



Financial Services: Is Your Company Compliant with Data Protection Regulations?

A lost or stolen laptop can spell disaster for financial institutions. But “laptop security” needn’t be an oxymoron thanks to developments in hardware-based full-disk encryption.

By W. Scott Blackmer
Technology Law and Consulting

Executive Summary	1
Data Security Beyond the Firewall	2
Potential Costs of Lost Data	3
The Regulatory and Liability Landscape	4
Laptop Security: Best Practices	6
The Comparative Benefits of Hardware-Based Full-Disk Encryption	7
Conclusions	8
Appendix A: Lost or Stolen Laptops and Hard Drives	9
Appendix B: Information Security Requirements and Sources	11
Appendix C: The Regulatory and Liability Landscape	12
About the Author	17
About Wave Systems	17

Abstract

Lost or stolen laptops and portable hard drives pose an increasingly significant risk to the modern enterprise, threatening its competitiveness, its credibility and even its bottom line. As a consequence, corporate data security officers and IT departments often find themselves accountable under increasingly stringent regulatory and legal standards for protecting the sensitive data stored on mobile devices.

This paper details and quantifies the risks posed by missing mobile devices, reviews the regulatory and legal backdrop that has evolved as a result of these risks, and discusses the relative merits of software- and hardware-based full-disk encryption technologies.

Executive Summary

One consequence of the “laptop revolution” is that the laptop computer has become a particular hazard to the modern enterprise. Although laptops enable business to become more mobile, the trade-off is they frequently carry sensitive or confidential data beyond the enterprise’s centralized firewalls and network access protections.

As a result, the lost or stolen laptop (or portable drive) represents a growing threat to an organization’s reputation and credibility. Even worse, it may also expose the institution to compliance and litigation risk management issues. The laws, regulations, and judicial precedents that hold enterprises accountable for exposure of sensitive data are proliferating. They include:

- The Gramm-Leach-Bliley Financial Services Modernization Act, which protects the financial privacy of individuals who do business with such regulated financial institutions as banks, brokerages, insurance companies and similar providers
- Security breach notice laws, such as California SB 1386, are mandating disclosure of laptop security breaches where and when they have put private consumer information at risk
- The Federal Financial Institutions Examination Council that, among other practices, examines the information security practices of banks and other federally regulated financial institutions, including the integrity of information on mobile devices. It also investigates reported security breaches such as those listed in Appendix A

September 2008
www.wave.com

- The Sarbanes-Oxley Act (SOX), which considers a corporation's information security policies and procedures when measuring its financial condition and risks. Such risks may encompass how well a company manages its data security or handles breaches
- The COSO framework, which provides a reference for SEC and independent auditors charged with evaluating a corporation's control of its assets, including the security of its data

Corporate data security officers and their peers are increasingly tasked to not only protect information stored on mobile devices before it is lost or stolen, but to also help quantify or even negate the potential damage in the wake of such events.

Unfortunately, conventional means such as software-based encryption technologies are showing serious gaps in the protection they offer before a laptop is lost or stolen, and little or no control over the stored data after the fact.

This has provided an opportunity for hardware-based full-disk encryption and drive management software. Such solutions enhance laptop security by working below the operating system. Plus, they can integrate additional security measures from remote administration to storage of authentication functions on a separate chip¹. Lastly, the truly integrated security of hardware-based full-disk encryption can reduce the total cost of ownership.

On a more practical level, hardware-based full-disk encryption shields more than the data stored on a lost or stolen mobile device. It protects a financial enterprise against the loss of competitive secrets and credibility, and it prevents exposure to the compliance and litigation costs that often follow in the wake of such an event.

Data Security Beyond the Firewall

Information security is critical to the modern financial enterprise. The loss or alteration of sensitive data can damage credibility, competitive viability and/or essential business relationships with other organizations or individuals. Representative examples of such sensitive data may include:

- Customer information, such as payment card and bank account details, social security numbers and other official identifiers
- Confidential commercial information and trade secrets of the enterprise, such as transaction records, personnel administration and third-party confidential material covered under nondisclosure agreements
- 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 building or computer network

Such sensitive electronic information requires appropriate security measures to protect both the enterprise and third parties from undue risk and exposure.

Software-based encryption is an adequate defense for data stored on stationary devices, such as mainframes, servers, desktops and work stations, as well as point-of-sale terminals. The point of greatest vulnerability, however, is the highly mobile laptop computer. Employees not only use laptops at work, they increasingly take them home or on the road, beyond the virtual defenses of network firewalls and access controls. Inevitably, some laptops or other portable hard drives are lost, stolen, or inadvertently left behind, ready for someone else to pick up.

As the number of reported lost or stolen laptops listed in Appendix A illustrates, such security breaches have become all too common. Clearly, they occur at a wide range of reputable financial institutions and other organizations. Presumably, these organizations maintain information security policies and an extensive central information security infrastructure. But, again, Appendix A underscores how laptops have become the weakest link in many institutions' data security infrastructure.

¹ See R. Enderle, "TPM to Bolster Laptop Security," darkREADING, June 19, 2006. Available online at www.darkreading.com/document.asp?doc_id=95391.

The increasing importance of laptop security is further substantiated by these statistics:

- 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 six 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 equipment²
- 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 annually³
- 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

Software-based full-disk encryption may confound casual interest in a laptop’s contents – assuming the owner remembered to implement appropriate protocols. But in the hands of an experienced hacker the possibility exists that a laptop’s software-based encryption key can be compromised, and the data accessed as demonstrated recently by a team of Princeton University researchers.⁴

Potential Costs of Lost Data

There is growing public concern about security breaches involving personal data, particularly because identity theft and subsequent 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.⁵ The FTC and the Identity Theft Resource Center estimate the annual cost to consumers is \$5 billion, and an average 600 hours is required to deal with the consequences of having one’s identity assumed.

Meanwhile, the direct cost to businesses is 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 are increasingly calling for greater care and accountability on the part of financial institutions that store the kinds of personal data most frequently used in identity theft. Part of this new accountability is evident in California’s Security Breach Notification Law, SB 1386, enacted in January 2005. It requires businesses to publicize data security breaches, including those caused by lost or stolen laptops. At least thirty other states have followed California’s lead and have passed similar legislation. Even before such mandates were enacted, the media covered an increasing number of security breaches involving the loss or potential exposure of thousands of personal records. The sheer volume of such incidents listed in Appendix A is sobering.

Even if the sensitive information on a lost or stolen laptop remains secure, however, the latent risk of exposure is enough to impose costly consequences to the enterprise.

The general practice when a laptop goes missing is to hold one or more press conferences. Enterprises are often also 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.

² See Network World, March 13, 2007. Available online at www.networkworld.com/news/2007/031307-data-breach-companies.html.

³ See eWeek.com, March 7, 2007. Available online at www.eWeek.com/article2/0%2C1895%2C2101683%2C00.asp

⁴ See http://www.informationweek.com/news/personal_tech/showArticle.jhtml?articleID=206801184

⁵ See <http://ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identitytheft.html>

Referring again to the Computer Security Institute study, survey responses indicated that in security breaches where customer data was compromised, the cost of notice and rectification averaged \$100 per record. The cost to enterprises, however, may become substantially higher.

Increasingly, in the wake of a security breach, such enterprises may also 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. This can be difficult to impossible with conventional data encryption based on software.

The Regulatory and Liability Landscape

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 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.

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. For more detailed descriptions please see Appendix C.

The Gramm-Leach-Bliley Financial Services Modernization Act

The Gramm-Leach-Bliley Financial Services Modernization Act (GLBA) of 1999 includes provisions to protect financial privacy.⁶ It applies to regulated financial institutions, such as bankers, brokers and insurers. But its definition is so broad as to include many companies that are "significantly engaged" in providing financial products or services.

The Act puts the responsibility of protecting the security and confidentiality of customers' nonpublic personal information on the financial services providers who serve them. To this end, it sets standards for administrative, technical, and physical safeguards against anticipated threats or hazards to the security or integrity of such records. These safeguards encompass the prevention of unauthorized access to or use of such records or information.

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 Appendix A indicate that this risk has not been fully addressed in the security management practices of some financial institutions.

Security Breach Notice Laws

California's SB 1386, the "Security Breach Notice" law, has triggered costly and embarrassing disclosure of numerous laptop security breaches. Importantly, it has also served as a model for new legislation in most of the states.

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.

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.

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

Thus, the first step in defending an organization would be to demonstrate that it has chosen encryption and authentication or other access controls that are considered effective, for example, by referencing 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.

Federal Financial Institutions Examination Council

The Federal Financial Institutions Examination Council (FFIEC) examines banks and other federally regulated financial institutions annually. The examination includes their information security practices, and 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 Appendix A.

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.

Sarbanes-Oxley and Corporate Internal Controls

For a financial reporting law, the federal Sarbanes-Oxley Act of 2002⁷ (SOX) gets enormous attention in information security circles. The law was enacted following corporate financial meltdowns at Enron, Tyco, WorldCom, Peregrine Systems and Global Crossing, in an attempt to tighten accounting and audit standards for public companies. It aimed to provide investors greater transparency and more reliable information concerning a corporation's financial condition and material risks.

The importance of information systems and data holdings to modern corporations qualifies many data security breaches as such a material loss or risk. Thus, the quarterly certification that all material internal controls are in place will cover the company's information security policies, procedures and recent experience.

As a result, information security officers now regularly report to senior executives and auditors, who must be satisfied that the corporation has evaluated significant data 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 COSO Framework

In the wake of SOX, the SEC and independent auditors typically refer to the COSO Framework in evaluating internal controls designed to protect assets and ensure compliance with applicable laws and regulations. Named for the Committee of Sponsoring Organizations of the Treadway Commission, the COSO Framework's Enterprise Risk Management – Integrated Framework (ERM) is commonly used in SOX audits to assess internal controls under SOX §404.

It identifies eight components of enterprise risk management including event identification, risk assessment and risk response.

The potential risks to data security associated with corporate laptops would be covered in these three aspects of risk management. 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.

⁷ See <http://thomas.loc.gov/cgi-in/query/z?c107:H.R.3763.ENR:%20>

The COSO control framework suggests 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, and should clearly define procedures for securing data on laptops and other portable drives
- 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)
- 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)

Laptop Security: Best Practices

All of these emergent trends in the regulatory and liability landscape have helped shape some best practices for managing security on data storage products. For example:

- **Encryption:** Enterprises are typically encouraged (and sometimes required) to protect certain categories of data with effective encryption methods, and to protect the secret keys themselves.

Laws on information security and security breach notice offer no “safe harbor” for encryption techniques that the enterprise cannot reasonably rely on. 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 is 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 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.

The Comparative Benefits of Hardware-Based Full-Disk Encryption

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.

This, in part, demonstrates the limits of software-based encryption methods, which can neither be activated after a laptop is lost or stolen, nor ensure against a breach in the hands of a talented expert.

This has helped fuel interest in hardware-based full-disk encryption on laptops and portable hard drives. Unlike software encryption keys, hardware-based solutions offer intrinsically more robust security, and do not hamper user productivity because they operate “underneath” a laptop’s operating system. Plus, they enable integration of additional security measures, such as remote administration, authentication tokens, biometrics, or a Trusted Platform Module (TPM) that keep devices or user authentication functions on a separate chip. Lastly, as a truly integrated security solution, hardware-based full-disk encryption solutions can reduce an enterprise’s total cost of ownership.

One notable illustration of what hardware-based full-disk encryption can deliver is Seagate's Momentus 5400 FDE.2 full disk encryption drive, combined with Wave Systems' EMBASSY® Trusted Drive Manager and EMBASSY Remote Administration Server (ERAS).

This solution offers an efficient way for enterprises to ensure automatic full-disk encryption, secure authentication, and remote administration controls. Briefly, here is how these products enhance information security:

- The Seagate Momentus 5400 FDE.2 full disk encryption hard drive incorporates strong cryptography that satisfies every encryption recommendation and the best practices detailed above, as well as the encryption “safe harbor” under breach notice laws.

Wave's Trusted Drive Manager client application activates the access control and authentication features of the Seagate drive. Trusted Drive Manager pre-boot authentication 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 those stored in the protected area of the hard drive during user enrollment. All of this is performed in a pre-OS environment; before the operating system is loaded and active.

- In cases of a stolen or lost laptop, claiming that the data was encrypted isn't good enough to avoid the sizeable costs associated with notifying customers whose data has been exposed.
- Wave's EMBASSY Remote Administration Server enables the enterprise to prove encryption was on after a laptop is lost or stolen, offering centralized “no touch” management of FDE drives. It also creates secure audit logs to help prove compliance with internal policies and data protection regulations.

Such capabilities meet or exceeds all of the best practices for endpoint data encryption security detailed above. Wave's EMBASSY remote management server then allows the organization's IT department to centrally 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,
- Log changes to the FDE drive security settings and user or administrator access to data⁸, 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 EMBASSY Remote Administration Server 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, such hardware-based solutions represent a superior answer to common laptop security problems. And, as the previous discussion on compliance and liability suggests, such technologies can 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 – all while protecting its business and its brand.

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 FDE hard drives is not expressly mandated in existing laws or regulations, but it facilitates satisfying a range of critical IT and security requirements – such as centralized management, remote access policies, secure audit records, and instant cryptographic hard drive erase – and therefore would be considered best practices. 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.

⁸ Note that NIST’s Computer Security Incident Handling Guide, Special Publication 800-61, Jan. 2004 (Available online at 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.

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 hardware-based 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

- September 2007, Gander Mountain: 10,000 credit card records included among 112,000 customer records on a lost or stolen computer
- April 2007, Bank of America: Customer records compromised by a stolen laptop
- March 2007, Tax Service Plus: Stolen computer with 4,000 tax records
- February 2007, CTS Tax Service: Stolen computer with individual tax records
- February 2007, Speedmark: Stolen computers with 35,000 consumer records
- December 2006, KeyCorp: 9,300 financial customer records on a laptop stolen from a KeyCorp vendor
- October 2006, Hilb, Rogal & Hobbs: Insurance broker's stolen laptop included data on 1,243 Villanova University faculty and students
- October 2006, Hancock Askew: Retirement fund data on a stolen laptop
- September 2006, American Family Insurance: 2,089 customer records on a stolen laptop
- August 2006, AFLAC: Stolen laptop with data on 612 policyholders
- August 2006, Sovereign Bank: Stolen laptop with data on "thousands" of customers
- August 2006, CoreLogic for ComUnity Lending: Stolen laptop with an unknown number of mortgage loan records
- June 2006, AIG Insurance Group: Records on 930,000 individuals, including Social Security numbers and some medical and disability information, on a stolen server
- May 2006, Mercantile Potomac Bank: Stolen laptop with 48,000 customer records
- March 2006, Olympic Funding: Three hard drives with an unknown number of consumer records stolen in a break-in
- July 2006, Marsh Inc. (CS Stars): Records of 540,000 workers compensation claims on a stolen computer. Computer was later recovered, but the company was required to reimburse the state \$60,000 in investigation costs
- July 2006, Old Mutual Capital Inc: Stolen laptop with records on 6500 shareholders

- June 2006, AllState Insurance: 2,600 consumer records on a stolen computer
- May 2006, Ernst & Young UK: Auditor's stolen laptop included credit card data on 243,000 customers of Hotels.com
- May 2006, Hummingbird: Contractor for the Texas Guaranteed Student Loan Corp., (1.7 million borrowers' records were stored on a lost hard drive).
- 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
- April 2006, Aetna: Health insurance records for 38,000 employees of the US Department of Defense, and Omni Hotels on a laptop stolen from an employee's car
- March 2006, Fidelity: Retirement fund data on 196,000 current and former HP and Compaq employees on a stolen laptop
- 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
- November 2005, TransUnion credit bureau: 3,600 consumer records on a stolen laptop
- September 2005, Bank of America: An undisclosed number of debit card details on a stolen laptop
- September 2005, North Fork Bank: 9,000 records on a stolen laptop
- August 2005, JP Morgan/Chase: Private information of banking client on stolen laptop
- June 2005, Bank of America: 18,000 records on a stolen laptop
- April 2005, MCI: 16,500 customer records on a stolen laptop

Appendix B: Information Security Requirements and Sources

Hardware-based full-disk encryption, as illustrated by Seagate FDE drives with Wave Trusted Drive Manager and EMBASSY Remote Administration Server, can meet or exceed each of the following selected requirements for laptop security:

Requirement	Encryption Data & Keys	Encryption Automatic	Access Controls ID Mgmt & Authentication	Remote Administration		
				ID Management & Authentication	Data Wiping	Audit Log & Suspicious Activity Monitoring
GLBA & FFIEC	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
State & 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
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
The Sarbanes- Oxley Act?						
COSO framework?						

Appendix C: The Regulatory and Liability Landscape

The Gramm-Leach-Bliley Financial Services Modernization Act

The Gramm-Leach-Bliley Financial Services Modernization Act (GLBA) of 1999 includes provisions to protect financial privacy.⁹ It applies to regulated financial institutions, such as bankers, brokers and insurers. But its definition is so broad as to include many companies that are “significantly engaged” in providing financial products or services.

The Act puts the responsibility of protecting the security and confidentiality of customers’ nonpublic personal information on the financial services providers who serve them. To this end, it sets standards for administrative, technical, and physical safeguards against anticipated threats or hazards to the security or integrity of such records. These safeguards encompass the prevention of unauthorized access to or use of such records or information.

These security safeguards must also specifically be designed to prevent “pretexting,” where individuals seek to obtain financial information about others under false pretenses. Note that pretexting could be facilitated by using authentication credentials found on a lost or stolen laptop.

- In addition to the detailed security guidelines and examination procedures under GLBA, the FTC promulgated in 2002 its own broadly similar guidelines to cover nontraditional financial institutions. Its Financial Information Safeguards Rule¹⁰ requires organizations to develop and maintain a “security program,” documented in writing, to protect nonpublic personal financial information. The program must
 - 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:
 - 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;
 - 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, 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.

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 Appendix A indicate that this risk has not been fully addressed in the security management practices of some financial institutions.

⁹ Title V - Privacy, §§ 501 et seq., Pub. L. 106-102 (1999), codified at 15 USC §§ 6801-6809, “Disclosure of Nonpublic Personal Information.” See <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ102.106>

¹⁰ Financial Information Safeguards Rule, 16 C.F.R. Part 314. See www.ftc.gov/os/2002/05/67fr36585.pdf

Security Breach Notice Laws

California's SB 1386, the "Security Breach Notice" law, has triggered costly and embarrassing disclosure of numerous laptop security breaches. Importantly, it has also served as a model for new legislation in most of the states.

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.¹¹

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.

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.

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. In the most extreme cases, timely notice means within 48 hours.

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.

Clearly, it is increasingly critical for an enterprise facing an administrative, civil, or criminal investigation or complaint to be able to establish that it made reasonable choices on how to protect the data at issue. But it is becoming equally important to provide some assurances 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.

¹¹ See Cal. Civ. Code §1798.82(e) and (f).

Thus, the first step in defending an organization would be to demonstrate that its chosen encryption and authentication or other access controls that are considered effective, for example, by referencing 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.

Federal Financial Institutions Examination Council

The Federal Financial Institutions Examination Council (FFIEC) examines banks and other federally regulated financial institutions annually. The examination includes their information security practices, and 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 Appendix A.

Elsewhere, supervisory authorities for the federal bank jointly issued Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.¹² It is a further interpretation of GLBA rules and existing Security Guidelines for banks.

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.

That means that banks and thrifts in states that have not yet adopted security breach notice laws (discussed below) are still 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.

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 in civil actions filed after major security breaches.

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.¹³

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.

Sarbanes-Oxley and Corporate Internal Controls

For a financial reporting law, the federal Sarbanes-Oxley Act of 2002¹⁴ (SOX) gets enormous attention in information security circles. The law was enacted following corporate financial meltdowns at Enron, Tyco, WorldCom, Peregrine Systems and Global Crossing, in an attempt to tighten accounting and audit standards for public companies. It aimed to provide investors greater transparency and more reliable information concerning a corporation's financial condition and material risks.

¹² See www.occ.treas.gov/consumer/Customernoticeguidance.pdf

¹³ See FTC privacy cases under FTC Act §5 summarized, with links to the relevant documents, at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html

¹⁴ See <http://thomas.loc.gov/cgi-in/query/z?c107:H.R.3763.ENR:%20>

Several provisions of SOX are of particular interest to corporate information technology departments and should be considered when planning operations, security and follow-up to a security breach:

- § 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

In addition, SEC regulations (e.g. S-K: 17 C.F.R. subpart 229) require companies to disclose material changes in business or risk exposure in their quarterly and annual reports. The 2003 Final Rule on Management's Reports on Internal Control over Financial Reporting¹⁵ emphasizes that internal controls must provide "reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of company assets."

The importance of information systems and data holdings to modern corporations qualifies many data security breaches as such a material loss or risk. Thus, the quarterly certification that all material internal controls are in place will cover the company's information security policies, procedures and recent experience.

As a result, information security officers now regularly report to senior executives and auditors, who must be satisfied that the corporation has evaluated significant data 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 COSO Framework

In the wake of SOX, the SEC and independent auditors typically refer to the COSO Framework in evaluating internal controls designed to protect assets and ensure compliance with applicable laws and regulations. Named for the Committee of Sponsoring Organizations of the Treadway Commission, the COSO Framework's Enterprise Risk Management – Integrated Framework (ERM) is 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.

¹⁵ See www.sec.gov/rules/final/33-8238.htm

The potential risks to data security associated with corporate laptops would be covered in the “event identification,” “risk assessment,” and “risk responses” aspects of risk management. 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.

While SOX, SEC regulations and the COSO Framework 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. The COSO control framework suggests 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, and should clearly define procedures for securing data on laptops and other portable drives
- 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)
- 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)

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>.

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.