
Data Encryption:

The Foundation of
Enterprise Security

Contents

- Executive Summary3**
- Safeguarding Intellectual Property is Central to Corporate Vitality3**
 - Data Encryption is Vital4
 - A Bleak Picture of Corporate Security4
 - The Costs of Lost Data5
- Encryption is Essential to Meeting Compliance Mandates6**
 - California’s Data Breach Notification Act (SB 1386)6
 - The Health Insurance Portability and Accountability Act (HIPAA)7
 - Gramm-Leach-Bliley Act of 1999 (GLBA)7
 - Sarbanes-Oxley Act (SOX)7
- Enterprises Need a Powerful IT Security Solution That Makes Sense8**
 - Traditional Drawbacks of Encryption8
 - Six Key Benefits of “Best of Breed” Data Encryption Solutions8
- Utimaco’s SafeGuard Security Suite Delivers All the Benefits of Full Encryption9**
 - Utimaco Offers Impenetrable Data Protection10
 - Utimaco Helps Customers Enhance Data Security11
 - About Utimaco11

Executive Summary

A successful organization is only as strong as its intellectual property. From proprietary product information to employee information, sensitive data must be protected from unauthorized access to ensure corporate integrity and confidentiality. In light of burgeoning legislative initiatives, data protection is no longer a corporate choice; it's the law. The consequences of compromising sensitive data—from financial losses to competitive threats—can cripple an organization. Data encryption is the most effective solution for safeguarding sensitive electronic data.

Safeguarding Intellectual Property is Central to Corporate Vitality

Information—such as customer lists, proprietary product details, employee information, and corporate strategy—is invaluable. Without it, a business cannot operate. In an effort to safeguard sensitive, personal, and/or confidential information, most companies have focused their security efforts on perimeter and physical security. Firewalls and routers are examples of the mechanisms most corporations employ to mitigate external threats and ensure their intellectual property is protected. This approach has merit because intruders will often attempt a perimeter attack, such as trying to break through a company's firewall.

But companies are vulnerable to more than virtual attacks by outside parties. They may be exposed to threats—both virtual and physical—from people within the organization, as well as physical attacks from those outside of the company.

Here are examples of the types of threats companies may face:

- **Virtual attack from an internal source:** An on-site contractor could bypass system security to gain access to proprietary competitive data with intent to resell it.
- **Physical attack from an internal source:** A disgruntled employee looking for a way to harm the company might steal a valuable disk or backup tape.
- **Virtual attack from an external source:** A criminal could hack into a corporate network to steal credit card account information or social security numbers.
- **Physical attack from an external source:** Someone could access information stored on a lost or stolen company computer or other mobile device.

External physical attacks are especially common. According to the World Security Corporation, 7%–10% of all notebook computers are stolen or lost each year. For PDAs, the percentage is estimated to be 15%–20%. In the U.S. alone, an estimated 1.6 million PCs have been stolen over the past three years, most of them notebooks. The Federal Bureau of Investigation (FBI) estimates that only 3% of stolen computers are ever recovered.

In today's world, it is necessary to build a security program founded upon the company's most fundamental and valuable asset: its data.

Even more chilling, Gartner Inc. estimates that as many as 90% of laptop PCs and other mobile devices lack protection to ward off hackers. Imagine the consequences if these devices fall into the wrong hands—trade secrets, confidential employee data, and sensitive customer information could be compromised and potentially made public.

So what happens when someone breaches an enterprise's perimeter security, despite the company's best efforts and most extensive precautions? If data is encrypted, nothing happens. That's because the data, no matter how sensitive, can't be read, altered, or used by an unauthorized intruder.

Data Encryption is Vital

Encryption obscures the meaning of a piece of information by encoding it so it can only be decoded, read, and understood by those for whom it is intended. Estimates for the year 2006 put the number of mobile workers at 105 million in the U.S. (two-thirds of its total workforce) and 95 million in Western Europe (half of its total workforce).¹ The layer of security offered by encryption becomes increasingly important as the modern workforce becomes more and more mobile. Encryption also becomes critical on the network if, despite all efforts, someone **does** gain unauthorized access. In today's world, it is necessary to build a security program founded upon the company's most fundamental and valuable asset: its data.

A Bleak Picture of Corporate Security

The San Francisco FBI Computer Intrusion Squad's 2004 *Computer Crime and Security Survey* paints a bleak picture of today's corporate security landscape. Below are survey results from 503 corporations, government agencies, financial institutions, medical institutions, and universities:

- 99% (primarily large corporations and government agencies) detected computer security breaches within the last 12 months
- 98% of respondents have WWW sites
- 80% acknowledged financial losses due to computer breaches
- 52% conduct electronic commerce on their sites
- 44% reported financial losses, which totaled over \$455 million
- 44% detected system penetration from the outside

What types of security breaches occur? Here are a few recent examples:

- In February 2005, Bank of America admitted that in December 2004 it lost unencrypted computer tapes containing account information on 1.2 million federal employee credit cards, potentially exposing workers to identity theft or hacking. According to the bank, the lost tapes may contain sensitive personal financial information, such as cardholders' names, addresses, and social security numbers.²

¹ Gartner, *Public WLAN Hot Spots: Worldwide Trend*

² *CNN Money*, Feb. 25, 2005

- For more than a year, a computer hacker accessed unencrypted servers at wireless giant T-Mobile, using the opportunity to monitor U.S. Secret Service e-mail and obtain customers' passwords and social security numbers.³
- Stockton, CA-based Delta Blood Bank lost an unencrypted laptop to theft at a recent blood drive. The company was forced to notify more than 100,000 donors that their personal information, including name, date of birth, and social security number, had been stolen and that they could be susceptible to identity theft.⁴
- For the third time in a year-and-a-half, Wells Fargo computers containing personal, unencrypted information on thousands of the company's mortgage and student loan customers were stolen. Thieves gained access to sensitive information including addresses, account information, and social security numbers.⁵
- Thieves stole desktop computers from government contractor Science Applications International Corp. Stockholders were warned that their personal information could be at risk because the data was not encrypted.⁶
- Airlines Reporting Corp., an Arlington, VA-based airline ticket processing company, lost two computers, one monitor, and a projector to theft. One of the computers held unencrypted sensitive customer data, including credit card account numbers and travel transaction-related information.⁷

The Costs of Lost Data

According to *Search Security Newsletter*, 60% of all corporate data assets are stored unprotected on PCs, notebooks, and removable media.⁸ Of the 40% of assets that **are** protected, many are safeguarded by only the most basic operating system measures, which are easily thwarted. The cost of losing the data stored on these devices is astronomical. According to the 2004 CSI/FBI Computer Crime and Security Survey of IT security practitioners, the average loss resulting from proprietary information theft is \$2.7 million.⁹ And money is not all that is at risk. Corporations that lose proprietary data may also face a damaged reputation, diminished stock prices, and the wrath of investors, customers, and vendors.

Although the stakes are high and the need to protect data is critical, many companies fail to devote adequate resources to the task. According to IDC, businesses in 2003 spent only a tiny fraction of their IT budgets—4.8%—on security. In response to data security-related crimes and widespread lack of corporate data protection, state and federal lawmakers have introduced numerous pieces of legislation designed to safeguard data integrity, business assets, and consumers' privacy. While some legislation is aimed at securing data itself, other legislation is focused on alerting consumers to any security breaches. Regardless of the legislative intent, compliance is mandatory.

³ *SecurityFocus.com*, Jan. 11, 2005

⁴ *CNET News*, Dec. 22, 2004

⁵ *CNET News*, Nov. 03, 2004

⁶ *ZDNet News*, Feb 14, 2005

⁷ *The Washington Post*, Jan 14, 2004

⁸ *Search Security Newsletter* (April 4, 2003)

⁹ *Network Computing*, Dec. 9, 2004

...businesses today are under extreme pressure to appropriately safeguard sensitive financial data, confidential patient records, and other personal information.

Encryption is Essential to Meeting Compliance Mandates

Thanks to the growing roster of regulatory compliance measures initiated by the U.S. and foreign governments, businesses today are under extreme pressure to appropriately safeguard sensitive financial data, confidential patient records, and other personal information. The California Data Breach Notification Act (SB1386), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act of 1999 (GLBA), and the Sarbanes-Oxley Act (SOX) are just a few of the legislative initiatives that require organizations to protect sensitive information at all times, regardless of its physical location.

That means protecting corporate databases and safeguarding information stored on the corporate network and on mobile devices, including those that are not connected to the corporate network. It means protecting data as it moves from corporate customer to supplier, and safeguarding that data at its destination. It even means protecting data stored on mobile devices purchased and owned by individual employees—not by the company itself—if the employee uses these devices to access corporate networks or data.

Matters are complicated by the fact that each legislative initiative carries its own set of compliance requirements, some more stringent than others. As enterprises strive for ways to manage these diverse requirements, organizational boundaries between IT and other departments are becoming blurred. In the face of SB1386, HIPAA, and the rest, compliance is no longer solely the concern of the CEO, CFO, board of directors, and internal auditing team, and data encryption is no longer the responsibility of only the CIO and IT managers. Today, compliance and IT security are enterprise-wide issues.

To understand how to best address compliance, it is first necessary to examine the requirements and intent of the major legislative initiatives.

California's Data Breach Notification Act (SB 1386)

To respond to the growing incidence of identity theft, one of the fastest-growing crimes in the country, the California legislature passed the Data Breach Notification Act (commonly referred to as SB 1386). Similar national legislation has been proposed. SB1386 requires that businesses in the state of California disclose to residents any breach of the security where **unencrypted** data that includes personal information is reasonably believed to have been acquired by an unauthorized person. Sensitive personal data includes social security numbers, driver's license numbers, California identification card numbers, and credit or debit card account numbers.

Though the law requires formal, immediate notification of a security breach, organizations are exempt from this reporting requirement **if their data is encrypted**. Legislators agreed that encryption provides a "safe harbor." In essence, they said that because **encrypted data** is useless if obtained without authorization, consumers would not be vulnerable to identify theft if a security breach occurred.

That's good news for organizations that encrypt all of their sensitive data. For those that don't, the consequences can be costly. Losing a single unencrypted laptop to theft can result in millions of dollars in unplanned expenses to cover the cost of sending out security breach notifications to thousands of customers and changing their passwords and account information. Add to that the intangible costs associated with a damaged corporate reputation and loss of community goodwill, and the need to safeguard data becomes clear.

The Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA), signed into law in 1996, was originally designed to improve administrative efficiencies in the health care industry by facilitating electronic transactions between health plans, health care providers, and similar entities. However, lawmakers soon realized that transferring individual health records via the Internet, although convenient, raised concerns about the privacy and security of patient-identifiable information. To protect the integrity of confidential health insurance information, HIPAA rules were refined effective April 14, 2003 to include a security standard for sharing personal health information over the Internet.

HIPAA's privacy protection provisions require companies to prevent the unauthorized disclosure of patients' "individually identifiable health information." The penalties of not complying are steep: \$10,000–\$25,000 for each instance of unauthorized disclosure by a health care provider. Intentional unauthorized disclosure carries penalties ranging from \$100,000–\$250,000 and possible jail time for each occurrence.

Gramm-Leach-Bliley Act of 1999 (GLBA)

Also known as the Financial Services Modernization Act, the Gramm-Leach-Bliley Act of 1999 (GLBA) mandates that financial institutions implement IT security measures to prevent unauthorized access to certain sensitive, personal information, such as social security numbers and credit and debit card account numbers. Financial institutions, including banks, lending companies, and brokerage firms, are required to give customers privacy notices that detail the company's information collecting and sharing practices. Companies must also develop and implement an IT security plan that safeguards the confidentiality of sensitive, personal information.

Sarbanes-Oxley Act (SOX)

The Sarbanes-Oxley Act (SOX) of 2002 significantly impacts the processes and accountability for financial reporting in publicly traded U.S. companies. An organization must establish specific enterprise security policies, procedures, and controls designed to protect sensitive information. For example, a company must define what kinds of mobile devices can be used (laptops, cell phones, PDAs), who can use them (employees, contractors, suppliers), where they can be used (home, office, while traveling), what applications can be used on them (e-mail), and what information can be stored on them (customer information, proprietary research, competitor data). In addition, SOX requires

that the company determines what security protection is required (access control, encryption, firewalls) to ensure that data is not lost or stolen. The company must enforce its policies and closely control the use of all mobile devices throughout the organization if it is to remain in compliance.

Enterprises Need a Powerful IT Security Solution That Makes Sense

...companies need to maintain a level of compliance that exceeds even the most rigid requirements by monitoring and enforcing security policies at all times.

In the face of data-related crime and stringent compliance requirements, an effective IT security solution is critical. What constitutes an effective solution? Clearly, complying with each legislative initiative individually makes little sense from a resource-management perspective. Instead, companies need to maintain a level of compliance that exceeds even the most rigid requirements by monitoring and enforcing security policies at all times. Therefore, an effective solution is one that surpasses all compliance requirements, whether set forth in SB 1386, HIPAA, GLBA, SOX, or elsewhere.

An effective solution must employ encryption, strong authentication, plug-and-play management, and authorization controls that can be centrally managed. An effective solution also must secure this sensitive data without negatively impacting an organization's existing workflow or system performance. In fact, the best solution may actually boost system performance and enhance the end-user's experience.

Traditional Drawbacks of Encryption

Despite the obvious need for—and benefits of—encryption, many organizations remain wary. In particular, U.S. organizations remain unconvinced of the necessity for data encryption. While data on more than 60% of mobile devices in Western Europe is encrypted, in the U.S. the figure is less than 5%. That's because early generations of encryption software were difficult to use, had a negative impact on system performance, and occasionally corrupted data. Understandably, many companies refused to encrypt their data, preferring to invest instead in perimeter security. Companies that did encrypt data realized a very limited ROI (Return On Investment) as users often found ways to turn off or circumvent security features that were considered too intrusive.

Six Key Benefits of “Best of Breed” Data Encryption Solutions

While outdated perceptions of encryption still exist, the reality has changed dramatically. Today, data encryption solutions are fast, simple, secure, and transparent to the user. They feature these six key benefits:

- 1. Fast:** Automated encryption solutions run in the background so they don't negatively impact workflow or system performance. In fact, some of today's best solutions enhance system performance by utilizing the most sophisticated and efficient algorithms and compression tools.

- 2. Easy:** Effective encryption solutions are easily rolled out via an enterprise's network without end-user involvement. An encryption system that seamlessly integrates with back-end systems and end-users' computers is key. The best solutions are those that don't demand extensive setup or increase administrative overhead, yet can be quickly deployed without user intervention or training, regardless of the size of the implementation.
- 3. Secure:** If data is encrypted, it doesn't matter if someone breaches an enterprise because the data can't be read or used. Not only does 100% encryption offer a company peace of mind, it frees corporate resources that were previously devoted to perimeter security. While still important, extraordinary perimeter security measures are not as critical if the data itself is adequately protected.
- 4. Powerful:** The best solutions, based on worldwide industry standards, mitigate the possibility of data corruption by encoding and decoding data without fail. The solution must also be robust enough to ensure that the enterprise is in full compliance with all applicable legislative mandates. Of course, the encryption tool should reflect and support—not alter—the company's organization-wide security policies.
- 5. Transparent:** Organizations won't use any security solution if it negatively affects the manner in which users send or receive data. An effective encryption solution allows an organization to secure content transparently without impacting the enterprise's workflow, requiring user training, or forcing users to change their work habits. In fact, the best solutions run without users even being aware they are present.
- 6. Flexible:** An encryption solution should protect data **wherever** it is stored, whether it be on an individual PC, the corporate network, a PDA, a smart phone, a network storage device, or an e-mail server. This way, users have the freedom to access vital company data from their office, while on the road, from a customer's facility, or from anywhere else they might conduct business. If a device is ever lost or stolen, or a hacker breaks into a corporate network, data protection is assured.

Utimaco's SafeGuard Security Suite Delivers All the Benefits of Full Encryption

Whether data is stored in a corporate network or on a mobile device, Utimaco has a proven data protection solution.

Utimaco Safeware is the largest public mobile encryption security firm in the world, offering a full portfolio of IT security products to protect enterprise data. While other companies offer piecemeal or partial encryption solutions, Utimaco is able to protect **all data regardless of its location**. Whether data is stored in a corporate network or on a mobile device, Utimaco has a proven data protection solution. With more than 2.5 million licenses on the market today, Utimaco meets the IT security needs of the majority of the world's government entities and the majority of Global 2000 companies.

Utimaco Offers Impenetrable Data Protection

Leading companies rely on Utimaco because its solutions are the most reliable in the industry. For example, the company safeguards data on PCs by encrypting 100% of the hard disk, and by enforcing a secured user authentication procedure that runs before the operating system boots. Not only are unauthorized users unable to gain access to the data on a PC or portable data storage device, they are also unable to use the device as a tool to enter the company's network. In fact, if a laptop or other mobile device does fall into the wrong hands, the data is securely protected—even if the hard disk is removed. Utimaco's solutions are so reliable that there has never been an incident in which data has been compromised due to a failure of one of its products.

Utimaco's products provide the following benefits:

- The company's solutions are **fast**, and are based on efficient, independently approved and publicly accepted algorithms that deter unauthorized access and hacker attacks.
- The company's full-disk encryption solutions **secure** all information stored on mobile devices and removable media. This superior level of protection ensures that customers maintain a level of compliance that **exceeds** the legal requirements of all applicable legislative initiatives. Organizations that utilize Utimaco's security products can ensure public confidence and protect community goodwill against the penalties and negative publicity associated with violating SB1386, HIPAA, SOX, and other regulations.
- The company's solutions are **easy** to use and administer. Network administrators can centrally control enforceable, automated mobile security practices that ensure data is protected without requiring user intervention or training.
- The company's solutions are **transparent**. For example, Utimaco's SafeGuard® Easy (a PC protection solution) is the most robust security tool in the industry, yet is virtually invisible to end-users.
- Utimaco's **flexible** solutions deliver exceptional scalability that allows companies to secure all databases, from the most valuable server to individual laptops, desktops and other mobile devices. Utimaco also supports most major operating systems for PCs, PDAs, smart phones, and other mobile devices.
- Solutions are **cost-effective**. There are no additional fees for data wiping or hard disk destruction in the event of the sale, disposal, or return of leased devices.
- All solutions are **certified** in accordance with leading industry certifications, including Common Criteria EAL3.

Utimaco Helps Customers Enhance Data Security

Companies worldwide rely on Utimaco to enhance their own products by delivering the most secure data possible to end-users. Take a look at how Utimaco has helped some of its customers.

IBM and Utimaco Join Forces to Fight Data Theft

IBM and Utimaco are working together to help protect valuable electronic data on desktops and notebooks against theft, loss, and unauthorized access. An alliance announced in October 2004 allows IBM to resell Utimaco's SafeGuard Easy hard disk encryption system, which complements IBM's ThinkVantage™ Technologies, a suite of tools designed to make IBM's ThinkPad® notebooks and ThinkCentre™ desktops easy to deploy, connect, protect, and support. If a computer or hard drive is lost or stolen, data encrypted using SafeGuard Easy cannot be accessed without the correct authorization.

Sony VAIOs Protected by Utimaco

All Sony VAIO notebooks and desktops now incorporate SafeGuard PrivateDisk, which creates a virtual, encrypted disk drive to protect valuable, confidential data. For the user, there is no difference between using a "virtual" disk drive and a "normal" disk drive, as both drives create, save, and copy files in the traditional way. "By working together with Utimaco, Sony is reacting to the growing demand for security solutions from private and SME users," announced Gildas Pelliet, Vice President, Sony Information Technology Europe. "This makes us one of the first suppliers to provide this type of encryption solution together with their hardware for the end-user sector."

"By working together with Utimaco, Sony is reacting to the growing demand for security solutions from private and SME users."

—Gildas Pelliet,
Vice President,
Sony Information
Technology, Europe

Utimaco Secures Construction and Design Information for Leading Auto Maker

The auto development center of one of the world's leading auto manufacturers is implementing Utimaco's SafeGuard Easy encryption solution on all mobile end-user devices as a way to address the risks associated with heightened competition—including the possibility that valuable research and development information could fall into the wrong hands. SafeGuard Easy ensures that the hard disk is encrypted transparently and automatically, and thus protects the saved data from access by outsiders.

About Utimaco

Utimaco, renowned for protecting sensitive data, has pioneered groundbreaking security solutions for mobile and wireless computing. The company developed its first enterprise IT security software solution nearly 25 years ago. Today, Utimaco is a global industry leader. Utimaco has offices in 11 countries, including the U.S., as well as partners located throughout Europe, Asia, Australia, and Africa. For more information on Utimaco and its security solutions, visit www.utimaco.us.

Utimaco Safeware, Inc.

10 Lincoln Road, Suite 102

Foxboro, MA 02035

Phone (508) 543-1008

Fax (508) 543-1009

utimaco[®]
s a f e w a r e

www.utimaco.us

© 2005 Utimaco Safeware AG. All rights reserved.

The information in this document is subject to change without notice.
This document is believed to be accurate and reliable, but the statements
contained herein are presented without express or implied warranty.

All SafeGuard Products are registered trademarks of Utimaco Safeware AG.
All other named trademarks are trademarks of the particular copyright holder.