



# 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

Executive Summary . . . . .	1
Introduction . . . . .	4
Hard Drives at Risk . . . . .	4
Full Disk Encryption and Drive Management Solutions . . . . .	10
Compliance Liability and Evidence . . . . .	11
United States . . . . .	12
Canada . . . . .	28
Europe . . . . .	29
Australia . . . . .	37
Japan . . . . .	38
Singapore . . . . .	38
Korea . . . . .	38
Information Security Standards and Best Practices . . . . .	39
Conclusions . . . . .	44
Appendix A: Lost or Stolen Laptops and Hard Drives. . . . .	45
Appendix B: Information Security Requirements and Sources. . . . .	53
About the Author . . . . .	56
About Wave Systems . . . . .	56

## 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.<sup>1</sup>

## 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.

<sup>1</sup> 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.

October 2007  
[www.wave.com](http://www.wave.com)

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](http://eweek.com), [www.eweek.com/article2/0%2C1895%2C2101683%2C00.asp](http://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](http://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](http://www.networkworld.com/news/2007/031307-data-breach-companies.html).)

The **Privacy 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](http://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](http://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](http://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).
- Ford Motor Company (70,000 employee records on a stolen computer, December 2005).
- FirstTrust Bank (100,000 customer records on a stolen laptop, December 2005).
- Ameriprise (data on 226,000 investors and financial advisors on a laptop stolen from a locked car in December 2005, later recovered by the police).
- 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).
- US Department of Veterans' Affairs (laptop and external hard drive with unencrypted Social Security numbers and other personal information on some **28.6 million** individuals stolen from an employee's home, May 2006; the laptop was ultimately recovered, apparently before the data had been used for ID theft or fraud, but the incident cost the VA hundreds of thousands of dollars in the interim and resulted in threatened legislation in addition to a vendor contract, which review patterns of laptop misuse.

The VA announced in August 2006 that a computer stolen from contractor Unisys contained records on at least 18,000 persons, and in January 2007 the VA disclosed that it had lost a portable hard drive with personal information and billing records on more than **500,000 veterans and 1.3 million doctors**).

- Aetna (health insurance records for 38,000 employees of the US Department of Defense and Omni Hotels on a laptop stolen from an Aetna employee's car, April 2006).
- Hummingbird (Toronto, Canada), a contractor for the Texas Guaranteed Student Loan Corp., (**1.7 million** borrowers' records were stored on a lost hard drive May 2006).
- Ernst & Young UK (an auditor's stolen laptop included credit card data on 243,000 customers of Hotels.com, May 2006).
- American Institute of Certified Public Accountants (330,000 member records, including Social Security numbers, on an unencrypted hard drive that was lost while being shipped back to AICPA from a computer repair company, May 2006).
- YMCA (stolen laptop with personal data on 65,000 members, June 2006).
- Union Pacific (stolen laptop with records on 30,000 employees, June 2006).
- AIG Insurance Group (records on 930,000 individuals, including Social Security numbers and some medical and disability information, on a stolen server, announced June 2006).
- National Association of Securities Dealers (ten laptops stolen from NASD investigators, with files on dealers under investigation, announced July 2006).

- Marsh Inc. (CS Stars) (records of 540,000 workers' compensation claims on a stolen computer that was later recovered, July 2006; the company was required to reimburse the state \$60,000 in investigation costs).
- US Department of Transportation (stolen laptop with records of 132,470 persons with drivers' or pilots' licenses, and another stolen laptop with records of investigations, both in August 2006).
- City of Chicago (laptop stolen from retirement benefits management company included data on up to 38,000 employees, September 2006).
- General Electric (50,000 employee records on a laptop stolen from a hotel room, September 2006).
- US Department of Commerce and Census Bureau (**1137 of their laptops** had been lost or stolen since 2001, September 2006).
- North Carolina Department of Motor Vehicles (computer stolen with data on 16,000 drivers' licenses, September 2006).
- New Jersey National Guard (**26** computers stolen 2004-2006, all unencrypted, October 2006).
- T-Mobile USA (records on 43,000 current and former employees on a laptop that disappeared in airline checked baggage, October 2006).
- Starbucks (four missing laptops with data on more than 60,000 US and Canadian employees and contract workers, November 2006).
- Colorado Department of Human Services (stolen computer with data on up to **1.4 million** individuals, November 2006).
- Pennsylvania Department of Transportation (stolen computers with records on more than 11,000 licensed drivers, November 2006).
- University of Idaho (three stolen desktop computers with data on **331,000** individuals, including 70,000 Social Security numbers, January 2007).
- US Internal Revenue Service, according to a 2007 audit report, has lost nearly **500 laptops** since 2003 from employees' homes, cars, and offices, compromising financial data on thousands of taxpayers.
- North Carolina Department of Revenue (30,000 taxpayer records on a stolen laptop, January 2007).
- Speedmark (stolen computers with 35,000 consumer records, February 2007).
- St. Mary's Hospital (stolen laptop with **130,000** patient records, February 2007).
- Kaiser Permanente Medical Center, Oakland (stolen laptop with 22,000 patient records, February 2007).
- California National Guard (stolen hard drive with records of 1,300 guardsmen on border patrol duty, March 2007).
- US Department of Agriculture (**95 department computers** were lost or stolen between October 2005 and May 2006, compromising an unknown amount of government and personal information, an estimated two-thirds of which was unencrypted, March 2007).
- Los Angeles County Child Support Services (three stolen laptops with data on **243,000** individuals, March 2007).
- Group Health Cooperative, Seattle (two stolen laptops with data on 31,000 patients and employees, March 2007).
- Chicago Public Schools (two stolen laptops with data on 40,000 current and former employees, April 2007).
- Neiman Marcus Group ("computer equipment" stolen from a consultant included data on **160,000** current and former employees, April 2007).

- US Transportation Security Administration (TSA) (a portable hard drive including records on **100,000** current and former TSA employees including undercover air marshals disappeared from its office, May 2007). This resulted in a **lawsuit** against TSA by the AFGE government employees union.
- Texas Commission of Law Enforcement Standards and Education (stolen computer belonging to Productivity Center Incorporated contained data on **230,000** Texas law enforcement officers, May 2007).
- Pfizer (three incidents - unauthorized file sharing software on a laptop compromised data on 17,000 employees, two stolen laptops including data on nearly 1000 independent contractors, and 34,000 employee records were copied and removed by an employee, June - September 2007).
- Yuba County Health and Human Services (70,000 social services records on a stolen laptop, July 2007).
- Connecticut Department of Revenue Services (106,000 taxpayer records on a stolen laptop, August 2007).

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](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](http://www.darkreading.com/document.asp?doc_id=95391) (the article mentions Wave Systems’ EMBASSY Solution and Seagate hard drives).

Seagate’s **Momentum 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 Momentum 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<sup>2</sup>, 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.

## 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.

<sup>2</sup> 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](http://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.

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.

### **United States**

In the United States, legal requirements to safeguard data derive from several different sources, based variously on the need to protect individuals, investors, business partners or public safety and national security. Some obligations are defined by statutes and regulations, while others arise from contract and express or implied promises, common-law principles of negligence and “invasion of privacy” tort law. There is no overarching, comprehensive data protection legislation as is found in Europe, Canada, Japan, Australia, Hong Kong and several other jurisdictions (see attachments at the end of this white paper for analysis of European and Asian data protection legislation as it pertains to laptops and portable devices). Instead, sectoral laws at federal and state level govern security and privacy in specific contexts, while general principles of contract, negligence or fair trading may be asserted in addition, or in other circumstances where there is an injury that is not covered by specific statutes and regulations.

There is a strong “**litigation culture**” in the United States that tends to make enterprises particularly anxious to establish compliance and reasonable care when handling potentially risky information. Regulatory bodies and enforcement agencies with broad powers, such as the Federal Trade Commission (FTC) and state attorneys general, have been very active in investigating data security breaches. Private litigants often ride their coattails. Unique features of the American legal system also encourage private litigation. These include the availability of class actions, “private attorney general” actions in some states (prominently California), contingency fees for legal counsel and extensive “discovery” procedures to obtain evidence of possible wrongdoing. As a result, enterprises must consider **civil liability risk management, as well as explicit compliance requirements** when planning for information security and incident response.

What follows is a summary of relevant requirements and legal standards for information security that derive both from legislation and from common-law principles that have been asserted in litigation following security breaches.

### ***Sarbanes-Oxley and Corporate Internal Controls***

For a financial reporting law, the federal Sarbanes-Oxley Act of 2002<sup>3</sup> (often abbreviated as “**SOX**,” “SarbOx,” or “SOA”) gets enormous attention in information security circles. The law was enacted following corporate financial meltdowns at Enron, Tyco, WorldCom, Peregrine Systems and Global Crossings, in an attempt to tighten accounting and audit standards for public companies. One of the side effects has been **greater scrutiny of corporate information systems**.

SOX imposed new obligations on publicly traded corporations to provide periodic management reports on the corporation’s “disclosure controls and procedures” and “internal control over financial reporting.” The Act, which first affected financial reports for larger corporations for fiscal years ending in 2004, was designed to provide greater transparency and more reliable information for investors concerning a corporation’s financial condition and material risks. SOX strengthens the independence of auditors and directors’ audit committees and imposes new sanctions for responsible corporate officers. Generally, SOX has raised the bar for corporate compliance and **risk management** efforts. It has also triggered a systematic review of IT practices and information security risks, since the data to be included in SEC reports are predominantly stored and processed in a company’s information systems.

<sup>3</sup> Available online at <http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3763.ENR:%20>

Several provisions of SOX are of particular interest to corporate information technology departments and should be taken into account in planning operations, security and security incident response:

- § 105 full-time availability of records to official investigators
- § 302 officers' responsibilities for financial reports
- § 401 disclosures in annual and quarterly reports
- § 404 management assessment of internal controls
- § 409 real-time disclosure of material changes in financial condition or operations, and
- §§ 802, 1102 penalties for destroying or altering records or impeding an official investigation

The Securities and Exchange Commission (SEC) has issued regulations detailing corporate reporting requirements following SOX. SEC Regulation S-K (17 C.F.R. subpart 229) is available online at the SEC website, [www.sec.gov/about/forms/regs-k.pdf](http://www.sec.gov/about/forms/regs-k.pdf). Generally speaking, the company's quarterly and annual reports, which are made public, must disclose any **material changes in the company's business or risk exposure**. Independent auditors must attest to the "effectiveness" of the company's internal disclosure controls and procedures. The chief executive officer and the chief financial officer must also submit their own "conclusions" as to the effectiveness of the company's internal controls. If the independent auditor advises the company that there are **material weaknesses in internal controls**, that fact must be disclosed in the company's public reports.

As a result, information of these requirements is that information security officers now regularly report to senior executives and auditors, who must be satisfied that the corporation has evaluated significant security risks and taken effective steps to avoid them. Over 1500 SEC filings since 2004 have disclosed control weaknesses, some resulting from IT security issues. These filings are closely watched by industry analysts and often affect a company's share price.

The SEC's 2003 Final Rule on Management's Reports on Internal Control over Financial Reporting ([www.sec.gov/rules/final/33-8238.htm](http://www.sec.gov/rules/final/33-8238.htm)) emphasizes that internal controls must provide "reasonable assurance regarding **prevention or timely detection of unauthorized acquisition, use or disposition of company assets**." Information systems and data holdings are important assets for most modern corporations, and security breaches can result in material loss exposure. Thus, for most companies, the quarterly certification that all material internal controls are in place will cover the company's information security policies, procedures and recent experience.

As indicated in the text accompanying this rule, the SEC relied on the concept of "internal controls" adopted by the American Institute of Certified Public Accountants (AICPA) as an auditing standard in 1995 (AU §319). This, in turn, was based on the report entitled, "Internal Control – Integrated Framework" issued by the Committee of Sponsoring Organizations of the Treadway Commission ("COSO") in 1992 (see [www.coso.org](http://www.coso.org)). The SEC commented on this auditing framework in its discussion of the internal control rules implementing SOX §404:

"The COSO Framework defined internal control as 'a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives' in three categories – effectiveness and efficiency of operations; reliability of financial reporting, and compliance with applicable laws and regulations. COSO further stated that internal control consists of: the control environment, risk assessment, control activities, information and communication and monitoring."

Under its SOX regulations, the SEC requires reporting companies to identify the evaluation framework they use to assess their internal controls. It does not mandate one or another control framework, but its explicit acceptance of the COSO Framework has led many if not most publicly traded US corporations to organize internal controls and audits according to that framework. The SEC's rules require that management's reports on internal controls identify the evaluation framework used by management to assess the effectiveness of the company's internal controls.<sup>4</sup>

<sup>4</sup> See [www.sec.gov/rules/final/33-8238.htm#iib3a](http://www.sec.gov/rules/final/33-8238.htm#iib3a)

In the wake of SOX, the SEC, independent auditors and a self-regulatory body created by SOX, the Public Company Accounting Oversight Board (**PCAOB**) typically refer to the **COSO Framework** in evaluating internal controls designed to **protect assets** and ensure **compliance with applicable laws and regulations**.

The COSO Framework was expanded in COSO's 2004 publication, "Enterprise Risk Management – Integrated Framework" (ERM) (available for purchase at [www.coso.org](http://www.coso.org)). The COSO ERM Framework is now commonly used in SOX audits to assess internal controls under SOX §404. It identifies eight components of enterprise risk management:

1. Internal environment or "tone" of an organization toward risk and integrity.
2. Objectives – a process for setting objectives to meet the organization's mission.
3. Event identification – internal or external events that could affect the achievement of those objectives.
4. Risk assessment – the likelihood and impact of adverse events.
5. Risk responses.
6. Control activities to ensure that the risk responses are carried out.
7. Information communication to ensure that people know how to fulfill their responsibilities.
8. Monitoring, evaluation, and modification.

Any company subject to SEC disclosure requirements needs to **implement a standard framework for internal controls and apply it to significant security risks**. In a corporation where laptop risks are significant, these should be covered in the "event identification," "risk assessment," and "risk responses" aspects of risk management. Those risk responses, such as encryption, controls on remote access and downloading, or the use of trusted platform modules to authenticate users or devices, can then be the subject of appropriate control activities, staff training and policy communication, and random or automated monitoring to test whether portable hard drives are compliant with the corporation's policies. (For many enterprises, simply locating their laptops at any given time is a challenge; some have resorted to installing GPS tracking devices similar to the Lo-Jack system for automobiles.)

A company's general framework for internal controls is often supplemented by frameworks or standards specifically addressing the security of information technology. The most commonly employed, for SOX purposes, is the Control Objectives for Information and Related Technology (CobiT) published by the IT Governance Institute (**ITGI**) and the Information Systems Audit and Control Association (**ISACA**) (available online with a paid subscription at [www.isaca.org](http://www.isaca.org)). This IT control model, now in its fourth edition, builds on the COSO Framework and is closely related to **PCAOB Auditing Standard No. 2** used by independent auditors. CobiT offers more detailed guidance on control measures relating to IT procurement and deployment and suggests factors to consider in selecting technical security measures such as **encryption** for categories of data that present a particular risk of loss or legal noncompliance. Companies and auditors employing CobiT should use this model to systematically evaluate the organization's laptop-related risks and responses.

Many public companies refer, in addition, to more specific information security standards and best practices, such as **ISO 17799 / 27002**, **ITIL**, and **NIST 800-series** standards and recommendations, which are described in the Information Security Standards section below. Conformance to such widely accepted standards can be an effective and defensible way to implement information management internal controls.

SOX, the SEC regulations, the COSO Framework, and CobiT all have a **procedural** focus on effective internal controls to protect a company's assets and operations assuring both legal compliance and reliable reporting. They do not prescribe any particular technical security measures. They do require a corporation to assess its security risks frequently, adopt both appropriate technical and organizational measures to manage those risks, and disclose security incidents that affect the corporation's financial results.

Given the scale and frequency of security incidents involving stolen business laptops and other hard drives containing sensitive data, a corporation would find it hard to persuade auditors, the SEC, or the investing public that such an incident was unforeseen and need not have been covered by internal control procedures. **Laptop security** can and should be addressed within the internal control framework adopted by the enterprise.

The COSO and CobiT control frameworks summarized above suggest that, at a minimum, the following elements of internal controls should be applied to laptop security:

- The policy and organizational control environment should encompass laptop risks (there should be a “laptop policy” and clearly defined responsibilities for securing data on laptops and other portable drives)
- IT risk assessment should expressly cover the risks associated with compromised laptops
- Technical and organizational control measures should be implemented to reduce laptop risks (these may include provisioning and access controls, restrictions and audit trails in downloading sensitive data from protected databases, **file or disk encryption**, **secure authentication** methods and **remote administration** capabilities to check, update and, if necessary, delete the contents of a hard drive)
- Staff should be trained in the laptop security policy and procedures
- Laptops and other portable drives should be monitored to establish that they are being used in conformance with company policies (techniques range from random spot-checks to automated, remote verification of status)

### ***FISMA***

While publicly traded corporations in the United States are required by SOX to establish and report effective internal controls over information security risks, federal agencies are generally subject to the Federal Information Security Management Act of 2002 (**FISMA**), 44 USC §§3541 *et seq*<sup>5</sup>. FISMA was included in the **Electronic Government Act of 2002** to establish a “comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets” (§3541).

Especially since SOX and FISMA were enacted in the same year, IT departments and information security vendors and consultants have taken a fresh look at the information security requirements of organizations.

FISMA directs the National Institute of Standards and Technology (NIST) to develop information technology security standards and guidelines for use by federal agencies (see discussion of relevant NIST documents in the Information Security Standards section below). Each federal agency must implement an information security program under the oversight of the Office of Management and Budget (OMB). Agencies must report annually to OMB on the effectiveness of their information technology security programs. The reports must include an independent evaluation by either the agency’s Inspector General (“IG”) or by an external auditor (most agencies have appointed an IG who performs this function).

In 2000, NIST and the federal government’s CIO Council developed and published the **Federal Information Technology Security Assessment Framework** (<http://csrc.nist.gov/organizations/guidance/framework-final.pdf>). Like CobiT, the NIST Framework describes procedures for ongoing risk assessment and the development, implementation, and monitoring of risk management techniques. Under this framework, as under COSO, CobiT, and ISO 17799 / 27002, organizations monitor and periodically re-evaluate information security risks, explicitly including those arising from mobile computing and remote access, and document that they have implemented security measures have been implemented proportionate to the identified risks.

The 2002 NIST **Risk Management Guide for Information Technology Systems** (Special Publication 800-30) provides guidelines for conducting an IT risk assessment and selecting appropriate risk mitigation measures. This guide would be a useful reference for an organization designing a periodic risk assessment program and documenting the choice of mitigation measures aligned to identified risks, including laptop risks, and their likely impact on the organization.

Highly publicized laptop incidents at the Veterans’ Administration, Internal Revenue Service, and other civilian federal agencies, as well as in the armed forces (see the Government section of Appendix A) have resulted in more extensive internal audits and recommendations for laptop security, promoting the routine use of **laptop encryption** in many agencies.

<sup>5</sup> Text at <http://csrc.nist.gov/policies/FISMA-final.pdf>

The recently published Report of the President's **Identity Theft Task Force**, "A Strategy to Combat Identity Theft" (April 2007), available at [www.idtheft.gov/reports/StrategicPlan.pdf](http://www.idtheft.gov/reports/StrategicPlan.pdf), mentions on page 28 that the Office of Management and Budget (OMB) has recommended thoroughgoing encryption practices on government laptops:

"Additionally, as part of its oversight role, Office of Management and Budget issued several guidance memoranda last year on how agencies should safeguard sensitive information, including a memorandum addressing FISMA oversight and reporting, and which provided a checklist developed by NIST concerning protection of remotely accessed information, and that recommended agencies, among other things, **encrypt all data on mobile devices** and use a "time-out" function for remote access and mobile devices." (Emphasis added.)

### **GLBA**

The Gramm-Leach-Bliley Financial Services Modernization Act of 1999 ("**GLBA**") includes provisions to protect financial privacy<sup>6</sup>. It applies to "financial institutions," but those are defined so broadly as to include many companies that are not traditionally regulated as bankers, brokers, or insurers but that are nevertheless "significantly engaged" in providing financial products or services.

Financial services providers under GLBA have an "affirmative and continuing obligation" to protect the "security and confidentiality" of their customers' nonpublic personal information (§501(a)). The regulatory agencies (which include the Federal Trade Commission in the case of nontraditional "financial institutions") are charged with setting and enforcing standards for "administrative, technical, and physical safeguards" to protect against any anticipated threats or hazards to the security or integrity of such records, and to prevent unauthorized access to or use of such records or information that could result in "substantial harm or inconvenience to any customer" (§501(b)).

These security safeguards must also specifically be designed to prevent "pretexting," where individuals seek to obtain financial information about others under false pretenses, which GLBA made a federal crime (§521). Note that pretexting could be facilitated by using authentication credentials found on a lost or stolen laptop.

GLBA mandates that financial institutions have "policies, procedures, and controls in place to prevent the unauthorized disclosure of customer financial information and to deter and detect activities proscribed under section 521" (§525). This suggests special care in handling Social Security numbers and account information and in validating the identity and authority of the person requesting information from the company.

In addition to the detailed security guidelines and examination procedures adopted by the federal banking and state insurance regulators under GLBA, in 2002 the FTC promulgated its own broadly similar guidelines to cover the nontraditional "financial institutions." The FTC's "**Financial Information Safeguards Rule**," 16 C.F.R. Part 314, is available online at [www.ftc.gov/os/2002/05/67fr36585.pdf](http://www.ftc.gov/os/2002/05/67fr36585.pdf). The Safeguards Rule, which took effect on May 23, 2003, requires organizations to develop and maintain a "security program," documented in writing, to protect nonpublic personal financial information. The program must include the following elements:

- Designate an employee or employees to coordinate the security program;
- Identify **reasonably foreseeable internal and external risks** to the security, confidentiality, and integrity of customer information and assess the **sufficiency of any safeguards** in place to control the risks, including each relevant area of operations and addressing at least the following:
  - Employee training and supervision,
  - Information systems, network and software design, information processing, storage, transmission, and disposal,
  - Means of detecting, preventing, and responding to attacks, intrusions, and systems failures;

<sup>6</sup> Title V - Privacy, §§ 501 et seq., Pub.L. 106-102 (1999), codified at 15 USC §§ 6801-6809, "Disclosure of Nonpublic Personal Information," text available online at <[http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106\\_cong\\_public\\_laws&docid=f:publ102.106](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ102.106)>

- **Design and implement safeguards** to address the identified risks; regularly test and monitor the effectiveness of the key security controls, systems, and procedures;
- Select and retain service providers that are capable of maintaining appropriate safeguards for the information and require them, by contract, to implement and maintain such safeguards (existing contracts were grandfathered until May 24, 2004); and
- Adjust the information security program in light of the results of testing, monitoring, and **incident responses**, taking into account changes in the organization's operations and information systems that may materially affect the security program.

The FTC Safeguards Rule does not prescribe particular security techniques. It allows flexibility for a company to design a security system that is appropriate to its "size and complexity," the "nature of its activities," and the "sensitivity" of the personal information it holds.

In 2005, the FTC settled an enforcement action with Superior Mortgage for noncompliance with the GLBA Safeguards Rule. The FTC's position was that the company's security procedures were deficient in the areas of risk assessment, access controls, document protection, and oversight of service providers. The FTC also asserted that Superior misrepresented to customers how it used encryption to protect sensitive financial information. Without admitting liability, Superior agreed to undertake a comprehensive data security program and retain an independent auditor to assess its security procedures and report to the FTC biennially for the next 10 years.

For many financial services providers, laptop security should be included in the required risk assessment, as well as in the safeguards adopted to avoid compromising protected financial information. The number and scope of laptop security breaches listed in the "Financial" section of Appendix A indicate that this risk has not been fully addressed in the security management practices of some financial institutions.

#### ***Other Financial Regulatory Requirements***

The Federal Financial Institutions Examination Council (**FFIEC**) examines banks and other federally regulated financial institutions annually. The examination includes their information security practices, using the 2006 version of the FFIEC Information Security Workbook, which tests the confidentiality, integrity, and availability of bank information systems. **Encryption** of customer financial data on mobile devices is generally required, and the examiners typically look into reported security breaches such as those listed in the "Financial" section of Appendix A.

The federal bank supervisory authorities (OCC, FDIC, OTS, and the Federal Reserve Board) jointly issued *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*<sup>7</sup>, as a further interpretation of GLBA §501(b) and the existing Security Guidelines for banks that have been in effect since 2001. The Guidance requires access controls and employee background checks to protect customer information and provides that if "sensitive" customer information is stolen or illegally accessed, the bank is required to first notify its primary regulator, and then, if certain conditions exist, notify the affected customers. (Sensitive information includes the customer's name, address, or telephone number in conjunction with a Social Security number, driver's license number, account number, credit or debit card number, PIN, or password that would permit access to the customer's account.)

This means that even in states that have not yet adopted security breach notice laws (discussed below), banks and thrifts will typically be required to **notify** regulators and, in many cases, customers when there is a laptop security breach. Also, the emphasis on access controls to customer financial information suggests that banks could be sanctioned for exposing customer data on **unencrypted** laptops.

<sup>7</sup> Text available at [www.occ.treas.gov/consumer/Customernoticeguidance.pdf](http://www.occ.treas.gov/consumer/Customernoticeguidance.pdf)

## HIPAA

In 2001 the federal Department of Health and Human Services finalized medical information privacy and security regulations under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA,” 42 U.S.C. §1301, *et seq.*). The **HIPAA Privacy Rule**, 45 C.F.R. Parts 160 and 164, took effect in 2003. It is available, along with related materials, on the HHS HIPAA website, [www.hhs.gov/ocr/hipaa](http://www.hhs.gov/ocr/hipaa). A separate HIPAA Security Rule (available from the same website) was later adopted, specifying much more detailed security standards that came into force in 2005 (2006 for small health plans).

HIPAA applies directly only to health care providers who use electronic information systems, health care clearinghouses, and health insurance plans. In some cases, employers that administer their own health plans or employee assistance programs are covered directly, while in most cases employers are indirectly affected because of obligations to maintain the confidentiality of “individually identifiable health information” obtained from a covered entity such as an insurer or HMO.

Even organizations that are not directly covered by the HIPAA rules would be well advised to secure the confidentiality of health-related employee information because

- (a) the organization may be subject to HIPAA indirectly, when it exchanges health-related information with covered entities;
- (b) a variety of state laws protect particular kinds of health information (such as information about pregnancy and maternity, tuberculosis, AIDS, and mental health treatment);
- (c) health-related information is typically covered by either comprehensive or sectoral privacy laws outside the United States, and
- (d) employees and other individuals in the US and elsewhere conceivably could assert a “reasonable expectation of privacy” with respect to such information in a legal action based, for example, on negligence, breach of confidence, or invasion of privacy.

The HIPAA Privacy Rule provides a self-proclaimed “**national standard**” for medical privacy that could be relevant in determining the “reasonableness” of a company’s security measures concerning health data, even where the data are not directly covered by HIPAA.

The HIPAA Privacy Rule includes an “**Administrative Requirements**” section, § 164.530, which requires

- designation of a “privacy official” responsible internally for HIPAA privacy policies and procedures, as well as a contact point for complaints (§ 164.530(a));
- staff training in HIPAA compliance, which must be documented (§ 164.530(b)), and
- “Safeguards” (§ 164.530(c)) in the form of “appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information” by preventing intentional or unintentional uses or disclosures in violation of the Rule. The HHS “Summary” of the Privacy Rule mentions that appropriate safeguards could include:
  - shredding documents before discarding them,
  - securing medical records with lock and key or pass codes, and
  - limiting access to keys and pass codes to those employees with a need to access the data for permitted or required uses.

Note that § 164.528 of the HIPAA Privacy Rule also gives individuals a right (with some exceptions) to an accounting concerning disclosures of protected health information to third parties. This suggests that authentication must be employed and an audit trail must be maintained to identify who has accessed the information and for what purposes. That is very difficult to provide once data are downloaded on a laptop, unless remote administration tools are used to track downloads and access.

The **HIPAA Security Rule**, 45 C.F.R. Parts 160, 162, and 164, contains much more specific “**security standards**” for **administrative, technical, and physical safeguards** designed to ensure the integrity and confidentiality of “electronic protected health information” (individually identifiable health information that is stored or transmitted electronically). The operative provisions of the HIPAA Security Rule, which is available

in full at [www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.PPDF](http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.PPDF), run to about five triple-column printed pages in the Federal Register. These provisions constitute one of the most recent and most detailed prescriptions for security in any privacy-related law or regulation.

The approach under the HIPAA Security Rule is to state briefly each security “Standard,” followed by “Implementation Specifications” that are labeled either “Required” or “Addressable.” The latter refers to specifications that must be considered (“addressed”) and then implemented if they are found “reasonable and appropriate,” in which case they must be included in the written security program documentation. If the entity does not consider an “addressable” specification to be reasonable and appropriate, it must document the reasons for its conclusion and implement, if reasonable and appropriate, an “equivalent alternative measure.” See § 164.306(d).

The standards, specifications, and requirements are divided into several parts - general rules, administrative safeguards, physical safeguards, technical safeguards, organizational requirements, and requirements for security policies and documentation.

The summary below shows how **laptop encryption, secure authentication, and remote administration tools** fit into an organization’s HIPAA compliance plan.

**General rules** (§ 164.306) require covered entities:

- To ensure the “confidentiality, integrity, and availability” of electronic protected health information;
- To protect against any “reasonably anticipated threats or hazards to the security or integrity of such information;”
- To protect against any “reasonably anticipated uses or disclosures” that are not permitted or required under HIPAA;
- To ensure compliance by the relevant employees;
- To determine appropriate security measures in view of the “size, complexity, and capabilities” of the covered entity, its technical infrastructure and its hardware and software security capabilities, the costs of security measures, and the “probability and criticality of potential risks;” and
- To review and modify security measures as needed to maintain reasonable and appropriate protection.

**Relevance:** Given the large number of hard-drive security incidents involving health-related information since 2005 (see the “Medical” section of Appendix A), it would be difficult to argue that laptop risks cannot be “reasonably anticipated,” or that a covered entity could not feasibly use **encryption, secure authentication, and remote administration** to mitigate those risks.

**Administrative Safeguards** (§ 164.308) generally require:

- Risk analysis;
- Risk management measures “sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level;”
- Sanctions for users who fail to comply;
- Review of information system activity such as audit logs, access reports, and security incident tracking reports;
- Identification of “the security official” responsible for developing and implementing HIPAA security policies and procedures;
- Procedures for authorization and supervision of employee access to protected health information (addressable);
- Procedures for modifying or terminating access by an employee (addressable);
- Security awareness and training for all employees and management;

- Periodic security updates (addressable);
- Procedures for guarding against and reporting malicious software (addressable);
- Procedures for monitoring log-in attempts and reporting discrepancies (addressable);
- Procedures for password creation, changes, and safeguards (addressable);
- Procedures to identify and respond to known or suspected security incidents, mitigate harmful effects, and document security incidents and outcomes;
- Procedures for regular data backup;
- A disaster recovery plan;
- Procedures for emergency mode operation;
- Periodic testing and revision of disaster recovery procedures and emergency mode operations (addressable);
- Analysis of the “relative criticality” of specific applications and data (addressable);
- Periodic technical and non-technical evaluation, taking into account environmental and operational changes that affect the security of protected health information, and
- Written contracts with business associates that include security assurances (transmissions of data for health care treatment and payment are generally exempted, since the data are transmitted to covered entities that must themselves comply with the HIPAA Security Rule).

**Relevance:** Several of these requirements implicate laptop security and suggest that **encryption**, **secure authentication**, and **remote administration tools** would be appropriate security measures as applied to protected health information on laptops, particularly:

- the general requirement for a risk analysis and appropriate risk management measures,
- the need to create audit logs and access reports,
- procedures for controlling access to protected information,
- a mechanism for modifying or terminating employee access to protected information,
- the ability to effect periodic security updates in mobile devices,
- the requirement for means of responding to security incidents and mitigating harm.

*Physical Safeguards* (§ 164.310) are chiefly directed to security on the organization’s premises, but these also include some items applicable to laptop security.

**Relevance:** Laptop **encryption**, **secure authentication**, and **remote administration** can be part of the solution for the following physical safeguards:

- policies and procedures limiting physical access to electronic information systems;
- a facility security plan to safeguard the facility and equipment from unauthorized physical access, tampering, and theft (addressable);
- policies and procedures specifying the functions to be performed at work stations (presumably including laptops) and the physical attributes and surroundings acceptable for work stations that can access protected health information;
- procedures for disposing of protected health information and the hardware or media on which it is stored;
- procedures for removing protected health information from electronic media before the media are reused for other purposes,
- records on the movements of hardware and electronic media and the responsible person in each instance (addressable).

*Technical Safeguards* (§ 164.312) include several items pertinent to laptop security.

**Relevance:** Laptop **encryption**, **secure authentication**, and **remote administration** are relevant to essentially all of the HIPAA technical safeguards:

- policies and procedures for technical access controls;
- unique user identification;
- emergency access procedures;
- automatic logoff procedure (addressable);
- encryption and decryption mechanisms (addressable);
- hardware, software, and/or procedural audit mechanisms to examine activity in information systems containing protected health information;
- electronic mechanisms to validate the integrity of data; i.e., to verify that data have not been altered or destroyed without authorization (addressable);
- authentication procedures to verify the identity of persons and entities seeking to access the protected health information;
- technical security measures to safeguard information during transmission over electronic networks (addressable);
- measures to assure the integrity of data that are electronically transmitted (i.e., to assure that data are not altered without detection) (addressable), and
- mechanisms to encrypt protected health information (addressable).

*Organizational Requirements* (§ 164.314) concern contractual obligations and contract management, as well as the inclusion of security obligations in health plan documents.

**Security Policies and Documentation** (§ 164.316) requires covered entities:

- to implement policies and procedures to comply with all “reasonable and appropriate” implementation specifications;
- to document security policies and procedures on paper or electronically;
- to modify security policies and procedures as necessary;
- to make security policies and procedures available to the persons responsible for implementation;
- to retain security policies and procedures for at least six years.

**Relevance:** The organization’s approach to laptop security should be documented.

### *FCRA and FACTA*

The Fair Credit Reporting Act<sup>8</sup> (**FCRA**) imposes purpose, use, notice, access, and confidentiality requirements for consumer reports (such as, those provided by credit bureaus) but does not mandate particular security measures. FCRA was amended in 2003 by the Fair and Accurate Credit Transactions Act (**FACTA**)<sup>9</sup>, which mandates that businesses take “reasonable” measures to destroy information derived from consumer reports before discarding them, in effect from June 1, 2005. The **Federal Trade Commission (FTC) Disposal Rule** specifies how that is to be done.

One potential use of **remote administration** tools is to establish whether such data resides on a laptop and to delete the data effectively at the end of its useful life.

<sup>8</sup> Text at [http://www.law.cornell.edu/uscode/html/uscode15/uscode15\\_usc\\_sec\\_15\\_00001681----000-.html](http://www.law.cornell.edu/uscode/html/uscode15/uscode15_usc_sec_15_00001681----000-.html)

<sup>9</sup> Text at [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108\\_cong\\_public\\_laws&docid=f:publ159.108](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ159.108)

### *Fair Trade Practices Acts*

In addition to legislation and regulations explicitly requiring information security measures for particular kinds of data, inadequate safeguards have been asserted as “unfair or deceptive trade practices” under section 5(a) of the Federal Trade Commission Act (“**FTC Act §5**”) (and its state analogues) in several civil actions filed after major security breaches. Some of these actions have been brought by individuals or as class actions, while others have been brought by state or federal authorities on behalf of all affected citizens under unfair trading practices and consumer fraud statutes.

The FTC, for example, obtained settlements from Guess? Jeans, BJ’s Wholesale Club, Discount Shoe Warehouse, ChoicePoint, Tower Records, Microsoft, and Eli Lilly following their inadvertent disclosures of personal information such as customer names, addresses, and purchasing history – even in cases where there was no breach of a clear promise of confidentiality nor any compromised financial data such as credit card details<sup>10</sup>.

Thus, the FTC has gone beyond the “deceptive practices” rationale, which is keyed to a company’s promises, to find that inadequate information security for consumer data itself may constitute an “unfair practice” actionable under FTC Act §5. This precedent was first established in *In the Matter of BJ’s Wholesale Club, Inc.*, FTC File No. 0423160, Agreement Containing Consent Order (May 17, 2005)<sup>11</sup>. Following security breaches that resulted in compromising large numbers of credit and debit cards, and without asserting that these breaches violated any company promises regarding privacy protection, the FTC’s consent order required BJ’s Wholesale Club to establish a comprehensive information security program, essentially based on the FTC’s Financial Information Safeguards Rule (described in the “GLBA” section above), and conduct biannual security audits, reporting the results to the FTC for twenty years.

The New York State Attorney General similarly obtained settlements from Barnes & Noble and Victoria’s Secret based on security flaws in their transactional websites that exposed consumer data.

Stolen hard drives containing the names of over 500,000 military personnel led to a pending class action negligence suit against TriWest Healthcare Alliance, a private company that manages health maintenance programs for the US Defense Department.

More recently, the FTC, state attorneys general, and private litigants have challenged ChoicePoint, Card Systems, and TJX for security breaches involving data on millions of payment cards. Some of these suits have already been settled for millions of dollars and obligations to establish and report the results of security audits over a period of years.

### *Negligence, Contract, and Fraud*

In many of the cases cited above, and in the action recently brought by an employees’ union against the US Transportation Security Administration (TSA) for a laptop security breach, the authorities or private litigants have asserted negligence under common-law tort doctrine. Such actions are generally available in the United States and other common-law jurisdictions (such as, the UK, Canada, and Australia), where a retailer, service provider, or employer could be held to owe a duty of care to protect companies or individuals from **foreseeable harm** resulting from a negligent security lapse involving sensitive information. Such data could include, for example, bank account and payment card details, Social Security numbers and other official identifiers commonly used in identity theft, medical records, and information about children that could make them vulnerable to pedophiles.

In addition, there could be liability based on contract or quasi-contract (enforceable promises), where an enterprise arguably fails to meet its own express or implied promises or live up to commonly accepted industry standards for protecting sensitive information.

<sup>10</sup> FTC privacy cases under FTC Act §5 are summarized, with links to the relevant documents, at [http://www.ftc.gov/privacy/privacyinitiatives/promises\\_enf.html](http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html)

<sup>11</sup> Available online at <http://www.ftc.gov/os/caselist/0423160/050616agree0423160.pdf>

With the rise of identity theft, and as the list of laptop security incidents grows (see Appendix A), it becomes difficult to argue that harm to others resulting from insecure data on a laptop is not “foreseeable.” Moreover, as the use of laptop **encryption** spreads, it will be harder and harder for organizations to insist that they took “reasonable” measures to prevent such harm unless they encrypted the data.

In tort cases involving harm resulting from commercial activity, the standard of **reasonableness** is often based on **industry custom and practice** and the **cost of preventive measures compared to the likelihood and seriousness of harm**.

Evidence of industry practice could be anecdotal, or it could be based more solidly on adopted standards, such as the PCI security rules for payment cards (discussed below) or the FTC’s Financial Information Safeguards Rule (see the “GLBA” section above). Failure to conform to such widely used security practices could be deemed evidence of “unreasonableness.”

As for the cost-benefit analysis implicit in many tort judgments, the economic value of privacy is notoriously difficult to quantify. But security incidents involving economic loss to third parties, documented identity theft consequences, or the cumulation of relatively small damages for a very large number of people can raise the bar for defendants. And the relatively small unit cost of solutions such as disk **encryption** may persuade juries that there is no good reason for not using them to protect large amounts of sensitive data on laptops.

Contract liability could be imposed wherever an enterprise arguably promised to maintain the confidentiality of the other party’s data and then failed to do so. This was one of the legal grounds named in several of the private lawsuits and enforcement actions mentioned in the preceding section. If a court agrees that the defendant was contractually obligated to maintain confidentiality, the fact of a breach, with resulting damages, is generally sufficient to support the plaintiff’s claims.

Finally, in some cases it may be asserted that the defendant was aware of its security deficiencies when it made promises of confidentiality, in order to attract business. Those facts could be characterized as fraud in a civil or criminal proceeding. In the United States, however, it has been easier to establish liability for negligence or for “unfair or deceptive” trade practices, so the cases have usually proceeded on one or both of those theories.

The point is that enterprises should manage their laptop risks with an eye toward potential civil liability for negligence, contract, or fraud claims, and not only with regard to statutory or regulatory compliance regimes. All such claims can damage a company’s reputation, even if they are not ultimately successful in court.

### *EU-US Safe Harbor Program*

As a consequence of the prohibition in Article 25 of the European Union Data Protection Directive (discussed below) against transferring personal data to countries without an “adequate” level of legal protection, the US Department of Commerce negotiated an arrangement with the European Commission for organizations in the United States to voluntarily certify conformance to the **Safe Harbor Privacy Principles**<sup>12</sup>, and hundreds of multinationals have done so. The Safe Harbor “**Security Principle**” is a requirement for any organization that certifies under the Safe Harbor program with respect to data collected in Europe and processed or used in the United States:

“Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.”

This is a high-level statement of the certifying Company’s responsibility for taking “reasonable” security precautions. No particular measures are specified, and the certifying Company’s publicly available privacy statement need only mention that the company complies with the Safe Harbor principles, including reasonable security safeguards.

<sup>12</sup> See [www.export.gov/safeharbor](http://www.export.gov/safeharbor)

There is more guidance, however, in the interpretive documents published by the US Department of Commerce and the European Commission. One of these is a list of Frequently Asked Questions (“FAQs”). FAQ 10 clarifies that where personal data are sent to the US merely for processing on behalf of a European company (rather than being sent to a data “controller” in the US, which can use the data for its own purposes as would be the case for many US-based parent corporations), the processing remains subject to the “Article 17” contract requirements discussed below under the EU Data Protection Directive, rather than the more general Safe Harbor principles. Thus, the controller in the EU must still ensure that the US processor has adopted security measures that are consistent with the Directive’s security obligations, as amplified by any applicable European national data protection law, such as the more detailed security requirements articulated in Italy and Spain (see below).

Moreover, the Department of Commerce “Safe Harbor Workbook” observes that “[i]t does little good to have a strict privacy policy if personal data is available to any employee or if your computer systems and paper files are not secured.” The security section of the Workbook also makes the point that greater security measures should be taken to protect “**sensitive**” data (defined in the Safe Harbor principles, as in the EU Data Protection Directive, as information concerning race or ethnicity, health or sexual life, religious or philosophical beliefs, or political or trade union activity). This suggests that it is not enough to secure the data from dissemination outside the corporate group and its contractors, but that access to personal data in general, and sensitive data in particular, should be limited to employees and vendors with a functional “need to know.”

A lost or stolen laptop with unencrypted personal data from Europe presents a risk that a Safe Harbor company will be investigated by the FTC or by European data protection authorities for failing to live up to its Safe Harbor security commitment (this has happened). Serious or repeated failures could result in the withdrawal of the company’s Safe Harbor listing, which would jeopardize its ability to continue transferring data from Europe.

#### *Security Breach Notice Laws*

**California SB 1386** (which came into effect in July 2003, amending and adding, respectively, §§1798.82 and 1798.29 of the California Civil Code), the “**Security Breach Notice**” law, has served as a model for new legislation in most of the states. It has triggered costly and embarrassing disclosure of numerous laptop security breaches.

SB 1386 does not mandate any particular security measures to protect privacy, but it creates an enormous **incentive to encrypt** certain kinds of personal information by requiring prompt notice to the affected individuals when a company or agency keeps such data in an “unencrypted” computer database and then becomes aware of a “breach of security” involving unauthorized disclosure of that data. It is likely that California courts or the California Attorney General will assert jurisdiction to enforce this law not only with respect to databases physically kept in California but to any databases that include information on California residents.

Most companies find it burdensome and embarrassing to provide such notices of security breaches. These incidents are almost inevitably publicized either because the company must try to reach at least some of the affected individuals through the media or because some of those receiving notices in the mail leak them to the media. Many businesses are reacting by both restricting the instances where relevant data are kept and “encrypting” them where they must keep that data. (The statute does not define “encryption,” so there is no mandated standard technique or level of encryption so far.)

Many of the incidents listed in the ten pages of Appendix A are laptop security breaches that were reported largely because notice was required by California SB 1386.

Apart from a data disposal obligation (discussed below), before SB 1386 the California statutes, like those of other American states, had little to say about privacy protection measures in maintaining legitimate business records. The motivation behind SB 1386, according to Section 1 of the bill, was concern over the rise in identity theft because of the widespread collection of personal data in both the public and private sectors and particularly the risks involved to those whose Social Security numbers are misused by others.

Responding to those concerns, SB 1386 actually covers security breaches for a fairly narrow range of personal data. The “personal information” protected by the statute is only information that is not publicly available from government sources and that combines a person’s last name and either first name or first initial with either

- The person’s **Social Security number or driver’s license** number (or California non-driver’s ID number) or
- The person’s **credit or debit card or financial account number**, “in combination with” any security code, access code, or password required to access the account.

(See Cal. Civ. Code §1798.82(e) and (f).)

Breaches of “the security of a system” are defined as “unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.” (§1798.82(d))

Any person that “conducts business in California” and owns or licenses computerized data that includes personal information is obligated to provide **notice of a security breach to any California resident** whose unencrypted personal information is believed to have been acquired by an unauthorized person. “The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system” (§1798.82(a)). If the business maintains data owned or leased by a third party, it must notify the owner or licensee of a security breach “immediately following discovery” (§1798.82(b)). Notification may be delayed if a law enforcement agency determines that it will “impede a criminal investigation” (§1798.82(c)).

Notice can be written or electronic. If more than 500,000 people are involved, or the cost of individual notice would exceed \$250,000, “substitute notice” can be made by emailing those for whom the business has email addresses and then publicizing the event on a website or in “major statewide media” (§1798.82(g)).

**More than 30 other states** and the City of New York have since adopted a variation of California’s SB 1386. Some of the state laws cover additional kinds of information used in identity theft, such as birth date, mother’s maiden name, or employee numbers. Some require notice to law enforcement or consumer protection authorities in addition to the affected individuals, and some set standards for “timely” notice (48 hours in the most extreme case).

Several **federal bills** have also been proposed that would similarly require breach notice, partly in an attempt to create a single national rule rather than many differing state rules.

Importantly, all of the statutes and bills so far require notice only when **unencrypted** data are exposed, or encrypted data accompanied by a decryption key. Thus, the ability to ensure that all data on a laptop hard drive are **encrypted**, and to use **secure authentication** and **remote administration** tools to control access to protected data, monitor relevant hardware and software changes, and delete data on the hard drive if necessary, would greatly reduce an organization’s exposure to security breach notice laws, as well as reducing the likelihood of injury to any person resulting from a lost or stolen laptop.

#### *Data Disposal Laws*

At the federal level, FACTA addresses data disposal in the context of consumer reports, as discussed above in the section on “FCRA and FACTA,” and GLBA and HIPAA security rules address the destruction of financial and medical records, respectively. In addition, several state laws require the proper disposal of sensitive personal information, particularly Social Security numbers and payment card details. The broadest legal obligation in this area is found in California law.

As noted in the California Legislative Counsel's Digest to SB 1386, the California Civil Code (§1798.81) already required companies, as a protective measure, to **destroy business records** containing personal information when the company decides it no longer needs to retain them:

“A business shall take all reasonable steps to destroy, or arrange for the destruction of a customer's records within its custody or control containing personal information which is no longer to be retained by the business by (1) shredding, (2) erasing, or (3) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.”

“Customers” are defined as those who provide personal information for the purpose of obtaining goods or services from a business. “Records” covers all media but does not include publicly available directories with information voluntarily provided by the individual for public listing, such as basic contact information.

This **data destruction** requirement, which has parallels (with more limited scope) in the laws of several other states, such as Colorado and Nevada, is notoriously hard to manage with data distributed on laptops. **Remote administration** software offers a solution to this compliance issue.

### *Beyond Notice and Disposal*

California's “**Personal Information Security**” law (**AB 1950**) came into effect on January 1, 2005<sup>13</sup>. Going beyond the “notice” requirements of the Security Breach Notice Law, this statute affirmatively requires businesses to use “**reasonable security**” procedures “appropriate to the nature of the information” to protect personal information from “unauthorized access, destruction, use, modification, or disclosure” (§1798.81.5(b)), and to **contractually require third parties to do the same** (§1798.81.5(c)).

The “personal information” covered by the law (§1798.81.5(d)) is a last name and first name or initial associated with any of the following (unless the name or the additional data elements are “**encrypted or redacted**”):

- The person's **Social Security number or driver's license number** (or California non-driver's ID number) or
- The person's **credit or debit card or financial account number**, “in combination with” any security code, access code, or password required to access the account.
- Medical information (defined as “any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional.”)

“Personal information” does not include “publicly available information that is lawfully made available to the general public from federal, state, or local government records” (§1798.81.5(d)(3)).

The law does not apply to businesses to the extent that they are subject to certain other information security laws (HIPAA, California medical and financial privacy statutes, any other laws that provide greater privacy protection) (§1798.81.5(e)).

California's Office of Privacy Protection has recently published guidance specifically on the subject of “Recommended Practices on Protecting the Confidentiality of Social Security Numbers” (April 2007), which includes **encryption** on page 11:

“Protect records containing Social Security numbers, including backups, during storage by encrypting the numbers in electronic records or storing records in other media in locked cabinets.”

<sup>13</sup> See [www.leginfo.ca.gov/pub/bill/asm/ab\\_1901-1950/ab\\_1950\\_bill\\_20040929\\_chaptered.html](http://www.leginfo.ca.gov/pub/bill/asm/ab_1901-1950/ab_1950_bill_20040929_chaptered.html), codified at §§1798.80-1798.84 of the California Civil Code.

<sup>14</sup> See [www.privacy.ca.gov/recommendations/ssnrecommendations.pdf](http://www.privacy.ca.gov/recommendations/ssnrecommendations.pdf)

**At least six other states** have already adopted personal information security requirements in the same acts incorporating security breach notice obligations, while others are considering separate legislation. At the same time, **federal bills** are under consideration that would impose security obligations on at least some kinds of companies (so-called “data brokers”) that collect and sell large amounts of consumer data but are not regulated under FCRA as consumer reporting agencies.

In addition, the financial services industry has been pressing for legislation requiring **merchants to compensate banks** and payment card issuers when a merchant’s security failure results in costs relating to investigation, consumer notices, and reissuing payment cards. Such legislation has already been adopted in Minnesota, awaits the governor’s signature in California, and is under consideration in Texas, Massachusetts, and elsewhere.

As with other legislation that refers to “reasonable” security measures, such laws make it imperative for enterprises to establish that they have assessed the risks involved with the kind of personal data they handle, including the obvious risks of holding such data on laptops. Laptop encryption, authentication, and remote administration software would likely be deemed “reasonable” and cost-effective means of protecting covered data in any of the jurisdictions that have enacted laws protecting sensitive categories of information and establishing rules for notice and liability.

### *Evidence*

In the United States (and, indeed, in most jurisdictions), it is critical for an enterprise faced with an administrative, civil, or criminal investigation or complaint to be able to establish not only that it made reasonable choices on how to protect the data at issue but also that those choices were implemented. Many organizations have felt compelled to announce security breaches, provide insurance or compensation, or negotiate settlements with the government or with private litigants simply because they could not be sure what protection was both available and actually used on a specific laptop or other device that was lost, stolen, or accessed without authorization.

In most legal contexts, the question would be posed somewhat like this: Is it probable (more likely than not) that the data at issue could not be accessed by an unauthorized person?

In the United States, the GLBA financial privacy regulations are even stricter, requiring notice to consumers whenever there is a “reasonable possibility” that protected financial data will be “misused.” Some states (such as Michigan) also expressly require notice of a security breach involving protected data even if it was encrypted, if there is “reason to believe” that the decryption key has been compromised. Law enforcement agencies and litigants in other states might well advance the same argument. Auditors examining the effectiveness of internal risk management controls may also test for indications that routine policies and procedures for encryption and authentication are not always followed, thus potentially exposing the organization to a material risk.

Thus, the first step in defending an organization would be to demonstrate that its chosen encryption and authentication or other access controls are considered effective, for example, by reference to government and industry standards and practices. The second step is to show that, more likely than not, the data at issue were encrypted and the access controls were in operation when the laptop went missing.

The organization can create a presumption in its favor by establishing through witnesses or business records its regular business practice of installing and employing encryption and authentication controls. If these controls are entirely dependent on affirmative actions by a user or network administrator, however, it may not be hard for a skeptical regulator or opposing counsel to challenge that presumption by getting a witness to admit that there were sometimes lapses or exceptions. Thus, **automatic full-disk encryption**, regularly checked and managed by **remote administration tools**, can create a much stronger presumption that the controls routinely required by the organization were in fact used on the laptop in question – particularly where the software has been configured to prevent local control over encryption and authentication. Further, a central log of the checks performed by remote administration software can establish when the laptop was most recently examined on connection to the network, as well as the status of encryption and authentication tools on the laptop at that time. This would be far more persuasive in a legal proceeding than simply an indication that the laptop had such tools available for the user when it was first deployed.

## Canada

The federal Personal Information Protection and Electronic Documents Act (“**PIPEDA**”), was enacted in 2000 and came fully into effect on January 1, 2004<sup>15</sup>.

PIPEDA lays down privacy principles that apply directly to federally regulated sectors (such as banking, railways, and air transport) and the territories, as well as to inter-provincial and international commercial transactions. These principles are also increasingly reflected in provincial laws that cover non-federally regulated employment and consumer relations and provincial government operations; such laws have been enacted so far in Alberta, British Columbia, and Quebec. The principles include an obligation to maintain the security of personal information.

PIPEDA § 5(1) requires covered organizations to comply with the obligations detailed in Schedule 1, which reproduces the **Model Code** for the Protection of Personal Information, a standard adopted by the **Canadian Standards Association** (CAN/CSA-Q830-96). Thus, the originally voluntary CSA privacy principles are incorporated by reference in both federal and provincial legislation, becoming an expression of legally binding obligations.

Principle 7 (§ 4.7) of the CSA standard (and therefore of PIPEDA Schedule 1 and analogous provincial measures) restates the familiar principle of proportionality: personal information “shall be protected by **security safeguards appropriate to the sensitivity of the information.**” Unlike the EU Directive, PIPEDA does not define categories of sensitive information, observing in §4.3.4 that sensitivity depends on context, but that same section also says that personal medical and income information are normally considered “sensitive” and require greater care.

The standard offers some additional instruction on information security:

- Security safeguards must protect information against loss or theft, as well as against unauthorized access, alteration, or disclosure, and safeguards should apply “regardless of the format” in which information is held (§ 4.7.1).
- Security safeguards must be adapted to the sensitivity of the information, its volume, distribution, and format, and the method of storage (§ 4.7.2).
- Safeguards should include the following (§ 4.7.3):
  - (a) “physical measures, for example, locked filing cabinets and restricted access to offices;”
  - (b) “organizational measures, for example, security clearances and limiting access on a ‘need-to-know’ basis;” and
  - (c) “technological measures, for example, the use of passwords and **encryption.**” (Emphasis added.)
- Organizations must train their employees to maintain the confidentiality of personal information (§ 4.7.4).
- Care must be taken in the disposal of personal information to prevent unauthorized disclosures (§ 4.7.5).

So far, the federal and provincial legislatures have not adopted security breach notice requirements as have most of the US states. However, the Federal and Ontario privacy commissioners have indicated that security breaches may fall under the heading of material disclosures generally required of those who handle sensitive personal information.

As in the United States, Canadian financial services regulation also requires risk assessment and risk mitigation, and these principles are applied to information security practices designed to protect the safety and soundness of financial institutions, as well as to protect their customers.

Ontario Bill 198 and new rules adopted by securities regulators in nearly all of the provinces emphasize corporate internal controls, similar to SOX in the United States. As in the US, this has raised the profile of corporate information management and security functions and required further documentation of security policies and risk assessment. In many companies, those would appropriately include laptop security risks and countermeasures.

<sup>15</sup> The statute is available from the Federal Privacy Commission website at [www.privcom.gc.ca/legislation/02\\_06\\_01\\_01\\_e.asp](http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp)

## Europe

All of the 27 Member States of the European Union, the three additional members of the European Economic Association (Norway, Iceland, and Lichtenstein) and several other European nations that trade heavily with the EU, such as Switzerland, have transposed the **EU Data Protection Directive** into national law. The EU Data Protection Directive includes very general security obligations to protect personally identifiable information.

Most countries have provided little additional guidance. Increasingly, however, companies are required to have a written security policy and make it available on request to the authorities, and some countries have articulated more detailed security requirements or guidance, as summarized below. In **Germany, France, the Netherlands, and Sweden**, companies may (or must) appoint an internal data protection officer who is typically responsible, among other things, for ensuring that the company has an updated security policy that protects personal data and makes a summary of that policy available on request to the data protection authorities and to other interested persons.

Thus, there is an increasing emphasis on risk assessment and documented risk management measures, under data protection law. At the same time, **SOX-like legislation and regulations** are pushing European public companies to document risk assessments and internal controls over information security, and **financial institutions**, in particular, are under pressure to do the same from their sectoral regulators.

Here is a summary of these developments, to the extent that they are relevant to laptop security, at European level, followed by reports on any additional or unique requirements at national level.

### *EU Eighth Company Law Directive*

The 2006 revision of the 1984 **Eighth Directive on Company Law**, which is to be transposed into national laws by 2008, reflects the current state of harmonization in auditing and financial disclosure requirements for public companies in Europe, which still permits considerable variation from country to country. It is sometimes called "E-SOX," since it has many of the same aims and features as the American SOX legislation (see the "Sarbanes-Oxley" section of this report, above), prominently including greater accountability for establishing and operating an internal control system. The European version is not as rigorous as SOX and does not entail the same degree of management and audit verification of internal controls as is found in SOX sec. 404.

Nevertheless, companies listed on European stock exchanges are under similar pressure as in the United States to conduct risk assessments and document effective control measures. For many of them, laptop risks are material and should be factored into their information security controls.

### *Basel II and Solvency II*

Banks operating in any of the "Group of Ten" countries (Belgium, Canada, France, Germany, Italy, Japan, the Netherlands, Sweden, Switzerland, the United Kingdom, and the United States), are typically subject to risk management and internal control requirements under banking regulations. The Group of Ten adopted a new framework for capital adequacy regulation in 2004, the "**Basel II**" accord, which was to be implemented in national bank supervisory practice by the end of 2006.

Basel II requires an independent review of internal control structures, including risk management controls, a method for monitoring compliance with internal policies, and verification of the effectiveness of internal controls in ensuring the prudent conduct of banking business (sections 744, 745). Basel II also provides for the periodic assessment of the quality of information systems and reporting and management's record in responding to emerging or changing risks. Bank management and government supervisors are to determine the appropriate level of capital to be retained based on the risk profile and the effectiveness of internal risk management controls in a banking group. Thus, Basel II emphasizes the need for banks to use an internal control system to manage risks, potentially including laptop risks.

The European Commission recognizes that the banking and insurance industries overlap, and with its "**Solvency II**" initiative, it is seeking to harmonize insurance regulation across Europe with Basel II. This would include an emphasis on internal controls and risk management procedures in the insurance industry as in banking.

Many global companies based in, or operating from, the EU find it efficient to apply throughout the EU the same approach to internal controls that they employ in the US, which is most commonly based on the COSO and CobiT Frameworks discussed above in the section on “Sarbanes-Oxley.” In addition, they increasingly look to international standards and recommendations such as ISO 17799 / 27002 and ITIL (discussed below in the section on “International Security Standards”) to implement information security controls.

### *EU Data Protection Directive*

The EU Data Protection Directive addresses security for personally identifiable data in Article 17:

"Article 17, Security of processing

"1. Member States shall provide that the controller [the person or entity that decides to process personal data] must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

"Having regard to the state-of-the-art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

"2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect to the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

"3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller “

Thus, the Directive mandates that the data controller must implement **appropriate technical and organizational measures** to protect personal data (the latter specifically including unauthorized access when the data are available over a network), and indeed against all unlawful forms of "processing." The "appropriate" level of security must be determined with reference to the nature of the data and the risks presented by the particular kind of processing involved. Consequently, countries implementing the Directive have in some cases specified higher security levels for "risky" operations such as consumer reporting, payment processing, and more sensitive categories of data such as health records and information about race or ethnicity.

Note that the Directive (Article 6(e)) also requires data disposal when the data are no longer needed for a legitimate purpose.

The “Article 29 Data Protection Working Party” established by the Directive (comprised of data protection authorities from the European Commission and each of the Member States) has, on occasion, examined privacy-enhancing technologies from the perspective of meeting the objectives of Article 17. One of its Working Documents, concerning the Trusted Platform Module (TPM) specifications produced by the Trusted Computing Group, includes relevant comments on the security of laptops and other mobile devices<sup>17</sup>. The Working Party stated the challenge of trusted computing succinctly:

“The concept of trusted computing platforms originates from the computer industry’s observation that the current personal computer model is not conducive to guaranteeing security, as demonstrated by virus attacks, the possibility of spying on data being input, pirating of software and works of art, etc.” (Working Document, at 2)

The Working Party observed that technological solutions are needed to address issues of “ownership, integrity, and, where necessary, confidentiality of intangible goods, and to controlling their use in terms of both software and hardware” (id.). One aim, according to the Working Party should be to use dedicated chips or **cryptography** to create “individual digital safes” (id. at 2-3).

<sup>17</sup> See “Working Document on Trusted Computing Platforms and in Particular on the Work Done by the Trusted Computing Group (TCG Group),” WP86 (the “Working Document”) (January 23, 2004), [http://europa.eu.int/comm/internal\\_market/privacy/docs/wpdocs/2004/wp86\\_en.pdf](http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp86_en.pdf)

The Seagate / Wave FDE solutions, as described further below, offer precisely that possibility, furthering privacy interests as well as organizational security interests.

### *United Kingdom*

The 2006 Combined Code on Corporate Governance published by the Financial Reporting Council emphasizes internal control systems to manage known risks, and many UK companies are already directly or indirectly affected by the US SOX legislation and SEC regulations that require a control framework and systematic risk assessment, as discussed in the “Sarbanes-Oxley” section above. With the spate of recent laptop security breaches in the UK, it is likely that laptop security will assume a higher profile in such assessments. The Financial Services Authority and the Bank of England are similarly requiring regulated financial institutions to document their information management and security practices.

The UK Office of the Information Commissioner (OIC) has offered few details on what it considers to be required security measures under the UK Data Protection Act, but it does encourage conformance to the BS 7799 information security management standard, which is essentially identical to ISO 17799 / 27002, discussed below in the section on “Information Security Standards.”

The OIC’s current registration form for data controllers includes the question, “Have you taken any measures to guard against unauthorized or unlawful processing of personal data and against accidental loss, destruction or damage?” There are then several yes/no questions, asking if the security measures include the following:

- Adopting an information security policy,
- Taking steps to control security,
- Putting controls on access to information in place,
- Establishing a business continuity plan,
- Training your staff on security systems and procedures,
- Detecting and investigating breaches of security when they occur,
- Adopting the British Standard on Information Security Management BS7799.

The form does not indicate that these are all mandatory elements for providing adequate security, although their presence suggests that the OIC considers them important.

In enforcing the UK Data Protection Act, the Office of the Information Commissioner found in March 2007 that eleven banks did not dispose of customer data properly and required them to sign undertakings to comply with the Act; failure to meet the obligations of such an undertaking can lead to fines or criminal prosecution. As mentioned elsewhere in this report, **remote administration** tools can figure in ensuring that data are properly deleted from laptops.

On July 11, 2007, the Information Commissioner released OIC’s annual report with an indictment of information security practices in many UK firms and agencies, specifically referring to **unencrypted laptops**<sup>18</sup>:

“Over the last year we have seen far too many careless and inexcusable breaches of people’s personal information. The roll call of banks, retailers, government departments, public bodies, and other organizations, which have admitted serious security lapses, is frankly horrifying.

**“How can laptops holding details of customer accounts be used away from the office without strong encryption? How can millions of store cards fall into the wrong hands?”**  
(Emphasis added.)

<sup>18</sup> See press OIC release available online at [www.ico.gov.uk/upload/documents/pressreleases/2007/annual\\_report\\_press\\_releases\\_110707004.pdf](http://www.ico.gov.uk/upload/documents/pressreleases/2007/annual_report_press_releases_110707004.pdf)

The Commissioner promised more rigorous enforcement action if companies do not improve in these areas. Thus, in the UK, organizations are on notice that unencrypted data on laptops may lead to public denunciation and official sanctions.

### *Germany*

The German Company Law was amended in 2002 to include a SOX-like emphasis on internal controls and risk assessment in public companies. This is reinforced by the 2006 version of the German Corporate Governance Code (the “Cromme Code”) and by parallel initiatives in financial regulation.

German data protection law (a federal statute mirrored in state acts) in most instances requires data controllers other than very small business to appoint an internal data protection officer with statutory responsibilities that include examining the security of personal data handled by the organization. A national professional association aids data protection officers in this task, and there is an increasing emphasis on conformance to standards, prominently ISO 17799 / 27002 (discussed below in the section on “Information Security Standards”).

### *France*

France adopted a Financial Security Law of 2003 that has many requirements similar to those found in SOX, including internal controls based on risk assessments. Banking regulators also look to such controls in the financial institutions they supervise, as contemplated by Basel II (see above).

The security provisions of French data protection law are based on Article 17 of the EU Data Protection Directive, with little additional guidance or regulation. France has recently adopted legislation that streamlines the data privacy notification obligations for many controllers, and it now allows the German-style option of appointing an internal data protection officer, who must oversee data protection practices including security. The notification form for data controllers that do register with CNIL, the national data protection authority, includes a question on “Security and Confidentiality,” requiring “yes/no” answers to the following simple questions:

- Are access controls in place for each application?
- Have you adopted measures to prevent intrusions into your network?
- Is the data itself subject to any particular form of protection (such as anonymisation or **encryption**)? (Emphasis added.)

CNIL may ask for further details, depending on its assessment of the volume and risk involved in the organization’s processing of personal information.

### *Italy*

Italy adopted SOX-like legislation elevating the role of internal controls in company management and audits, including controls over information security risks, even before the recent amendments to the EU Eighth Company Law Directive (see above). Financial regulators also increasingly examine information security risks (see discussion above on “Basel II”).

The Personal Data Protection Code (2003), which is the most recent codification of Italian law implementing the EU Data Protection Directive, took effect in 2004. It is more specific about security measures than is typical in European countries with laws based on the EU Directive.

The Code requires an organization that controls personal data to draft and annually update (by March 31 of each year) a written **security policy** with respect to the processing of **sensitive personal data** (defined as in

<sup>7</sup> Text available at [www.occ.treas.gov/consumer/Customernoticeguidance.pdf](http://www.occ.treas.gov/consumer/Customernoticeguidance.pdf)

the Directive to denote information relating to race and ethnicity, health and sexual life, religious and philosophical beliefs, political and trade union activity). The security policy must contain the following:

- a description of the company's processing operations that involve sensitive personal data;
- a description of the departments and staff with responsibility for the processing of sensitive data;
- an analysis of the risks associated with the processing of the data;
- a description of the company's security measures with respect to sensitive data;
- a description of the company's data recovery system (that is, the system in place for recovering data in the event of destruction or damage);
- a description of the company's staff training measures with respect to the handling of sensitive personal data, and
- a description of the security measures the company employs when outsourcing sensitive employee data processing to external contractors.

Additional specific measures apply to any database of biometric identification data or data from geographic location systems (such as GPS or RFID).

The annual risk assessments and updated security measures should, in many cases, take into account laptop security risks and countermeasures, such as **encryption**.

### *Spain*

Spanish corporate law is relatively less developed on internal controls at present but will be enhanced with the transposition, by 2008, of the EU Eighth Company Law Directive (see above). Spanish financial regulators regularly examine the security controls of financial institutions, as contemplated by the Basel II accord (see above).

The Spanish Data Protection Agency (AEPD) has developed relatively detailed security regulations to protect personal data. The registration form that data controllers must submit to the agency requires that one of three boxes be checked, indicating whether the security measures adopted for a given information system are of a "basic," "medium," or "high" level. The Instructions that accompany the notification form explain that sensitive data (information revealing race or ethnicity, health or sexual life, religious or philosophical beliefs, or political or trade union activity) must be protected at a "high" level of security; financial and credit information must be handled with a "medium" level of security, and all other personal data must receive at least "basic" protection.

These levels of protection are defined in Royal Decree 994/1999 (June 11, 1999) approving a Regulation on Mandatory Security Measures for Computer Files That Contain Personal Data. An unofficial English translation is available on the AEPD website at [https://www.agpd.es/upload/reglamento\\_ingles\\_pdf.pdf](https://www.agpd.es/upload/reglamento_ingles_pdf.pdf). The Regulation requires the following for a basic level of security:

- a written security policy and procedures document,
- defined staff responsibilities for security and appropriate training,
- a record of security incidents and consequences,
- identification and authentication procedures for authorized users, including controls on password assignment, storage, and validity,
- access limitation to data required for an employee to perform his or her duties,
- management of data storage media (to be kept only at locations with restricted access and removed only with approval),
- backup and recovery procedures (including at least weekly backups of any files that are updated).

Medium-level security involves the following additional measures:

- the security document must identify the officer(s) responsible for security, procedures for periodic checks to monitor compliance, and procedures for disposing of or reusing storage media,
- appointment of security officer(s),
- internal or external audits conducted at least biennially,
- greater access controls (“unequivocal” identification of persons attempting to access the information system, with a check for current authorization, limits on the number of access attempts, access to physical premises restricted to authorized users),
- more detailed media management (incoming and outgoing media logs, measures to prevent retrieval of data from discarded or reused media, procedures for protecting data from unauthorized retrieval when media are removed from the premises),
- adding to the incident records any data recovery activities, which must be authorized in writing,
- no testing with real data unless it is subject to basic, medium, or high-level security measures, according to the level of security mandated for the data in question.

High-level security adds the following to the basic and medium-level protections:

- **encryption** is required when distributing personal data in any medium; data cannot be transmitted over telecommunications networks without a mechanism to make them unintelligible to third parties and prevent unauthorized manipulation of the data,
- access records must be more detailed, with the user’s identity, data and time of access, files accessed, type of access, and whether access requests were authorized or denied; identification of each record accessed,
- no possibility of deactivating access recording,
- access records must be kept at least two years,
- periodic monitoring of access controls by a security officer; monthly reports on access controls and any problems detected,
- backup and recovery media must be kept at a different location.

Laptop **encryption, authentication, and remote administration** would help organizations comply with the requirements for encryption, access controls, and access records.

### ***Belgium***

Belgium is strengthening internal control requirements for publicly traded companies and regulated financial institutions consistent with the EU Eighth Company Law Directive and Basel II, respectively (see above). As in the UK, the Belgian data protection registration form requires the registrant to provide certain disclosures (which are then made publicly available) about a registrant’s security practices. These include:

- Contractual guarantees by third-party recipients of personal data.
- Technical measures such as **encryption** and passwords.
- General notices to affected individuals about the registrant’s security practices.

<sup>6</sup> Title V - Privacy, §§ 501 et seq., Pub. L. 106-102 (1999), codified at 15 USC §§ 6801-6809, “Disclosure of Nonpublic Personal Information,” text available online at <[http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106\\_cong\\_public\\_laws&docid=f:publ102.106](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ102.106)>

In addition, the registration form requires the company to check the applicable boxes in a list of possible security measures, as follows:

- Security service,
- Security consultant,
- Security plan,
- Disaster recovery plan,
- Other organizational measures (describe),
- Risk analysis,
- Risk prevention measures,
- Backup system,
- Procedures to respond to fire, flood, or intrusion,
- Security measures for buildings, sites, and equipment,
- Secure access to information systems,
- Authentication procedures,
- Log-on procedures,
- Other technical security measures (describe),
- Contractual safeguards with employees,
- Contractual safeguards with processors,
- Code of conduct (indicate which codes of conduct apply),
- List of persons authorized to access health-related or other sensitive information data and information concerning judicial actions or proceedings (and if so, the name, address, telephone, fax, and email of the contact person in case the Commission wishes to review this list),
- Contact information in case the Commission wishes to review written consents to process health-related or other sensitive information.

Thus, a data controller in Belgium is encouraged to disclose his/her use of security measures such as **encryption**, but the legal obligation is simply to adopt appropriate technical and organizational security measures, as stated in Article 17 of the EU Data Protection Directive.

### *Switzerland*

Swiss financial regulation is still more secretive than in other countries, and Switzerland has not adopted SOX-like legislation. However, the voluntary Swiss Code of Best Practice for Corporate Governance does speak of internal control systems, and Swiss corporate practice increasingly tends to reflect of the EU, involving more documentation of risk assessment and more attention to information security risks in many companies.

The Swiss Federal Act on Data Protection of 1992 was based on an early draft of what became the EU Data Protection Directive, even though Switzerland is not a member. Thus, it is very close in language, structure, and principles to the data protection laws enacted by the EU Member States, including security provisions similar to those found in Article 17 of the EU Directive as discussed above<sup>19</sup>.

<sup>19</sup> An English version of the Act is available at the website maintained by the Swiss Federal Data Protection Commissioner at [www.edsb.ch/e/gesetz/schweiz/act.htm](http://www.edsb.ch/e/gesetz/schweiz/act.htm). Although Switzerland is not a member of the European Union, the federal legislature determined that it was important for Swiss law to conform to the model of the Directive. The European Commission has since ruled that the Swiss law provides an adequate level of protection for personal data, so personal data are allowed to flow freely between Switzerland and the EU.

The Federal Data Protection Commissioner's 2002 Annual Report included an opinion on transborder data flows in the context of "Disclosure of Employee Data outside Switzerland," which is available online (in English translation) at [www.edsb.ch/e/doku/jahresberichte/2002/disclosure.htm](http://www.edsb.ch/e/doku/jahresberichte/2002/disclosure.htm). The opinion notes that staff recruitment and "cost-effective wage management" would generally be considered legitimate reasons for transferring data abroad, particularly within a multinational corporate group. However, equivalent data protection must be "guaranteed on a contractual basis." Moreover, **security measures including encryption** "must" be in place:

"Appropriate technical and organisational measures must be used to protect transferred personal data from unauthorised processing. It is therefore recommended that special protective measures be put in place that take account of the classifications of the data categories involved. It must be guaranteed that unauthorised access to the infrastructure and to data carriers is at all times impossible. Likewise the unauthorised access of persons to personal data during their storage and transfer must be prevented by encrypting the data. The **encryption must reflect the latest technical advances**. This is applicable both to data and to data protection specifications. The identification of the persons authorised by the specifications to receive the data must be unambiguously and clearly guaranteed. The identification must be made using the latest technical advances. Data processing activities must be recorded so that they remain permanently reproducible." (Emphasis added.)

Thus, personal data from Switzerland downloaded to a laptop abroad, or carried out of the country, should, in principle, be **encrypted**.

### *Austria*

The Austrian Code of Corporate Governance (2006) does not detail internal control obligations directly implicating information management, but Austrian law will reflect the EU Eighth Company Law Directive by 2008. Austrian financial regulation includes the Basel II provisions on internal control systems (see above). The "DSG 2000," Austria's implementation of the EU Data Protection Directive, includes quite detailed security provisions in Part 3<sup>20</sup>.

Section 14 provides as follows:

"(1) Measures to ensure data security shall be taken by all organisational units of a controller [Auftraggeber] or processor [Dienstleister] that use data. Depending on the kind of data used, as well as the extent and purpose of the use, and considering the state of technical possibilities and economic justifiability, it shall be ensured that the data are protected against accidental or intentional destruction or loss, that they are properly used and are not accessible to unauthorised persons."

Section 14(2) requires a documented security organization and policy, training for staff, physical access controls, controls on access to data and programs, device security, and logs of processing, access, unauthorized access attempts, and modifications (to be retained for three years).

Where registration is required, the data protection authority requires data controllers to attach a General Description of Data Security Measures. This form requires a "yes" or "no" response to each of the following statements:

1. Data processing tasks are expressly assigned to designated organizational units and personnel.
2. Use of the data is restricted to authorized organizational units and personnel.
3. Relevant personnel are trained concerning the organization's internal security procedures and the data controller's obligations under DSG 2000 (the Austrian data protection act).
4. There are measures to prevent unauthorized access to the physical premises where data are processed.

<sup>20</sup> An English version of the text is available online at <http://www.dsk.gv.at/dsg2000e.pdf>

5. There are measures to control access to the data processing programs and stored data.
6. Data processing devices must be authorized before they can be initiated.
7. The data controller keeps records of procedures, changes, inquiries, and data transmissions, so that the validity of an operation can be verified.
8. Evidence is preserved to establish compliance with the above measures.
9. (Describe other security measures).

Laptop **encryption, authentication, and remote administration** would be a means of satisfying the concerns reflected in items 5 and 7.

### *Norway*

The Norwegian Code of Practice for Corporate Governance (2006) addresses risk management and internal controls, much as does the EU Eighth Company Law Directive (see above).

The Personal Data Regulations (December 2000)<sup>21</sup> include a lengthy section on “Data Security” in Chapter 2. They establish a “proportionality” test for reasonable security measures following a **mandatory risk assessment and written security plan**. “Regular” security audits are required and responsible persons must be identified. **Encryption** is generally required for electronic transmission of personal data and the data must be erased when no longer needed for its original purpose. The regulations also call for access controls, backup and disaster recovery facilities, precautions against “malicious software,” internal compliance controls, and contractual obligations on vendors. Many of these requirements can be facilitated, with regard to laptops, by **remote administration tools**.

### **Australia**

The 2003 “Principles of Good Corporate Governance and Best Practice Recommendations” promulgated by ASX (the Australian Stock Exchange) include a SOX-like emphasis on internal controls, which is reinforced by 2004 legislation. These are also featured in Australian financial services regulation, with more specific emphasis on information security controls.

The Federal Privacy Act 1988 applies to Commonwealth government agencies; some of the Australian states have similar legislation. The federal act includes ten National Privacy Principles (“NPP”). The Privacy Amendment (Private Sector) Act 2000 extended the NPP to businesses with more than AUS \$3 million in annual revenues, some small businesses, and all health services providers (but the law does not cover privacy in employment). Some state laws further extend privacy protection in particular sectors or activities. Principle 4 of the NPP, “Data security,” consists of two sentences:

“4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

“4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2.”

Thus, techniques such as laptop **encryption** that protect against unauthorized access are consistent with the NPP, as are techniques such as **authentication** and **remote administration** of laptops that control access and facilitate remote deletion of data.

The Federal Privacy Commissioner’s 2001 “Guidelines to the National Privacy Principles”<sup>22</sup> highlights the need for risk assessment based on the sensitivity of the data and the likelihood of harm if it is compromised. The Guidelines encourage Australian organizations to look to international standards as a guide (see “International Security Standards,” below).

<sup>21</sup> Available in English at [http://www.datatilsynet.no/dtweb/attachment/1573/POF\\_eng.pdf](http://www.datatilsynet.no/dtweb/attachment/1573/POF_eng.pdf)

<sup>22</sup> See [www.privacy.gov.au/publications/nppg1\\_01.html#npp41](http://www.privacy.gov.au/publications/nppg1_01.html#npp41)

## Japan

“J-SOX,” the 2003 amendments to company law in Japan, and 2006 revisions of Japanese securities laws are aimed at SOX-like reforms in Corporate audit and internal governance. As in the US, this has focused more attention on risk management and internal controls, including information management and security risks. Regulations of the Ministry of Finance impose information security requirements on regulated financial institutions, which generally require risk assessments and appropriate risk mitigation and incident response measures.

Article 20 (“Security Control Measures”) of Japan’s Personal Information Protection Act provides simply as follows:

“An entity handling personal information must take necessary and proper measures for the prevention of leakage, loss, or damage, and for other control of security of the personal data.”

This “necessary and proper” standard has not yet been elaborated by any of the responsible ministries. However, in May 2005, Japan’s Financial Supervisory Agency issued a public warning to Michinoku Bank after it lost compact disks including data on 1.3 million customers, resulting in the resignation of the Bank’s senior executive officers. Thus, unencrypted data on a lost or stolen laptop is unlikely to be deemed consistent with the “necessary and proper” standard for information security.

Two more recent incidents have elevated regulatory scrutiny of bank information security practices. In October 2006, the Bank of Tokyo – Mitsubishi announced that financial records on 960,000 customers had possibly been compromised. And in July 2007 Resona bank disclosed that records of branch and ATM transactions affecting 980,000 customers were simply missing.

As a result of these incidents and several other well-publicized security breaches involving personal data held by employers, retailers, and government agencies, Japanese ministries, charged with enforcing the Personal Information Privacy Act in their respective sectors, are reportedly considering security and breach notice rules more or less on the California model.

## Singapore

The Code of Corporate Governance published by the Ministry of Finance in 2005 provides for internal control systems, including risk management controls and compliance controls, and an annual audit of their effectiveness. Financial regulators examine the internal controls of financial institutions, including their known security risks and planned countermeasures. Thus, Singapore has followed much of the spirit of SOX and Basel II (see above).

Government regulations require or recommend conformance with ISO 17799 / 27002 (see the section on “Information Security Standards” below) by financial services and e-commerce businesses.

There is no comprehensive data protection law in Singapore as there is in Europe, Japan, and Hong Kong. The Ministry of Finance enforces laws on the confidentiality of financial information. There is a self-regulatory E-Commerce Code for the Protection of Personal Information and Communications of Consumers of Internet Commerce, as well as a voluntary 2002 Model Data Protection Code; neither is very specific about security requirements, but measures such as laptop **encryption** and **secure authentication** would further the objective of ensuring confidentiality.

## Korea

The Republic of Korea has not, to date, adopted SOX-like audit and corporate governance legislation. Korea’s Financial Supervisory Service does not appear to have provided a great deal of guidance on information security issues.

Korea's Constitution provides explicit protection of privacy in Articles 16-18, and the government has endorsed the OECD Privacy Guidelines<sup>23</sup>. There is no comprehensive data protection law. Rather, as in the United States, there are laws regulating government uses of personal information and sectoral privacy legislation in particular fields: the 1994 *Act on the Protection of Personal Information Managed by Public Agencies*, the 1995 *Act Relating to Use and Protection of Credit Information*, the 1996 *Act on Disclosure of Information by Public Agencies*, and the 1999 *Basic Act on Electronic Commerce*.

These laws include an obligation on the part of data holders to maintain the security of personal information, which is not detailed in regulations or legal precedents. Certainly, laptop **encryption** could be one means of satisfying the obligation of security, along with access controls including **authentication**.

## Information Security Standards and Best Practices

In addition to information management controls (prominently under the COSO and CobiT Frameworks discussed above in connection with Sarbanes-Oxley compliance in the United States), many organizations design security policies and procedures around widely accepted information security standards or best-practice recommendations. Even if these are not mandated by law or contract, they are extremely useful in devising an effective security program, and they may serve as evidence of industry custom and practice in assessing the “reasonableness” of an organization’s practices, if the organization finds itself in court or responding to a governmental investigation of a laptop security breach. Not surprisingly, **encryption** is commonly addressed in such standards and recommendations, as well as, several controls that can be achieved in laptops by using **secure authentication** and **remote administration** tools.

### *OECD Information Security Guidelines*

The Organisation for Economic Co-Operation and Development (OECD) adopted Information Security Guidelines in 2002. These represent an international consensus on the necessary elements of database and network security<sup>24</sup>. The Guidelines, which influence legislation and regulations in the 30 OECD member states and the 70 other countries that have cooperation arrangements with OECD, focus on process rather than technique. They recommend that governments and private organizations promote a “culture of security” by implementing nine principles:

1. **Awareness** (education and training concerning security risks and countermeasures).
2. **Responsibility** (accountability for use of information systems and networks; responsibility for furnishing or using updated software and related products).
3. **Response** (timely efforts to prevent, detect, and respond to security incidents; sharing information about threats and vulnerabilities; cooperating in responding to network-wide security incidents).
4. **Ethics** (respect for the legitimate interests of others, including privacy and the risk of injury to other persons and organizations).
5. **Democracy** (security measures compatible with the freedom and confidentiality of communication, openness in business and government, and the appropriate protection of personal information).
6. **Risk assessment** (conducting periodic risk assessments to identify threats and vulnerabilities, including consideration of technological changes, physical and human factors, internal policies, and third-party products and services with security implications; determining appropriate levels of risk and control measures for the nature of the system and information at issue).
7. **Security design and implementation** (incorporating security in system design and operations, including safeguards against identified and emerging threats and vulnerabilities; technical and non-technical solutions proportionate to the value of the information on the organization’s systems and networks; security requirements included in purchasing and outsourcing, with products and services properly configured for the security needs of the organization).

<sup>23</sup> See [www.oecd.org/document/18/0,2340,en\\_2649\\_34255\\_1815186\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html)

<sup>24</sup> See Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (OECD Council Recommendation, 25 July 2002), available at [www.oecd.org/dataoecd/16/22/15582260.PPDF](http://www.oecd.org/dataoecd/16/22/15582260.PPDF)

8. **Security management** (dynamic and coordinated management based on risk assessment and evaluation of all aspects of the organization's operations, including forward-looking responses to emerging threats, means of prevention and detection, response procedures, systems recovery, ongoing maintenance, review and audit procedures).
9. **Reassessment** (review and reassess security needs periodically, making appropriate modifications to policies, practices, and measures, recognizing that information security threats evolve rapidly).

**Encryption** of sensitive data is consistent with the seventh and ninth principles, **secure authentication** supports the seventh principle, and **remote administration** tools could be used in connection with the second, third, seventh, and ninth principles.

### *ISO 17799 / 27002*

This is easily the best-known and most widely adopted international standard for information security processes. In the 1990s, the British Standards Institute developed a Code of Practice for Information Security Management, which is now Part A of the second edition of the **BS 7799** standard (BS 7799-1:1999). Part B (BS 7799-2:2002) is a more technically detailed Specification for Information Security Management Systems.

In 2000 the Code of Practice (BS 7799 Part A) was adopted essentially verbatim as an international standard, ISO/IEC 17799:2000 (usually called "**ISO 17799**") by ISO, the International Organization for Standardization (a United Nations body based in Geneva) and IEC, the International Electrotechnical Organization (a more specialized intergovernmental body also based in Geneva). The full text can be purchased from ISO<sup>25</sup> or from commercial sources.

ISO 17799 was updated in a **2005 version** (ISO/IEC 17799:2005) and supplemented with a new **ISO 27001** based on BS 7799 Part B (specifications for an Information Security Management System (ISMS) with guidance for use). Many companies assert conformance to ISO 17799 or 27001 or obtain certification of their ISMS under ISO 27001. The 2005 version of ISO 17799 expressly addresses privacy by referring to the security of personal data.

In 2007, ISO is **renumbering ISO 17799:2005 as ISO/IEC 27002**.

ISO 17799 / 27002 defines information security in terms of the now-familiar "C-I-A" acronym: **confidentiality** (limiting access to those authorized to access the protected information), **integrity** (ensuring accuracy and completeness of information and processing methods), and **availability** (ensuring access to information and information systems when required, including business continuity arrangements). Laptop encryption is a means of ensuring confidentiality, while **authentication** and **remote administration** tools may be used to promote confidentiality by controlling access and deleting data if necessary.

The ISO 17799 / 27002 elements of information security systems were taken into account in drafting the **CobIT** framework for information management controls. Thus, an ISO approach to information security can be mapped readily to the information management control objectives adopted by a company using the CobIT framework, in connection, for example, with a SOX audit.

ISO 17799:2005 / 27002 defines twelve elements of information security:

1. **Risk assessment** (evaluating and prioritizing the organization's security risks, on an ongoing basis).
2. **Security policy** (compliant organizations must establish a written security policy and an ongoing process for its review and revision).
3. **Organizing information security** (addresses the information security infrastructure, third-party access, and outsourcing).
4. **Asset management** (inventory and labeling of information assets; classification according to appropriate level of protection required).

<sup>25</sup> See [www.iso.org](http://www.iso.org)

5. **Human resources security** (to reduce human error and vulnerability to intrusions and manipulation, organizations must include security as an aspect of job requirements and employee awareness and training; organizations must assign responsibilities for responding to security incidents and malfunctions).
6. **Physical and environmental security** (establishing secure areas, equipment security, and general security controls).
7. **Communications and operations management** (operational procedures and responsibilities, system planning and acceptance, protection against viruses and other malicious software, housekeeping such as system logs and backups, network management, proper handling of storage media, exchanging information and software with other organizations).
8. **Access control** (setting business and procurement requirements for access control devices; user access management; responsibilities of authorized users; network access control; application access control; monitoring system access and use; access controls for mobile and remote computing).
9. **Information systems acquisition, development, and maintenance** (security requirements of systems; security in applications; cryptographic controls; security of file systems; security in development and support processes).
10. **Information security incident management** (incident response, documentation, and subsequent modification of security measures).
11. **Business continuity management** (mitigation of potential disruption of business activities and critical business processes by major failures or security breaches).
12. **Compliance** (compliance with applicable legal requirements; reviews of security policy and technical compliance with the organization's security policy; system audits).

**Relevance:** Laptop risks should be evaluated as part of an organization's risk assessment (element 1) and security policy (element 2). Laptop **encryption** and **remote administration** can be used to establish device security (element 6) and protect the laptop and the data on it from viruses and malware (element 7). Remote administration can be used to implement access controls (element 8). Laptop encryption should be considered in connection with cryptographic controls (element 9). Remote administration can be employed to detect and respond to a security incident (e.g., by remotely deleting data at risk) (element 10), thereby mitigating business risks from a laptop security breach (element 11). As indicated in earlier sections of this report, laptop encryption and remote administration also aid in legal compliance and legal risk management (element 12).

Most of the specific IT "controls" identified in ISO 17799 were written in the context of networks and data centers. However, the 2005 version emphasizes some new or enhanced controls that are particularly important for managing the risks associated with laptops and other portable devices. These include **encryption** for sensitive classifications of data, access controls including **authentication** for remote devices, and deprovisioning of terminated employees and contractors. **Remote administration** tools are an important means of achieving these controls with respect to laptops.

#### *ITIL / ISO 20000*

The Information Technology Infrastructure Library (ITIL), version 3<sup>26</sup>, does not define IT control objectives but rather consists of a collection of IT procedural best practices. It was developed in the United Kingdom from work done originally for the Office of Government Commerce (OGC) to guide UK government IT procurement and support. Continuing work is supported by OGC and the IT Service Management Forum.

As described by OGC, ITIL

"is the most widely accepted approach to IT service management in the world. ITIL provides a cohesive set of best practice, drawn from the public and private sectors internationally. It is supported by a comprehensive qualifications scheme, accredited training organisations, and implementation and assessment tools. The best practice processes promoted in ITIL support and are supported by, the British Standards Institution's standard for IT Service Management (BS15000)."

<sup>26</sup> See [www.itil.co.uk](http://www.itil.co.uk)

ITIL documents also refer to **ISO 17799 / 27002** (see the “ISO 17799” discussion above), offering guidance on the implementation of that security standard. In 2005, **BS15000** (the British IT Service Management standard that incorporates several of the ITIL documents) was adopted, with some additions, as **ISO 20000**. ITIL, ISO 17799 / 27002, and CobiT are not mutually exclusive. Some companies that use CobiT for SOX compliance, for example, or ISO 17799 / 27002 for security management policy, also refer to ITIL for implementation guidance.

ITIL publications (which must be purchased individually) address several topics to which **laptop encryption** and **remote administration** are relevant, including “IT service design and planning,” “IT service operation and support,” “IT and communications infrastructure management,” “software asset management,” and “IT security management.” **Encryption** is addressed primarily under the last heading. ITIL does not prescribe particular encryption methods but offers guidance on evaluating the contexts in which encryption is appropriate, based on the likelihood and severity of consequences flowing from a security breach.

### *NIST*

The US National Institute of Standards and Technology (NIST), a function of the Department of Commerce, studies information security risks and tests countermeasures on behalf of the United States government. The FISMA act, discussed above, requires federal agencies to refer to NIST standards and recommendations in procurement and in designing and implementing information security management plans. Thus, NIST standards and recommendations affect not only federal agency security practices but federal requirements for government contractors and software and hardware vendors. NIST documents are also influential with state governments and with governments and standards bodies outside the United States.

NIST recommendations on information security management procedures (800-series guidelines) are discussed above in connection with FISMA. As also noted in that section, NIST and OMB have recommended routine **encryption of all personal data on mobile devices**, because of the risk of identity theft when unencrypted data are exposed on lost and stolen laptops and other mobile hard drives<sup>27</sup>.

Some of NIST’s definitions and recommendations are codified as Federal Information Processing Standards (**FIPS**). These include **FIPS 197**, defining the Advanced Encryption Standard (AES)<sup>28</sup>. AES incorporates the Rijndael symmetric encryption algorithm, which NIST and OMB recommend for use by federal agencies to protect sensitive information.

NIST recommends AES encryption to protect data on laptops used by telecommuting or traveling employees:

“The advantage of publicly available algorithms such as NIST’s Data Encryption Standard (DES) and new Advanced Encryption Standard (AES) is that they have been scrutinized extensively by some of the world’s best cryptographers, so you have greater assurance of the encryption scheme’s strength.” (NIST Special Publication 800-46, Security for Telecommuting and Broadband Communications, §5.7)

**Seagate’s FDE drives use AES encryption as defined in FIPS 197.**

NIST’s guidance “Baseline Security Controls for High-Impact Information Systems,” Special Publication 800-53, rev. 1 (Recommended Security Controls for Federal Information Systems, Annex 3) (December 2006) addresses **encryption, authentication**, and a variety of other security measures for laptops and other mobile devices, many of which could be effected with **remote administration** tools. (Note that many of these recommendations are also included in the Annexes for low- and moderate-impact information systems, as well.)

<sup>27</sup> See Report of the President’s Identity Theft Task Force, “A Strategy to Combat Identity Theft” (April 2007), [www.idtheft.gov/reports/StrategicPlan.pdf](http://www.idtheft.gov/reports/StrategicPlan.pdf) p. 28.

<sup>28</sup> See <http://csrc.nist.gov> the website of NIST’s Computer Security Resource Center.

#### “AC-19 ACCESS CONTROL FOR PORTABLE AND MOBILE DEVICES

“Control: The organization: (i) establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and (ii) authorizes, monitors, and controls device access to organizational information systems.

“Supplemental Guidance: Portable and mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are only allowed access to organizational information systems in accordance with organizational security policies and procedures. Security policies and procedures include device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), configuration management, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Protecting information residing on portable and mobile devices (e.g., employing cryptographic mechanisms to provide confidentiality and integrity protections during storage and while in transit when outside of controlled areas) is covered in the media protection family. Related security controls: MP-4, MP-5.”

The cross-referenced Recommendation MP-4 (media storage) recommends that the organization consider routinely **encrypting** information at rest on selected secondary storage devices. MP-5 (media transport) notes that “[c]**ryptographic mechanisms** can provide confidentiality and/or integrity protections depending upon the mechanisms used” for handling data that is being transported on a portable device. Recommendation SI-3 (malicious code protection) also addresses the need to install and update protection software on mobile devices (something that can be accomplished with **remote administration** tools rather than relying on the user to download and install anti-trust protection and other protective software and updates).

Other portions of NIST SP 800-53, rev. 1 are also particularly relevant to laptop security and are greatly facilitated by using secure authentication and remote administration tools. These include AC-3 (access enforcement), AC-6 (“least privilege” access), AC-17 (automatic monitoring of remote access), AU-6 (audit monitoring and reporting for suspicious activity), CM-4 (monitoring configuration changes), IA-1 through IA-7 (user and device identification and authentication management), IR-4 (incident handling), MA-4 (remote maintenance), MP-6 (media sanitization and disposal), SC-12 (key management), SC-13 (use of cryptography), SI-3 (malicious code protection), SI-4 (monitoring tools and techniques), SI-7 (software and information integrity).

#### *PCI DSS*

Common information security standards for credit and debit cards are now developed by the PCI (payment card industry) Security Standards Council established by Visa, MasterCard, American Express, Discover, and JCB<sup>29</sup>. The PCI Data Security Standard, v. 1.1 (“**PCI DSS**”) was released in late 2006 and became mandatory, under payment card network contracts, for card issuers, acquiring banks, and retailers after December 2006.

Conformance to PCI DSS is enforced contractually by the payment card networks and card issuers. But it is also cited as establishing a standard for reasonable care in handling credit card and debit card data, in complaints recently filed against TJX by state attorneys general and class-action lawyers. A new Minnesota law, and bills introduced in California, Massachusetts, and Texas, would make retailers liable to card-issuing banks for the costs they incur in investigating security breaches and reissuing cards after a security breach in which the retailer failed to meet the PCI DSS standard. Thus, the standard has already had a legal impact beyond contractual enforcement.

When cardholder data are stored on laptops, PCI DSS requirements can be met in large part with **encryption** and **remote administration** tools. PCI DSS requires those who handle cardholder data to protect it in storage and encrypt it in transmission (Requirements 3 and 4). They must also maintain secure systems and applications (Requirement 6) (note that this can be accomplished with the aid of remote administration tools,

<sup>29</sup> See [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

in the case of laptops). Users must restrict access to cardholder data according to a business need-to-know (Requirement 7), restrict physical access to cardholder data (Requirement 9), and monitor access to cardholder data (again, in the case of laptops, this can be facilitated with encryption and remote administration tools). Noncompliance can result in fines and the suspension of privileges to use the payment card networks. Note that the network contracts expressly require notice of security breaches involving cardholder data to the payment networks, whether or not otherwise required by law.

Under Requirement 3.4, at a minimum the personal account number (“PAN”) must be protected with “strong cryptography” or “compensating controls” that are documented (and not always accepted by the card networks). If disk encryption is used (rather than file- or column-level encryption), “logical access must be managed independently of native operating system access control mechanisms” (Requirement 3.4.1), as in the Seagate / Wave FDE products. Keys must be changed periodically, preferably automatically (Requirement 3.6.4); card data must be deleted according to a data disposal policy (Requirement 3.1), purging data so that it cannot be reconstructed (Requirement 9.10.2). “Strict” control of the distribution of card data on any media (including laptops) must also be assured (9.7). All of these requirements can be addressed with **remote administration** software in the case of laptops.

## 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 A: Lost or Stolen Laptops and Hard Drives

- **Financial Services**

- Bank of America (18,000 records on a stolen laptop in June 2005, and an undisclosed number of debit card details on another stolen laptop, September 2005).
- JP Morgan Chase private banking clients (stolen laptop, August 2005).
- North Fork Bank (9000 records on a stolen laptop, September 2005).
- FirstTrust Bank (100,000 customer records on a stolen laptop, December 2005).
- Ameriprise (data on 226,000 investors and financial advisors on a laptop stolen from a locked car in December 2005, later recovered by the police).
- Olympic Funding (three hard drives with an unknown number of consumer records stolen in a break-in, March 2006).
- Mercantile Potomac Bank (stolen laptop with 48,000 customer records, May 2006).
- M&T Bank (May 2006, number unknown).
- AIG Insurance Group (records on 930,000 individuals, including Social Security numbers and some medical and disability information, on a stolen server, announced June 2006).
- AllState Insurance (2600 consumer records on a stolen computer, June 2006).
- Marsh Inc. (CS Stars) (records of 540,000 workers compensation claims on a stolen computer that was later recovered, July 2006; the company was required to reimburse the state \$60,000 in investigation costs).
- Old Mutual Capital Inc. (stolen laptop with records on 6500 shareholders, July 2006).
- CoreLogic for ComUnity Lending (stolen laptop with an unknown number of mortgage loan records, August 2006).
- AFLAC (stolen laptop with data on 612 policyholders, August 2006).
- Sovereign Bank (stolen laptop with data on “thousands” of customers, August 2006).
- American Family Insurance (2089 customer records on a stolen laptop, September 2006).
- Hilb, Rogal & Hobbs (insurance broker’s stolen laptop included data on 1243 Villanova University faculty and students, October 2006).
- Hancock Askew (retirement fund data on a stolen laptop, October 2006).
- KeyCorp (9300 financial customer records on a laptop stolen from a KeyCorp vendor, December 2006).
- New Horizons Community Credit Union (9000 member records on a laptop stolen from a consultant conducting a due diligence investigation in connection with a proposed acquisition, April 2007).
- Bank of America (customer records on a stolen laptop, April 2007).

- **Retailers and Service Providers**

- MCI (16,500 customer records on a stolen laptop, April 2005).
- Eastman Kodak (5800 records on a stolen laptop, June 2005).
- TransUnion credit bureau (3600 consumer records on a stolen laptop, November 2005).
- Safeway Hawaii (1400 records on a stolen laptop, November 2005).
- Ernst & Young UK (an auditor's stolen laptop included credit card data on 243,000 customers of Hotels.com, May 2006).
- KB Home (stolen laptop with data on 2700 prospective home buyers, January 2007).
- CTS Tax Service (stolen computer with individual tax records, February 2007).
- Speedmark (stolen computers with 35,000 consumer records, February 2007).
- Tax Service Plus (stolen computer with 4000 tax records, March 2007).
- Gander Mountain (10,000 credit card records included among 112,000 customer records on a lost or stolen computer, September 2007).

- **Employers**

- Boeing (161,000 employee records on a stolen laptop, November 2005; 3600 employee records on another stolen laptop, April 2006).
- Ford Motor Company (70,000 employee records on a stolen computer, December 2005).
- Washington Employment Security Department (500 employee records on a stolen laptop, December 2005).
- Fidelity (retirement fund data on 196,000 current and former HP and Compaq employees on a stolen laptop, March 2006).
- Verizon (March 2006, number undisclosed).
- Aetna (health insurance records for 38,000 employees of the US Department of Defense and Omni Hotels on a laptop stolen from an Aetna employee's car, April 2006).
- Ahold USA (Stop & Shop, Giant Food, etc.) (EDS employee lost a laptop on an airplane; data concerned an unknown number of Ahold employee records, June 2006).
- Union Pacific (stolen laptop with records on 30,000 employees, June 2006).
- ING (two stolen laptops with information on 8500 Jackson Health System employees, and a stolen laptop with data on 13,000 District of Columbia employees, both in June 2006).
- Equifax credit bureau (stolen laptop with 2500 employee records, June 2006).
- Armstrong World Industries (laptop stolen from a Deloitte & Touche auditor contained records on 12,000 Armstrong employees).
- Belhaven College (300 employee records on a laptop stolen at gunpoint, July 2006).
- Los Angeles County (stolen laptop with employee data, July 2006).
- Toyota (stolen laptop with 1600 employee and job applicant records, August 2006).
- Chevron (employee data on a laptop stolen from an outside auditor, August 2006).

- Williams-Sonoma (1200 employee records on a laptop stolen from an outside auditor, August 2006).
- Diebold (employee records on a stolen laptop, August 2006).
- Wells Fargo (laptop stolen from an outside auditor included employee records, August 2006).
- City of Chicago (laptop stolen from retirement benefits management company included data on up to 38,000 employees, September 2006).
- Howard, Rice (San Francisco law firm) (laptop stolen from the firm's outside auditor, with data on 500 current and former employees, September 2006).
- General Electric (50,000 employee records on a laptop stolen from a hotel room, September 2006).
- T-Mobile USA (records on 43,000 current and former employees on a laptop that disappeared in airline checked baggage, October 2006).
- Gymboree (3 stolen laptops with human resources data on some 20,000 employees, October 2006).
- Hertz (data on employees since 2002 found on the home computer of a former employee, October 2006).
- Avaya (employee records on a stolen laptop, October 2006).
- Greater Media (stolen laptop with employee data, November 2006).
- Intermountain Health Care (6244 employee records on a used computer sold through a second-hand store, November 2006).
- Starbucks (4 missing laptops with data on more than 60,000 US and Canadian employees and contract workers, November 2006).
- TD Ameritrade (stolen laptop with employee data, December 2006).
- Boeing (stolen laptop, later recovered, with data on 382,000 current and former employees, December 2006).
- Notre Dame University (a director's stolen laptop contained Social Security numbers and salary information on employees, January 2007).
- Altria (Philip Morris, Kraft Foods, United Technologies) (5 laptops stolen from a benefits consultant, with data on some 18,000 current and former employees, January 2007).
- Springfield, Ohio Schools (1950 employee records on an auditor's stolen laptop, March 2007).
- US Army, Fort Monroe (stolen laptop with data on 16,000 civilian employees, March 2007).
- Chicago Public Schools (2 stolen laptops with data on 40,000 current and former employees, April 2007).
- Neiman Marcus Group ("computer equipment" stolen from a consultant included data on 160,000 current and former employees, April 2007).
- Caterpillar, Inc. (employee data on a laptop stolen from a benefits consultant, April 2007).
- University of New Mexico (3000 employee records on a laptop stolen from a consultant, April 2007).
- Pfizer: unauthorized file sharing software on a laptop compromised data on 17,000 employees (June 2007); two stolen laptops reported with data on nearly 1000 independent contractors (August 2007); electronic files on 34,000 employees copied and "removed" by an employee (September 2007).

- Verisign (laptop with employee data stolen from an employee's car, August 2007).
  - Merrill Lynch (stolen "computer device" with 33,000 employee records, August 2007).
  - AT&T (laptop stolen from a professional services contractor with AT&T employee data, August 2007).
- **Government**
    - California Department of Health Services (21,600 patient records on a stolen laptop, April 2005).
    - Colorado Health Department (1600 family records on a stolen laptop, May 2005).
    - US Department of Justice (80,000 individuals' records on a stolen laptop, May 2005).
    - US Marine Corps (stolen portable drive with personal data on 207,750 individuals, March 2006).
    - US Department of Health and Human Services (data on 17,000 Medicare beneficiaries downloaded by an insurance company employee on a laptop stolen from a hotel room, April 2006).
    - US Department of Veterans Affairs (laptop and external hard drive with unencrypted Social Security numbers and other personal information on some 28.6 million Americans stolen from an employee's home, May 2006; the laptop was ultimately recovered, apparently before the data had been used for ID theft or fraud, but the incident cost the VA hundreds of thousands of dollars in the interim and resulted in threatened legislation and a vendor contract to review patterns of laptop misuse).
    - Minnesota State Auditor (records on state employees in three missing laptops, June 2006).
    - US Federal Trade Commission (stolen laptops included Social Security numbers and financial account details on over 100 consumers, June 2006).
    - Montana Public Health and Human Services Department (stolen computer contained information about persons on drug dependency programs, July 2006).
    - Hattiesburg, Mississippi (hard drives stolen from city computers contained information on thousands of city contractors and employees, July 2006).
    - US Navy (36,000 recruiting records, some with Social Security numbers, on two stolen laptops, July 2006).
    - West Virginia Division of Rehabilitation Services (stolen laptop, July 2006).
    - Los Angeles County Adult Protective Services (11 laptops stolen, July 2006).
    - US Department of Veterans Affairs (computer stolen from contractor Unisys contained records on at least 18,000 persons, August 2006).
    - US Department of Transportation (stolen laptop with records of 132,470 persons with drivers' or pilots' licenses, and another stolen laptop with records of investigations, both in August 2006).
    - Florida National Guard (stolen laptop with data on 100 soldiers, September 2006).
    - US Department of Commerce and Census Bureau (reported in September 2006 that 1137 laptops have been lost or stolen since 2001).
    - North Carolina Department of Motor Vehicles (computer stolen with data on 16,000 drivers' licenses, September 2006).

- New Jersey National Guard (26 computers stolen 2004-2006, all unencrypted, announced October 2006).
- Cleveland Air Traffic Control Center (missing hard drive with data on 400 air traffic controllers, October 2006).
- US Marine Corps, Camp Pendleton (missing laptop with data on 2400 residents, October 2006).
- US Census Bureau (Travis County, Texas resident records, October 2006).
- US Transportation Security Administration (USB drive with data on 900 TSA employees, October 2006).
- US Army Cadet Command (stolen laptop with data on 4600 high school seniors, November 2006).
- Colorado Department of Human Services (stolen computer with data on up to 1.4 million individuals, November 2006).
- Pennsylvania Department of Transportation (stolen computers with records on more than 11,000 licensed drivers, November 2006).
- US Army National Guard, West Virginia (stolen laptop with data on Guard members, December 2006).
- Santa Clara Employment Agency (2500 records on a stolen laptop, December 2006).
- US Department of Veterans Affairs (portable hard drive lost in January 2007 with personal information and billing records on more than 500,000 veterans and 1.3 million doctors).
- New York Department of Labor (auditor's stolen laptop with records of more than 500 area employees, February 1007).
- US Internal Revenue Service, according to a 2007 audit report, has lost nearly 500 laptops since 2003 from employees' homes, cars, and offices, compromising financial data on thousands of taxpayers.
- North Carolina Department of Revenue (30,000 taxpayer records on a stolen laptop, announced January 2007).
- California National Guard (stolen hard drive with records of 1300 guardsmen on border patrol duty, March 2007).
- US Department of Agriculture announced in March 2007 that 95 department computers were lost or stolen between October 2005 and May 2006, compromising an unknown amount of government and personal information (an estimated two-thirds of which was unencrypted).
- Los Angeles County Child Support Services (3 stolen laptops with data on 243,000 individuals, March 2007).
- US Navy, San Diego (3 missing laptops with data on Navy personnel, March 2007).
- Broward County, Florida (12,000 foster care records on a laptop stolen from a services vendor, April 2007).
- Baltimore County Department of Health (stolen laptop with 6000 patient records, April 2007).
- US Transportation Security Administration announced that a portable hard drive including records on 100,000 current and former TSA employees (including undercover air marshals) disappeared from its office, resulting in a lawsuit brought by the AFGE union, May 2007.
- Champaign (Illinois) Police Department (data on police officers left on a computer donated to charity, May 2007).
- Detroit Water and Sewerage (stolen laptop with data on 3000 employees, May 2007).

- Texas Commission of Law Enforcement Standards and Education (stolen computer belonging to Productivity Center Incorporated contained data on 230,000 Texas law enforcement officers, May 2007).
  - Ohio Bureau of Workers' Compensation (two laptops stolen from employees' homes with data on taxpayers and injured workers, June 2007).
  - Yuba County Health and Human Services (70,000 social services records on a stolen laptop, July 2007).
  - Idaho Army National Guard (stolen portable drive with data on 3400 soldiers, August 2007).
  - Connecticut Department of Revenue Services (106,000 taxpayer records on a stolen laptop, August 2007).
  - Maryland Department of the Environment (stolen laptop with licensing databases, August 2007).
- **Medical Records**
    - Incidents in 2005 involving lost or stolen hard drives with medical data: Ohio State University Medical Center (15,000 patient records), University of Florida Health Sciences Center (3851 patient records), University of Tennessee Medical Center (3800 patient records), USC Keck School of Medicine (50,000 patient records).
    - 2006 incidents: University of Pittsburgh Medical Center (700 patient records), the University of Washington Medical Center (1600 patient records), Mount St. Mary's Hospital, New Jersey (17,000 patient records on two laptops stolen in an armed robbery), Medco Health Solutions (4600 patient records), Buckeye Community Health Plan (72,000 patient records on four stolen laptops), University of Alabama (stolen computer with records of 9800 kidney donors, recipients, and potential donors), Cape Fear Valley Health System (portable computer with more than 24,000 medical records stolen from an ambulance), Lancaster General Hospital (hundreds of records on doctors), Kaiser Permanente (160,000 patient records on a stolen laptop), PSA HealthCare (52,000 patient records on a stolen laptop), Madrona Medical Group (employee arrested after downloading at least 6000 patient records onto a laptop), Hospital Corporation of America (thousands of patient files on 10 stolen computers), Compass Health (stolen laptop with records on mental patients), Labcorp (patient records on a stolen computer), DePaul Medical Center (more than 100 patient records on two stolen computers), Allina Hospitals (17,000 patient records on an obstetric nurse's stolen computer), Manhattan Veterans Affairs Hospital (1600 patient records), Jacobs Neurological Institute (patient records on a stolen laptop), Indiana State Department of Health (records on 7500 women cancer patients on two stolen computers), Kaiser Permanente Colorado (38,000 patient records on a stolen laptop, Electronic Registry Systems (records on more than 63,000 cancer patients of several hospitals).
    - St. Mary's Hospital (stolen laptop with 130,000 patient records, February 2007).
    - Kaiser Permanente Medical Center, Oakland (stolen laptop with 22,000 patient records, February 2007).
    - Seton Healthcare Network (stolen laptop with 7800 patient records, February 2007).
    - Gulf Coast Medical Center (stolen computers with 9900 patient records, February 2007).
    - Group Health Cooperative, Seattle (2 stolen laptops with data on 31,000 patients and employees, March 2007).
    - Swedish Urology Group, Seattle (3 stolen hard drives with data on hundreds of patients, March 2007).
    - Highland Hospital (2 stolen laptops with 13,000 patient records, May 2007).

- **Student Records**

- University of California (Berkeley) (personal data on 98,400 students and alumni on a laptop stolen from an employee, March 2005).
- Other incidents in 2005: Oklahoma State University (records on 37,000 students and alumni), Cleveland State University (44,000 individuals affected, although the laptop was subsequently recovered), Kent State University (1400 student records in June 2005 and 100,000 in September 2005), Georgia Tech (13,000 individuals' records on a stolen computer).
- 2006 incidents: Metropolitan State College (Denver) (93,000 student records on a stolen laptop), Vermont State Colleges (14,000 records), Miami University (850 student records on a lost handheld computer), University of Kentucky (6500 student records on a stolen flash drive), San Francisco State University (3000 student records on a professor's stolen laptop), University of Iowa (280 graduate student files), California Polytechnic State University (3020 student records on a laptop stolen from a professor's home), University of Minnesota Institute of Technology (13,084 student records on two stolen desktop computers), University of Colorado, Boulder (two missing computers with 1372 student records), San Juan Capistrano Unified School District (5 stolen computers), Troy Athens High School (stolen hard drive with 4400 student records), University of Texas at Arlington (two stolen computers with 2500 student records), Germantown Elementary School (stolen computer with student Social Security numbers), University of Minnesota (student records on a stolen laptop), Connors State College (records on more than 22,000 college and high school students on a stolen laptop), Greenville County School District (records on 101,000 students and employees found on used computers sold at auction), California State University, Los Angeles (2534 student and faculty records on a stolen USB drive).
- University of Idaho (3 stolen desktop computers with data on 331,000 individuals, including 70,000 Social Security numbers, January 2007).
- Vanguard University (2 stolen computers with data on over 5000 financial aid applicants, January 2007).
- Eastern Illinois University (stolen desktop with 1400 student records, January 2007).
- Notre Dame University (student records left on a decommissioned computer, January 2007).
- Metropolitan State College, Denver (stolen laptop with nearly 1000 student records, March 2007).
- University of Montana (stolen hard drive with 400 student records, March 2007).
- Northwestern University (stolen laptop with records of thousands of students and alumni, May 2007).
- University of Minnesota (student data on a professor's stolen laptop, July 2007).
- American Education Systems (5000 records on a subcontractor's stolen laptop, July 2007).
- Yale University (10,000 student and faculty records on two stolen computers, August 2007).
- De Anza College (4375 student records on an instructor's stolen laptop).

- **Nonprofits**

- American Institute of Certified Public Accountants (330,000 member records, including Social Security numbers, on an unencrypted hard drive that was lost while being shipped back to AICPA from a computer repair company, May 2006).

- YMCA (stolen laptop with personal data on 65,000 members, June 2006).
- American Red Cross (three stolen laptops with personal data, July 2006).
- National Association of Securities Dealers (ten laptops stolen from NASD investigators, with files on dealers under investigation; announced July 2006).
- American Cancer Society (several stolen laptop computers, reported in November 2006).

- **Other Countries**

Data breaches attributable to insecure hard drives are by no means limited to the United States, although security breach notice laws tend to ensure more publicity in the US.

- 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).
- 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).

## Appendix B: Information Security Requirements and Sources

Seagate FDE drives with Wave 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  CA AB 1950 and several other state laws require "reasonable" security measures  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  Several states considering reference to PCI DSS standard	CA AB 1950 and several other state laws require "reasonable" security measures  Several states considering reference to PCI DSS standard	Sensitive data disposal required in CA, other states  Several states considering reference to PCI DSS standard	CA AB 1950 and several other state laws require "reasonable" security measures  Several states considering reference to PCI DSS standard

## Information Security Requirements and Sources:

Requirement Source	<i>Encryption (data and keys)</i>	<i>Encryption (automatic)</i>	<i>Access Controls (ID mgmt and authentication)</i>	<i>Remote Admin. (ID mgmt and authentication)</i>	<i>Remote Admin. (data wiping)</i>	<i>Remote Admin. (audit log, suspicious activity monitoring)</i>
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”  UK: threatens enforcement for losses due to unencrypted laptops  Spain: encryption required for sensitive data  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;  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.



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 # 03-000226/version 1.01 Effective Date: 2008-02-11

Copyright © 2008 Wave Systems Corp. All rights reserved. Wave "Juggler" and EMBASSY logo are registered trademarks of Wave Systems Corp. All other brands are the property of their respective owners. Distributed by Wave Systems Corp. Specifications are subject to change without notice.