# Comply with Data Protection Laws and Regulations

*Using the Seagate Momentus FDE.2 Hard Drive and the Wave Systems EMBASSY® Trust Suite Solution to Comply with Legal and Industry Standards*

***W. Scott Blackmer***
*Technology Law and Consulting*



**October 2007**
**www.wave.com**

## Abstract

This White Paper, prepared for Wave Systems Corp. and Seagate LLC, demonstrates how the use of hardware-based **full disk encryption** (FDE), especially paired with **secure authentication** and **remote administration** tools, can help organizations satisfy information security compliance requirements and avoid liability arising from lost or stolen laptops.[1]

## Executive Summary

### Laptop Risks

The lost or stolen laptop (or other portable drive) represents a growing threat to an organization's reputation, compliance and litigation risk management, as illustrated by the long list of recent laptop security incidents in **Appendix A**. Laws, regulations, and judicial precedents holding the enterprise accountable for the exposure of sensitive data are proliferating. They include:

- SOX, E-SOX, J-SOX and similar laws and rules requiring internal controls over information management and information security in public companies.
- GLBA financial privacy rules and financial services regulations in the United States and other industrialized nations.
- HIPAA medical privacy rules.
- Liability under fair trade practices acts and in negligence and contract cases.
- State laws and proposed federal laws in the United States, and similar proposals in Canada and Europe, on personal information security standards, security breach notice, and data disposal, all largely driven by the rise in identity theft.
- Comprehensive data protection laws in Europe, Canada, Japan, and other jurisdictions.
- Reference to information security standards such as ISO, ITIL, NIST, and PCI DSS in contracts, enforcement actions, and negligence cases.

[1] This white paper was prepared by a technology lawyer whose practice emphasizes information privacy and security. The paper is intended to provide general information concerning relevant compliance and risk management issues for enterprise information management. It is not intended as legal advice for any organization's specific circumstances.

Experience suggests that no amount of training will assure that sensitive data are consistently protected by policies against downloading or user-controlled encryption on portable devices. On the other hand, the combination of full-disk encryption and drive management software, providing secure authentication and remote administration, overcomes this vulnerability and allows the enterprise to centrally manage security on the laptop.

There are many sources of general legal requirements to employ "reasonable" security measures to protect sensitive data, a dynamic standard that only gets tougher over time. But there is also a discernable trend toward specifying encryption, authentication, and related measures, especially when the data are stored on an inherently less secure, mobile device; such as a laptop computer. Some prominent examples:

- In the United States, the President's Identity Theft Task Force, the Office of Management and Budget, the Department of Homeland Security, and the National Institute for Standards and Technology have all issued guidance to the effect that sensitive data on laptops should routinely be encrypted, mandating this practice for government laptops and recommending it for the private sector.
- California and more than 30 other states have enacted security breach notice laws and related requirements that generally apply only to the loss or theft of certain categories of unencrypted personal data. The European Union, Canada, and New Zealand are also considering mandatory breach notice requirements.
- The major payment credit and debit card networks now contractually require encryption (with few exceptions) and authentication controls by banks and retailers storing payment card details.
- The UK Information Commissioner recently threatened enforcement action against organizations that allow personal data to be taken away on laptops without "strong encryption."
- Spain now requires encryption for sensitive categories of personal information, as do Italy and Switzerland for certain kinds of data.

**Product Requirements**

As detailed below, laws, standards, and recommendations concerning information security encourage an enterprise to conduct risk assessments and adopt appropriate, documented control measures, as well as procedures for responding to security incidents. Several of the commonly mandated or recommended control and response measures are particularly relevant to managing laptop risks, with implications for product selection and configuration:

- ***Encryption***. Enterprises are typically encouraged (and sometimes required) to protect certain categories of data with effective encryption methods, and to protect the decryption keys themselves. Laws on information security and security breach notice offer no "safe harbor" for encryption techniques that the enterprise cannot reasonably rely on, and some expressly require breach notice to regulators or affected individuals if there is reason to believe that the decryption key was compromised.
- ***Automatic vs. optional encryption***. A classic problem in lost and stolen laptop incidents is that the laptop user did not use available encryption tools, or the user is uncertain whether he/she did so with respect to all of the data on the laptop. Policies do not ensure compliance, and uncertainty can trigger legal breach notice requirements even without evidence of theft or injury. Techniques for forcing file or disk encryption are the surest means of establishing that laptop data are in fact encrypted.
- ***Access controls***. Access controls, including identity management, access policies based on rules and roles, and log-on authentication techniques, are nearly universal features of information security requirements and procedures. They typically apply to remote network access, but enterprises increasingly see a need to apply access controls to the remote device as well, because sensitive information is stored on the laptop, as well as the network.

- ***Remote administration of access controls***. Compared to the constantly connected desktop terminal, the laptop presents unique challenges for network administrators seeking to modify or revoke a user's access permissions and authentication credentials. One solution is to use remote administration tools that allow the administrator to do so whenever the laptop connects to the enterprise network.

- ***Remote data destruction***. Once sensitive data are no longer needed, they should be destroyed to reduce security risks. This principle appears in many of the relevant laws and standards. And, if the data are at risk on a lost or stolen laptop, or a laptop controlled by a user no longer trusted with such data, a potent defensive measure is the ability to "wipe" the data when the laptop next connects to the enterprise network.

- ***Audit log and monitoring for suspicious activity***. Remote administration tools, including an audit log of events, allow an enterprise to track network access by a laptop user. These tools can also track significant changes to the laptop itself that might indicate it is no longer in the hands of a trusted user, making it possible for the enterprise to investigate and, if necessary, take defensive measures such as, remotely destroying data on the laptop and denying further network access. The audit log also establishes proof that the laptop drive was in fact encrypted. This can be critical in determining whether it is likely that sensitive data were compromised because of a lost, stolen, or hacked laptop and whether officials, business partners, or affected individuals must be notified of the security breach.

In short, enterprises should take laptop risks into account when choosing laptop hardware and software and related access and remote administration controls. Where protected or risky data may reside on the laptop, the enterprise should consider deploying products that offer the functionality described above. Appendix B maps these product requirements to leading information security laws, standards, and recommendations.

**Seagate / Wave Solutions**

Seagate's Momentus 5400 FDE.2 Trusted Drive, combined with Wave's EMBASSY Trusted Drive Manager and EMBASSY Remote Administration Server (ERAS), protects data on laptops with each of the functions mentioned above, offering automatic full-disk encryption, secure authentication, and remote administration features.

With this combination of products, data are automatically and reliably encrypted. The user is authenticated, independently of the operating system, before accessing data on the hard drive itself. This means that data are protected even on a lost or stolen laptop. The network administrator remotely updates, modifies, and, if necessary, revokes access privileges and authentication credentials. The central network monitors the laptop for suspicious activity and creates an audit log for investigative and forensic purposes. The remote administrator can even wipe data from the laptop on connection to the network.

Each of these functions is described more fully below. Most importantly, they prove that Seagate's FDE drives and Wave's Trusted Drive Manager and ERAS applications offer real protection for data residing on laptops and satisfy today's legal requirements and information security standards. Further, they allow enterprises to anticipate the trend toward assuring encryption and control of all protected data on laptops, wherever located. This is clearly the safest way for enterprises to avoid laptop-related loss and liability.

## Introduction

Information management is critical to the modern enterprise. The loss or alteration of certain data, or its exposure to unauthorized persons, can damage the enterprise and, in many cases, other organizations or individuals, as well. Such sensitive data may include, for example:

- Confidential commercial information and trade secrets of the enterprise (business plans, research and development data, transaction records, personnel administration, etc.).
- Third-party confidential material provided by the enterprise's clients or business associates under nondisclosure agreements (NDAs).
- Protected personal information (such as payment card and bank account details, social security numbers and other official identifiers, health records, and information about children).
- Legally privileged communications.
- Insider information that could affect stock prices or planned mergers and acquisitions.
- Authentication credentials that could give a thief access to the enterprise's physical or network facilities.
- Information that could compromise national security interests or endanger critical infrastructure.

All of these kinds of sensitive information require appropriate security measures to protect both the enterprise itself and third parties. Increasingly, laws and regulations mandate such safeguards, although the precise rules vary by sector and jurisdiction. Some of the more influential laws and regulations are summarized below.

Further, in the event of security breaches that affect third parties, enterprises may be obliged to establish that they exercised **reasonable care**, based on legal and industry standards, to defend themselves against claims of **negligence, breach of contract,** or **unfair or deceptive trade practices**. Where technical safeguards such as encryption are readily available, it may be very hard following a security breach to argue plausibly to shareholders, regulators, and litigants that the organization acted reasonably in storing large amounts of sensitive data on portable devices without encryption and other appropriate controls.

Both to protect their own operations and to avoid causing injury to others, organizations spend millions securing their data centers and networks from hacking, malware, and other threats to sensitive data. Often, however, the point of greatest vulnerability is the humble but ubiquitous (and highly mobile) **laptop computer**, particularly in the hands of a careless – or, more rarely, ill-intentioned – employee. This is why solutions based on full disk encryption (FDE), especially combined with remote administration capabilities, can play an important role in an organization's security plan and, the worst possibility, in mounting a legal defense and protecting the organization's reputation.

This paper summarizes: first, the nature of the risk; second, the relevant legal standards for compliance, reasonable care, and proof; and, third, the extent to which full disk encryption and remote administration products can serve to meet those standards.

## Hard Drives at Risk

Mainframes, servers, desktops and work stations, point-of-sale terminals, storage media, handheld computers, and smart phones each present their own security risks. Disk encryption is an effective tool to secure data on many of these devices. In computing, one consequence of the "laptop revolution" is that the laptop computer has become a particular hazard to protected data held by an enterprise, being unable to be controlled solely by firewalls and network access protocols.

Employees use laptops at work, as well as take them home. Laptops are left in cars and hotel rooms, routinely carried on airplanes and into offices, conference rooms, restaurants, and public restrooms.

In addition to their employees, the enterprise makes sensitive data available to contractors, temporary workers, auditors, consultants, and business partners. Like employees, some of these users download and carry with them large amounts of the same data that the enterprise takes great care to secure on its own premises.
Inevitably, some of these laptops and other portable hard drives are lost, stolen, or inadvertently left behind, ready for someone else to pick up. Some are hacked into without their owners realizing it.

Many enterprises train their staff in laptop security and establish policies against downloading large amounts of sensitive data, but the practice still occurs. Firing the careless worker is an inadequate remedy once the damage has been done. And an employee with a grudge – or a criminal agenda – can cause a great deal of harm with nothing more than a company laptop, both before and after his network privileges have been revoked.

Senior executives are not immune to the hazards of inadequately protected data on a laptop. In a memorable incident in September 2000, Qualcomm's CEO left his laptop on the podium for a few minutes after giving a presentation to the Society of American Business Editors and Writers. When he returned, the laptop was gone. Witnesses report that the CEO was especially distraught because he said his laptop contained unencrypted files concerning sensitive negotiations with Chinese telecommunications companies, which could be of considerable interest to competitors and foreign governments.

As a result of profligate downloading and inadequate protection of data on laptops and portable hard drives, such security breaches are all too common. **Gartner Group** estimated in 2002 that **the chances of a business laptop being stolen were one in ten**. The **US Federal Bureau of Investigation** reckons that **97% of stolen laptops are never recovered** by the owner.

Professional groups such as the **Computer Security Institute** have conducted surveys on the frequency of laptop theft since at least 1998, and the trend is not improving. The **IT Policy Compliance Group** recently reported that 68% of surveyed companies say that they experience data theft at least six times each year; 20% say they experience more than 21 incidents annually (see eweek.com, www.eweek.com/article2/0%2C1895%2C2101683%2C00.asp, March 7, 2007). According to the report, the most frequently cited cause of security breaches is lost or stolen laptops and other mobile devices, combined with the user's failure to follow the organization's security policies for downloading and securing sensitive company or consumer data. Where customer data was compromised, the survey responses indicated that the cost of notice and rectification averaged $100 per record.

Similarly, a 2007 survey of more than 700 executives conducted by the **Ponemon Institute**, "The Business Impact of Data Breach," revealed that 85% of respondents had experienced a data breach incident. One of the most frequently cited causes was a stolen laptop. (See article published by PC World, May 16, 2007, available online at www.pcworld.com/article/id,131884-c,privacysecurity/article.html).

A 2007 study of security breaches by **University of Washington** researchers, analyzing incidents reported in the media since 1980, concludes that electronic records in the United States are now lost or stolen at the rate of 6 million per month, a number that has risen since 2006. Only a third of the reported incidents involved hacking, while the researchers attributed 60% to "organizational mismanagement," prominently including unencrypted data on stolen equipment. (See article published by Network World, March 13, 2007, available online at www.networkworld.com/news/2007/031307-data-breach-companies.html.)

The P**rivacy Rights Clearinghouse** maintains an online chronology of reported data breaches involving sensitive personal data (such as Social Security numbers and financial account or payment card numbers) concerning consumers, employees, students, or medical patients (see www.privacyrights.org/ar/ChronDataBreaches.htm). Many such security breaches have become public knowledge since January 2005, when California's Security Breach Notification Law, **SB 1386**, came into effect. (Most states now have similar legislation, as outlined below.) The Privacy Rights Clearinghouse lists over 500 reported incidents since January 2005, involving records on more than 155 million individuals. A similar list, the "**Non-Encrypted Hall of Shame**," is maintained on the website of

**Network Information Security & Technology News** at www.nist.org/nist_plugins/content/content.php?content.54. There is growing public concern about security breaches involving personal data, particularly because identity theft (leading to several kinds of fraud) is the fastest-growing crime in America, according to the United States Department of Justice. The Federal Trade Commission (FTC) estimates that some 9 million Americans are the victims of **identity theft** each year (see http://ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html). The FTC and the Identity Theft Resource Center estimate the annual cost to consumers at $5 billion (and an average 600 hours required to deal with the consequences of having one's identity assumed), while business direct costs are estimated at $47.6 billion. Stolen bank account or payment card details, social security numbers and other identifiers are auctioned in chat rooms and on computer bulletin boards and "floating" websites, or exchanged on USB drives for cash, drugs, and other contraband. Not surprisingly, legislators, courts, and the public increasingly call for greater care and accountability on the part of enterprises that store the kinds of personal data most frequently used in identity theft.

In February 2007, the **California Office of Privacy Protection** published a report based on its own study of a sample of reported security breaches, "Recommended Practices on Notice of Security Breach Involving Personal Information" (http://www.privacy.ca.gov/recommendations/secbreach.pdf). The report draws the following conclusion:

> "One lesson is made clear by the significant share of breaches resulting from lost or stolen laptops and other portable devices, about 53% of the Office's sample. Organizations have begun to pay more attention to protecting personal information on portable devices. Some organizations are doing this by using **encryption**. Others have adopted new procedures to safeguard the information, such as cabling PCs to desks, not allowing the downloading of Social Security numbers from mainframes onto PCs or laptops, and tightly restricting the number of people who are permitted to carry sensitive personal information on portable devices." (Emphasis added.)

Publicized security breaches illustrate the scope of the problem with unencrypted laptops and portable hard drives. These incidents involve a wide range of reputable corporations, government agencies, universities, hospitals and other organizations. Presumably, most, if not all, of these organizations maintain information security policies and an extensive central information security infrastructure. Despite this, unencrypted sensitive data has been compromised – repeatedly, in some cases. The larger cases typically required **reporting to directors and shareholders, as well as to law enforcement and regulatory bodies**. In most of the incidents, the enterprise held one or more press conferences and was obliged to send mass mailings on short notice, set up special **websites and hotlines** to disseminate information and answer questions, and train call center personnel to field, in some cases, thousands of calls daily from anxious individuals over a period of weeks.

In several cases, the organization was targeted in **lawsuits and federal or state investigations**. In some of these cases, the organization was fined, subjected to consent orders to implement security changes or required to reimburse the costs of a government investigation. Even though most of these data security breaches never resulted in known cases of fraud or identity theft, they nevertheless damaged the reputation (and often the share value) of the organization concerned, as well as imposing substantial costs and burdens on both the organization and affected third parties. The number of unbudgeted hours required of IT and legal departments, customer and public relations and human resources is typically not quantified but is surely substantial. The Computing Technology Industry Association (CompTIA), which conducts an annual survey of IT professionals, reported that more than a third of its respondents indicated that their organization had suffered a "major security breach" in 2006, and the consequences of such breaches were more severe than reported in prior years, averaging some $370,000 per incident. See Network World, "Security breach severity worsens, study finds" (Sep. 18, 2007) (available online at www.networkworld.com/news/2007/091807-security-breach-severity.html?page=2).

What follows are some examples of significant data security breaches involving lost or stolen hard drives, drawn from media and government reports. The sheer volume of such incidents is sobering.

- University of California (Berkeley) (personal data on 98,400 students and alumni on a laptop stolen from an employee, March 2005.)
- US Department of Justice (80,000 individuals' records on a stolen laptop, May 2005.)
- Bank of America (18,000 records on a stolen laptop in June 2005; an undisclosed number of debit card details on another stolen laptop, September 2005; more customer records compromised by a stolen laptop in April 2007.)
- Boeing (161,000 employee records on a stolen laptop, later recovered, November 2005; 3600 employee records on another stolen laptop, April 2006; records on 382,000 current and former employees on yet another stolen laptop, later recovered, December 2006.)
- Fidelity (Retirement fund data on 196,000 current and former HP and Compaq employees on a stolen laptop, March 2006.)
- US Marine Corps (stolen portable drive with personal data on 207,750 individuals, March 2006.)
- Ernst & Young UK reported a laptop stolen from a car with data on 38,000 employees of BP, IBM, Sun, Nokia and Cisco (March 2006.)
- Hummingbird (Toronto, Canada), a contractor for the Texas Guaranteed Student Loan Corp., reported that **1.7 million** borrowers' records were stored on a lost hard drive (May 2006.)

(For a complete list of examples of significant data security breaches involving lost or stolen hard drives, drawn from media and government reports, please see **Appendix A** at http://www.wave.com/about/whitepapers/FDE-Compliance-AppendixA.pdf)

The problem is not limited to the United States, as some of the examples above from the UK and Canada demonstrate. British businesses surveyed by silicon.com in May 2007 report that they are using encryption, thin-client and other security measures in the wake of recent stolen laptop incidents involving Marks & Spencer, the Metropolitan Police, Nationwide Building Society, Serco and Worcestershire County Council. Half of silicon.com's CIO user panel said that they are using or planning to use **hard disk encryption** to protect corporate data on laptops. Britain's Independent Television Network (ITN) reported that it uses technology that allows it to **remotely erase** the hard drive of a lost or stolen laptop (presumably when it goes online). See article at http://news.zdnet.co.uk/security/0,1000000189,39287101,00.htm (*ZDNet* UK, May 16, 2007). The UK Information Commissioner and Canadian privacy commissioners at federal and provincial levels have all weighed in on the topic, advising companies and public agencies to encrypt and otherwise protect sensitive personal information on laptops and other mobile devices. Officials in other European countries and Japan have made similar statements, but the lack of legal obligations to report security breaches results in less publicity about the problem outside the United States.

The examples listed above are those that involve **unencrypted** data, putting the enterprise and individuals at greater risk when a hard drive was lost or stolen. The frequency of such events suggests that no amount of training or policy writing will completely eliminate the hazard of compromised sensitive information on a portable device. As these cases illustrate, laptops are left behind at airports, libraries and coffee shops; they are stolen from unlocked offices and conference rooms and from parked cars, burglarized from homes and offices and even taken from their owners at gunpoint on the street or in a parking garage.

Based on information from law enforcement bodies and identity theft support groups, it appears that the misappropriation of a laptop or other portable device is often a crime of opportunity. The thief is interested in taking the laptop for himself or fencing it for as little as a hundred dollars. Many stolen laptops and desktops are sold as used equipment on eBay or other auction sites, as well as online classified advertising portals. The data may, or may not be, accessed before the hard drive is wiped and reused.

Sometimes, however, the person who comes into possession of the hard drive realizes the greater value of the data it contains and either sells the data to criminals or unscrupulous competitors or effectively "ransoms" the

hard drive back to the original user (who may fear repercussions from his or her employer if the loss becomes known) or directly to the enterprise.

More ominously, on other occasions, the theft is deliberately planned, in order to obtain valuable information for purposes of **fraud** or **identity theft, extortion, industrial or national espionage, terrorism**, or to gain access to information or credentials that would facilitate **intrusion** into the physical premises or computer network of the targeted enterprise.

These risks, and the frequency of security failures, have provoked legal and regulatory responses that enterprises should take into account in IT procurement and in establishing security policies and practices.

## Seagate/Wave Full Disk Encryption and Drive Management Solutions

The foregoing summary of laptop risks, more fully documented in **Appendix A**, shows that lost or stolen laptops loaded with unencrypted, sensitive data are a common and persistent problem. And, as the discussion on compliance and legal risks demonstrates, enterprises are exposed to an increasingly critical legal, investor, and market environment in reaction to such losses.

Notably, reports concerning many of the security breach incidents listed in Appendix A indicate that the organization made encryption software available to the user of the laptop, desktop, server, or portable hard drive – **but the user either did not know how to encrypt the data** (thereby making it unusable to a thief) **or did not take the time to do so**. Only a technical solution that automatically encrypts all data recorded on the hard drive fully addresses this costly human vulnerability.

Full-disk encryption is one way to ensure that an organization has the benefit of legal defenses and is not required to announce every laptop that goes missing under security breach notice laws in the United States (and under consideration in other jurisdictions). This has not gone unremarked in the information security industry. See, e.g., the **Burton Group** analysis report, "Lost or Stolen Laptop? Have No Fear, Encryption Is Here!," Inflection Point podcast, August 24, 2006, available online at http://podcast.burtongroup.com/ip/2006/08/lost_or_stolen_.html.

Encryption is clearly one critical technique for avoiding data losses and liability arising from laptops. Data protection is even more effective when (a) **encryption is automatic** and (b) it is combined with other security tools such as remote administration, authentication tokens, biometrics, or a Trusted Platform Module (TPM) that keeps device or user authentication functions on a separate chip. See, e.g., R. Enderle, "TPM to Bolster Laptop Security," darkREADING, June 19, 2006, available online at www.darkreading.com/document.asp?doc_id=95391 (the article mentions Wave Systems' EMBASSY Solution and Seagate hard drives).

Seagate's **Momentus 5400 FDE.2 Trusted Drive**, combined with Wave's **EMBASSY Trusted Drive Manager** and **EMBASSY Remote Administration Server** (ERAS), offers an efficient way for enterprises to ensure automatic full-disk encryption, secure authentication, and remote administration controls. Briefly, here is how these products enhance information security:

- The Seagate Momentus 5400 FDE.2 Trusted Drive has been tested and certified compliant with **AES encryption** as defined in NIST FIPS 197. Seagate's certificate #587 is posted on the NIST website at http://csrc.nist.gov/cryptval/aes/aesval.html.

  This form of strong cryptography is consistent with FIPS 197 and NIST, US Department of Homeland Security, and Office of Management and Budget recommendations and satisfies every encryption requirement and recommendation detailed below, as well as the encryption "safe harbor" under breach notice laws.

- The Wave Trusted Drive Manager pre-boot authentication feature enforces policy-driven access control immediately as the drive powers up. The **pre-boot authentication** application displays the pre-boot screen to request the user's credentials. These credentials are then compared to the credentials that were stored in the drive's hardware-protected credential cache during user enrollment. All of this is performed **outside the operating system**. Wave's Trusted Drive Manager is also integrated into the EMBASSY Security Center to activate the access control and authentication features of the Seagate drive, which has its own security controller and embedded capabilities for media-speed full disk encryption and pre-boot authentication. In short, the Trusted Drive Manager software activates the security that distinguishes a Trusted Drive from a standard hard drive.

  This meets or exceeds all of the access control and authentication requirements and recommendations detailed below, including the PCI DSS requirement to manage logical access independently of native operating system access control mechanisms.

- Wave's EMBASSY Remote Management feature then allows the organization's central IT department to **remotely effect provisioning and deprovisioning, deploy applications and updates, and delete data**.

  These features facilitate remote compliance with requirements and recommendations to

  - control data access dynamically on a "least privilege" or "need to know" basis as the user's role changes,
  - disable local administrative controls so that only remote, centrally administered controls can effect changes in security settings and maintain a full audit log of such changes,
  - deploy and update applications software, including antivirus and other security applications and patches,
  - log changes to the FDE drive security settings and user or administrator access to data[2], and
  - destroy stored data at the end of its usefulness or in the event of deprovisioning or a suspected security breach.

Laptops are not only lost or stolen but often repurposed in connection with organizational restructuring or outsourcing. In each of these scenarios, the Trusted Drive Manager makes it possible for a drive administrator to destroy the drive's encryption key remotely, as soon as it connects to the network. This renders all the data on the drive permanently unreadable. The entire file system is cryptographically obliterated, allowing the drive to be repurposed with confidence that no residual data can be recovered, and satisfying applicable data disposal requirements.

Wave's Trusted Drive Manager and EMBASSY Remote Administration Server also create an audit trail for provisioning, deprovisioning, updates, and data destruction on the laptop. This is an aid in forensic investigation. It can also bolster an enterprise's legal claims and defenses and help the enterprise reach an appropriate decision about notifying officials or individuals based on the likelihood of unauthorized access to protected data.

In sum, Seagate's FDE drives, managed with Wave's Trusted Drive Manager and EMBASSY Remote Management, represent a superior solution to common laptop security problems. And, as the following discussion on compliance and liability suggests, this product combination will effectively protect enterprise and personal data, achieve legal compliance, avoid public notice of laptop security breaches, allow the enterprise to declare conformance with relevant standards and best-practice recommendations, and position the enterprise to defend its reputation and strengthen its legal defenses.

[2] Note that NIST's Computer Security Incident Handling Guide, Special Publication 800-61 (Jan. 2004) (www.csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf) emphasizes the need for an audit trail and evidence of access and changes when a security breach is suspected.

## Compliance, Liability and Evidence

Legislators and regulators have reacted to the tide of data security breaches with measures mandating information security governance controls, documented security policies and procedures, notice of security breaches, and sanctions including private rights of action to recover damages. These measures are meant to establish a higher level of **enterprise accountability** to individuals, shareholders, business partners, and regulators, while exposing the enterprise's information security practices to greater public scrutiny so that market forces can punish carelessness and encourage safe practices.

At the same time, injured parties are beginning to assert **legal claims** against allegedly negligent organizations for failing to protect sensitive information. Large numbers of affected individuals are represented in class action lawsuits or legal actions brought by state attorneys or trade unions. The standards established in these compliance and liability contexts provide at least a starting point for enterprises considering how to reduce their exposure to security breaches involving sensitive data.

In both compliance and liability contexts, there is an important forensic and evidentiary application of remote administration tools. The enterprise must be able to show, for example, that its security measures were not only reasonable and appropriate but were, more likely than not, in place at the time a laptop was lost or stolen. Remote administration tools, combined with central recordkeeping, provide the means to prove that a laptop was regularly checked to ensure that automatic encryption was installed and turned on and that authentication tools and credentials were updated, thus making it improbable that sensitive data were compromised.

For a more in-depth analysis of data protection regulations throughout the world, please see the folowing:

**Data Protection Laws and Regulations within North America**
from the unabridged white paper, ***Comply with Data Protection Laws and Regulations***
http://www.wave.com/about/whitepapers/FDE-Compliance-US.pdf

**Data Protection Laws and Regulations within Europe**
from the unabridged white paper, ***Comply with Data Protection Laws and Regulations***
http://www.wave.com/about/whitepapers/FDE-Compliance-Europe.pdf

**Data Protection Laws and Regulations within Asia-Pacific (APAC)**
from the unabridged white paper, ***Comply with Data Protection Laws and Regulations***
http://www.wave.com/about/whitepapers/FDE-Compliance-Asia.pdf

**Information Security Standards and Best Practices**
from the unabridged white paper, ***Comply with Data Protection Laws and Regulations***
http://www.wave.com/about/whitepapers/FDE-Compliance-S&P.pdf

## Conclusions

The preceding discussion indicates that laptop **encryption** and **authentication** are sometimes mandatory but are more often simply an efficient means of avoiding both actual harm and the legal obligation to provide notice of a lost or stolen hard drive. They also support a "reasonable care" defense in the event that sensitive data are still somehow compromised. Remote administration of hard drives is not expressly mandated in existing laws, regulations, standards, or best practices, but it facilitates satisfying a range of security requirements -- such as access control, audit records, and data deletion -- when the laptop is not on the organization's premises. Like encryption, these techniques also support a legal defense based on reasonable care.

As such technical security measures become more common in industry and government, it will be harder to defend against negligence claims and government enforcement actions if they are not employed.

It is important for an enterprise not only to protect data but to be able to prove that it does so. Remote administration software, combined with central audit logs, can furnish evidence that a lost or stolen device was routinely (and recently) checked to ensure that updated encryption and authentication measures were in place and working effectively.

It should be emphasized that the best protection for the enterprise and for other potentially affected parties is prevention, using any practicable means to keep sensitive data out of the hands of wrongdoers. Enterprises handling such data should keep current with available and cost-effective hardware and software solutions. Adopting only the minimum legally required security measures may serve as a defense in a legal proceeding, but is unlikely to satisfy public opinion or engender confidence among customers, employees, and regulators. In most cases involving sensitive data, an organization is more at risk in the court of public opinion than in a court of law, and it should evaluate technical security solutions with the aim of protecting its reputation, as well as ensuring compliance and avoiding liability. Products combining full disk encryption with secure authentication and remote administration offer an effective approach to managing laptop risks from each of those perspectives.

# Appendix B: Information Security Requirements and Sources

*Seagate FDE drives with Wave EMBASSY Trusted Drive Manager and ERAS remote administration meet or exceed each of the following selected requirements for laptop security:*

| **Requirement** / **Source** | *Encryption (data and keys)* | *Encryption (automatic)* | *Access Controls (ID mgmt and authentication)* | *Remote Admin. (ID mgmt and authentication)* | *Remote Admin. (data wiping)* | *Remote Admin. (audit log, suspicious activity monitoring)* |
|---|---|---|---|---|---|---|
| FISMA / NIST standards (mandatory for US federal agencies, recommended for private sector) | NIST / OMB / ID Theft TF recommend AES (FIPS 197) or DES encryption of laptop data; see also NIST SP 800-53 rev.1, MP-4 | NIST / OMB / ID Theft TF recommend encrypting all sensitive data on laptops | NIST SP 800-53 rev.1, AC-3, AC-6, AC-17, AC-19, IA-1 – IAN-7 | NIST SP 800-53 rev.1, AC-19 | NIST SP 800-53 rev.1, MP-6 (media sanitization) | NIST SP 800-53 rev.1, AU-6 |
| PCI DSS security standard (payment card industry) | Requirements 3, 4; "strong encryption" (3.4) | Requirements 3, 4 | Requirements 7, 9; logical access separate from OS (3.4.1) | Requirements 7, 9; automatic key changes (3.6.4) | Requirement 3.1, 9.10.2 | Requirement 9.7 |
| ISO 17799 / 27002 and BS 7799 | As indicated by analysis conducted under Risk Assessment element | As indicated by analysis conducted under Risk Assessment element | Access Control element; Communications and Operations Mgmt requirement | Communications and Operations Mgmt element | Information Security Incident Mgmt element | Information Security Incident Mgmt element |
| ITIL / ISO 20000 | IT Security Mgmt requirements | IT Security Mgmt requirements, as indicated by risk assessment | IT Security Mgmt | IT Security Mgmt | IT Security Mgmt; Software Asset Mgmt | IT Security Mgmt requirements |
| GLBA and FFIEC (US financial data) | Safeguards appropriate to identified risks | Safeguards appropriate to identified risks | Access on a "need-to-know" basis; access controls required by FFIEC | As appropriate for identified risks | FFIEC guidelines | FFIEC guidelines |

## Information Security Requirements and Sources:

| **Requirement** / **Source** | *Encryption (data and keys)* | *Encryption (automatic)* | *Access Controls (ID mgmt and authentication)* | *Remote Admin. (ID mgmt and authentication)* | *Remote Admin. (data wiping)* | *Remote Admin. (audit log, suspicious activity monitoring)* |
|---|---|---|---|---|---|---|
| HIPAA Privacy Rule (US health information) | 164.306 appropriate methods to assure confidentiality of electronic health information; 164.312 encryption | 164.306 appropriate methods to assure confidentiality of electronic health information; 164.312 encryption | 164.308, 164.312 ID and access controls, authentication | 164.308, 164.312 ID and access controls, authentication | 164.310 data disposal from electronic media | 164.308 audit logs, access reports, incident tracking |
| FCRA / FACTA (US consumer reports) | Confidentiality obligation | Confidentiality obligation | Confidentiality obligation | | FACTA Disposal Rule | |
| US FTC, State enforcement of "fair trade" acts and related private litigation | Required in consent decrees for SSNs, payment card data; negligence standard with reference to PCI DSS and GLBA Financial Safeguards Rule | Negligence standard (reasonable care) | Required in consent decrees for SSNs, payment card data; negligence standard with reference to PCI DSS and GLBA Financial Safeguards Rule | Negligence standard (reasonable care) | Consent decrees address life-cycle security; negligence standard (reasonable care) | Negligence standard of reasonable care, based on industry practice |
| US state (and proposed federal) laws on security and security breach notice for personal data that raises ID theft risks | Encryption "safe harbor" in laws in 30+ states based on CA SB 1386<br><br>CA AB 1950 and several other state laws require "reasonable" security measures<br><br>Several states considering reference to PCI DSS standard | Safe harbor not available if enterprise cannot be sure that covered data were encrypted | CA AB 1950 and several other state laws require "reasonable" security measures<br><br>Several states considering reference to PCI DSS standard | CA AB 1950 and several other state laws require "reasonable" security measures<br><br>Several states considering reference to PCI DSS standard | Sensitive data disposal required in CA, other states<br><br>Several states considering reference to PCI DSS standard | CA AB 1950 and several other state laws require "reasonable" security measures<br><br>Several states considering reference to PCI DSS standard |

## Information Security Requirements and Sources:

| **Requirement** / **Source** | *Encryption (data and keys)* | *Encryption (automatic)* | *Access Controls (ID mgmt and authentication)* | *Remote Admin. (ID mgmt and authentication)* | *Remote Admin. (data wiping)* | *Remote Admin. (audit log, suspicious activity monitoring)* |
|---|---|---|---|---|---|---|
| Canada PIPEDA (and similar provincial laws) | Principle 7 (security measures proportional to risk of harm); §4.7.3 encryption | Principle 7 (security measures proportional to risk of harm) | Principle 7: limit access on a "need-to-know" basis (§4.7.3) | Principle 7: limit access on a "need-to-know" basis (§4.7.3) | Principle 7, §4.7.5 | Principle 7 (security measures proportional to risk of harm) |
| European Union Data Protection Directive and related laws and regulations | Art. 17 "appropriate organizational and technical measures"<br><br>UK: threatens enforcement for losses due to unencrypted laptops<br><br>Spain: encryption required for sensitive data<br><br>Art. 29 WP opinions encourage laptop encryption | Art. 17 "appropriate organizational and technical measures" | Art. 17 "appropriate organizational and technical measures;" European data protection authorities require access restrictions based on functional responsibilities | Art. 17 "appropriate organizational and technical measures" | Art. 6(e) data disposal;<br><br>Art. 17 "appropriate organizational and technical measures" | Art. 17 "appropriate organizational and technical measures" |

## About the Author

W. Scott Blackmer has been practicing technology law for more than 20 years. Based in Washington, DC, Brussels and Salt Lake City, his practice centers on intellectual property and issues relating to Web services and e-commerce, privacy, data protection and information security. He was admitted to the Bar of Washington, DC, Maryland and Utah.

## About Wave Systems

Consumers and businesses are demanding a computing environment that is more trusted, private, safe and secure. Wave is a leader in delivering trusted computing applications and services with advanced products, infrastructure and solutions across multiple trusted platforms from a variety of vendors. Wave holds a portfolio of significant fundamental patents in security and e-commerce applications and employs some of the world's leading security systems architects and engineers. For more information about Wave, visit http://www.wave.com.

Part # 03-000227/version 1.01 Effective Date: 2008-08-31