion of Growth Modeling**

This appendix is extracted from part one of a two part article. This piece appeared in the July 2011 issue of the *Digital Storage Technology Newsletter*. The full article contains material drawn from Stephen J. Daniel’s book, *Understanding the Future, A Practical Guide to Designing and Developing Context Specific Segmented Forecasts and Models For Technology Markets.*
The individuals in the population receive the information from an external source simultaneously at a single point in time, or over a period of time. However, the individuals differ as to the susceptibility to change. Some change instantly while others delay the change, and still other do not ever change, sometimes terminating the process before 100% penetration. The change process is therefore dependent on these additional attributes that vary across the population and govern the susceptibility to change. Both the growth process and the termination process are dependent on the distribution of the resistance attributes in the population. The observed data from this classification will best fit a logistics curve since the individuals’ attributes will act as resistance to change and therefore slow the growth process as shown in Figure 12.

Figure 12. External Resistance Model Growth Curve

A clear example of this is the way kernels of corn pop as heat is applied. If all the corn kernels were physically identical, they would all pop simultaneously. However, the kernels are not physically identical, they differ in size and starch content. Since these differ over the population, the rate at which the kernels pop will vary over time. It is important to note that whether or not a kernel pops is totally independent of what any other kernel does. The percentage of kernels that have popped over time will create an “S” shaped logistic curve that is entirely caused by the heterogeneity of the kernels in terms of starch content.
An external marketing message may be considered analogous to the heat and the kernels analogous to potential customers. If the chance that a customer buys the product is dependent on some decision influencing factor, and that factor is distributed heterogeneously throughout the population, then that factor will act as a resistance force to the growth process and produce an “S” shaped logistics curve.

A single or small group of individuals changes and then communicates information to its neighbors that may trigger their change. However, the susceptibility to change in each unit varies across the population therefore only some of the units that receive the information will change. This is identical to the resistance model. The only difference is that information is communicated internally from individual to individual rather than from an external source.

While the growth process is driven by the rate at which the information propagates through the populations it is increasingly countered by the resistance factor in the remain unchanged portion of the population. In some case, growth may even stop prior to reaching 100% of the population. The observed data from this classification will best fit a logistics curve.

From the above classification examples, it should be clear that if the population is homogeneous then the penetration rate, i.e. the rate of adoption, is simply the information propagation rate. If the communication process is internal than the process will be best modeled with exponential, growth, or power functions. If the communication process is external then a power or logarithmic function will provide the best model.

However, if the population is heterogeneous then regardless of the communication process penetration will follow a logistics curve.

As time progresses the remaining unchanged population will contain an increasing proportion of individuals that are less likely to change. This implies that in heterogeneous populations factors are present that exert a counter force, a resistance to the process driving change, and that these also increases in strength over time. It is the heterogeneity in the population that creates the counter force to the communications driven growth process, and therefore the “S” shaped logistics pattern such as shown in Figure 13.
Figure 13. Internal Social Model Growth Curve

- Logistics
- Internal Communication of Information within a Heterogeneous Population
- Individual Resistance

Copyright © 2010 Daniel Research Group. All rights reserved.
About the Author:

Tom Coughlin, President, Coughlin Associates is a widely respected storage analyst and consultant. He has over 30 years in the data storage industry with multiple engineering and management positions at high profile companies.

Dr. Coughlin has many publications and six patents to his credit. Tom is also the author of Digital Storage in Consumer Electronics: The Essential Guide, which was published by Newnes Press. Coughlin Associates provides market and technology analysis (including reports on several digital storage technologies and applications and a newsletter) as well as Data Storage Technical Consulting services. Tom is publishes a Digital Storage in Consumer Electronics Report, a Media and Entertainment Storage Report, and a Capital Equipment and Technology Report for the Hard Disk Drive Industry.

Tom is active with SMPTE, SNIA, IDEMA, the IEEE Magnetics Society, IEEE CE Society, and other professional organizations. Tom is the founder and organizer of the Annual Storage Visions Conference (www.storagevisions.com), a partner to the International Consumer Electronics Show, as well as the Creative Storage Conference (www.creativestorage.org). He is also a Senior member of the IEEE, Leader in the Gerson Lehrman Group Councils of Advisors and a member of the Consultants Network of Silicon Valley (CNSV). For more information on Tom Coughlin and his publications go to www.tomcoughlin.com.

Sources and References

1 Trusted Platform Module (TPM): Adoption Dynamics, IDC, 2006
2 Trusted Computing is Real and it’s Here, Endpoint Technologies Associates, 2007
3 Perceptions about Self-Encrypting Drives: A Study of IT Partitioners, Ponemon Institute, 2011.
7 Reliably Erasing data from Flash-Based Solid State Drives, M. Wei et. al, Presented at Fast 2011
8 Based upon discussions with encryption and SED experts during the course of this research
13 Solid State Drives: Outlook 2010, Objective Analysis, 2010