A LINOMA SOFTWARE WHITE PAPER:

Beyond the Security Breach: Protecting Sensitive Data Using Encryption & Key Management

EXECUTIVE SUMMARY:

Security breaches cost business millions of dollars each year, yet data theft is increasing at an alarming rate. At the same time, disclosure laws addressing data breaches are dramatically increasing company liabilities. Many of the data breach incidents result from network intrusions, theft of portable devices, and unauthorized access by internal employees.

What has happened to the touted security of our IT systems? How did our organizations arrive at this juncture? What can be done to minimize the exposure costs while better securing the information assets?

This paper identifies how organizations need to deploy new solutions to protect their information assets from theft and misuse. It explores the landscape of legal liabilities and identifies the technical hurdles facing both management and IT. It demonstrates how the use of encryption can reduce the exposure of data theft without hampering the productivity of the current information flow. Finally, it maps how management can deploy stronger technologies to lock, monitor, and audit the use of sensitive information within the larger information system.

LINOMA SOFTWARE

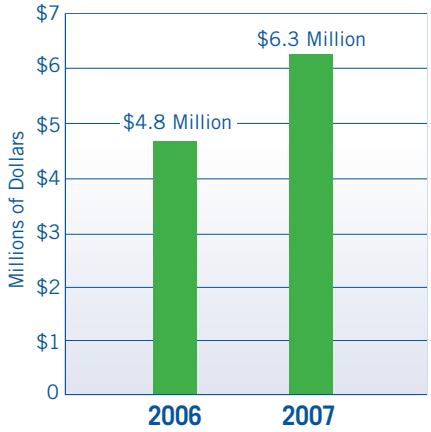
Publication date: November 21, 2008

The Business Problem

According to a recent estimate published in a Forester Research report entitled "Calculating the Cost of a Security Breach", the average cost of a data breach can be between $90 and $300 per record, averaging about $197 per record lost. These costs include legal fees, notifications through call centers, lost employee productivity, regulatory fines, stock plummets and customer losses. According to "The Ponemon Institute", this cost rose at an astounding rate of 100% between 2005 and 2006, and the Gartner Group believes it will continue to rise at 20% through 2009.

Cost Per Record Compromised

Average Total Per Data Breach Incident



If Forester's research is accurate, the cost to the victimized companies in legal and notification charges alone will likely be in the billions of dollars.

So what happened to the touted security of our information systems?

What About Security?

No matter how "secure" your systems appear to the auditors and security experts monitoring your information systems – no matter how confident your IT staff may be – the risks of your company experiencing an incident of data theft are real, and they continue to grow daily.

How can this be? How can our systems be both technically secure and vulnerable at the same time?

To address the exposures, we need to look at the problem from both a technical and a business management perspective. There are no simple fixes, but with a full grasp of today's security landscape, there are steps – beyond the obvious – that you and your team of IT professionals can take to minimize your organization's exposure and liability.

The Growth of Data Theft and Globalization

Let's first look at why data theft today has become such a high-profile concern for companies in a globally connected economy. Today our IT systems are hosts to:

- Interconnected Supply Chain Management (SCM).
- Online ordering with credit cards.
- Integrated Customer Relationship Management (CRM).
- Enterprise Resource Planning (ERP).

In the past, integrated information services of this magnitude could only be afforded by the largest of organizations when automated interactions between business partners, vendors, and customers were relatively few. Computing systems were islands of information used primarily for internal accounting activities.

Today, in our globally connected economy, even the smallest of companies are supporting their business models with many more interconnected, highly automated processes and services. The data contained in these systems is expensive to collect and maintain while it fuels the productivity our businesses, and drives the company's success. Likewise, the value of this information concentration also makes our IT information systems primary targets for organized, highly sophisticated thievery.

46%

of organizations interviewed expect a serious data loss at least once a year.

Source: Symantec Corporation, January 2008

Open Standards

At the same time, the nature of the expanding global marketplace requires "openness" – in the form of well-published standards – to foster and expand the company's virtual services. Our IT departments have responded to the challenge by building the technical infrastructure necessary to enable these services. In fact, IT's success has often been measured by how quickly these new information services could be expanded to a wider audience of users and business partners.

Yet this expansion of IT services – using the open communication services and standards – places incredible strains on our traditional methods of securing our information systems.

The Limits of Access Control Security

Traditionally, IT's approach to securing the data within corporations focused upon restricting the access to services and the sources of information. This is often called Access Control, and it works by assigning access privileges to information resources through a hierarchy of user profiles and classes.

Access Control is a proven technology for securing information systems, and industry standards are robust. Nonetheless, there are limitations when it comes to protection of the content of files by Access Control alone.

For instance, as users come and go – or their jobs change within an organization – the assigned security levels of the files they once accessed are not always kept up to date by security officers. Also, classes of users sometimes overlap, making it difficult for security officers to know precisely what access is permitted, and what should be restricted. And

finally, if a user profile is compromised, the contents of all the related user's files can be accessed and potentially stolen.

Moreover, companies no longer are homogenous computing centers, running a single operating system. i5/OS, Windows, Linux, AIX, UNIX, and even Mac OSX computers are now frequently deployed simultaneously in the networks of organizations, and these operating systems use different technical schemes to provide Access Control security. Consequently, as files move from system to system, there is no guarantee that the Access Control scheme of a copied file will be sustained. This heterogeneity of security exposes our data to potential misuse and theft.

Ultimately, though Access Control security schemes are good for keeping unwanted people from obtaining access to the data and services, they can fail. And when they fail they have proven to be insufficient to protect the contents of the data itself.

1 out of 3 computer professionals **admit** to accessing confidential data.

Source: MSNBC, June 2008

An IT Conundrum: Expanded vs. Restricted Access

This is a conundrum for our IT shops. On the one hand IT must implement new technologies to permit the wider use of data to meet the challenges of an interconnected economy. On the other hand IT must limit what those authorized users can see and how they can use the content of the data itself.

But technical analysts insist that any network can be hacked; any password to a user profile can be stolen; any laptop PC can be lost.

Even off-site disaster recovery services and portable devices are exposures that IT must address. Everyone knows that a backup tape can be misplaced or stolen. A USB thumb drive, PDA, or cell phone – complete with password codes and access to other databases – can easily go missing. On those powerful portable devices, copies of confidential data can disappear without a trace.

Once a device is lost, what is to prevent its contents from being scrutinized, extracted, examined and misused?

Unfortunately, this IT conundrum ends up as a management problem that may inflict serious financial repercussions upon the organization itself.

The Management Crisis

If a burglar breaks into your business and rifles through files and desk drawers, everyone knows the steps of recourse: Notify the police, file a complaint, and inventory the missing items. It's a tedious process, but at least it's well-understood. Then you change the locks.

Unfortunately, when a burglar hacks into your system, or steals a backup tape of your data, the processes for reporting and evaluating the damage are less clear. Law-enforcement jurisdictions are not well-established, and the recourses available to the organization are limited. Even if the missing data is recovered, there is seldom a means of determining how it has been accessed or compromised.

Notification: The Conflict

Moreover, a majority of states have implemented laws that require the victimized companies to report the data theft – not only to the law enforcement officials, but to the very business customers whose identities may have been compromised. These well-intentioned notification laws do nothing to punish the thief or recover the information, and the cost to the victimized company can be exorbitant. Worse, data theft often tarnishes the reputation of the victimized company.

Average Business Loss Per Incident

Assessing the Damage

Perhaps just as disturbing is that companies that have been victimized by data theft often do not always know precisely what data has been stolen.

For instance, if a database system is hacked, it may have included sensitive financial data, credit card numbers, social security numbers, trade secrets, payroll data, or other highly sensitive information. Some of this information could be used by a hacker to steal personal identities and create untold ramifications for your organization and its customers.

If a hacker penetrates the network, merely determining where his virtual trail has led can take weeks to unravel. And with hundreds of in-house or network-attached peripheral devices now connected to the system, the number of potential break-in portals has multiplied.

Changing the Locks

Protecting the systems after media is lost or a breach is encountered is also a problem: Which locks need to be changed? How does management know the extent of the exposure? And what about the actual data that has been lost? Is the company subject to legal recourse? Even if management has a comprehensive plan for notifying both authorities and customers, what are the implications for the organization? More importantly, how does management prevent future theft from occurring?

Missing Management Tools

Many organizations do not have the proper tools to protect or even control how the content of the organization's data is being used. The limit of the best operating system security schemes may simply mean that management receives a report that identifies which files have been accessed. If a user profile has been compromised, management has nothing to help determine how its data may be compromised, or even the level of the threat that the breach represents.

The theft of laptops with personal information about current and former employees of Anheuser-Busch affects more than 90,000 people nationwide.

Source: Tampa Bay Business Journal

Legal Requirements

Perhaps just as difficult is the realization that legal standards, rules, guidelines, and regulations are still evolving, and that existing laws are inconsistent and sometimes contradictory.

- Forty-four states within the US have data theft notification laws. But each law has differing requirements and different penalties for the companies that fail to comply.
- The Payment Card Industry (PCI) has its own security standards that dictate how credit card information must be stored and transmitted. But these standards do not secure other important information that may be contained in other files.
- The U.S. Treasury requires its own form of security for electronic funds transfer. But these requirements only apply when funds are being electronically transferred.
- The American National Standards Institute has guidelines detailing how key personal identification numbers must be protected. But these guidelines say nothing about how other data elements should be secured.
- HIPPA, Sarbanes-Oxley, and numerous other compliance regulations provide overlays of guidelines and requirements to which management must adhere. Unfortunately, these guidelines are open to interpretation by auditors, IT staff, and management.
- Internationally, ISO 7799 and the New Basel Capital Accord have built stringent requirements for how member organizations must preserve their information assets from accident and misuse. These requirements, nonetheless, are silent when dealing with the specifics technical underpinnings of preservation.

Sorting through these requirements takes considerable time. Interpreting and implementing them can be tedious. And yet, in many cases, ignoring them can lead to serious liabilities for the company. What is worse, even when they are implemented, they do not provide management with the tools it needs to vouchsafe the security of critical content contained within files and database systems.

"The message to ChoicePoint and others should be clear: Consumers' private data must be protected from thieves. Data security is critical to consumers, and protecting it is a priority for the FTC, as it should be to every business in America."

Source: Deborah Platt Majoras, Chairman of the Federal Trade Commission.

Potential Liabilities

Since 2004, the Federal Trade Commission (FTC) has claimed that a company's failure to take reasonable measures to protect customers' personal information is itself an unfair practice in violation of the FTC Act.

In the past three years, the FTC has brought more than a dozen enforcement actions under this theory, with settlements requiring tighter data security measures and payment of significant fines, as well as the FTC's legal expenses.

The most publicized enforcement was against data broker ChoicePoint, Inc. In January, 2006 the FTC fined ChoicePoint $10M in civil penalties and $5M in consumer redress for a breach of 130 thousand consumer financial records that were stored in its databases.

Regulation Trends

Moreover, according to predictions by some legal analysts, political pressure will lead to legislative changes that give plaintiffs the right to sue over private data security breaches.

For instance, Congress has passed the "Identity Theft Enforcement and Restitution Act" which aims squarely at identifying the liability standards which companies will face, should their data be lost or stolen. At this writing, the bill awaits the signature of the President, but – if signed – it will add significant liability exposure to companies that suffer from data theft.

In addition, recent data theft cases have created concerns that company executives could become personally liable if their organization's data is compromised.

Business As Usual vs. Data Asset Protection

Business managers are facing the same conundrum as IT. On the one hand, global business models require them to build information assets that can be readily exchanged to drive business plans. On the other hand, managers need to preserve and protect the information assets in a way that shields the organization from lawsuits and liability.

Organizations need stronger tools for controlling and protecting sensitive information assets. Quite simply, when management "locks" the contents of a file – containing sensitive identity information, financial data, credit card data, or trade secrets – business and legal requirements demand that the lock can not be broken.

Data Encryption – Part of the Solution

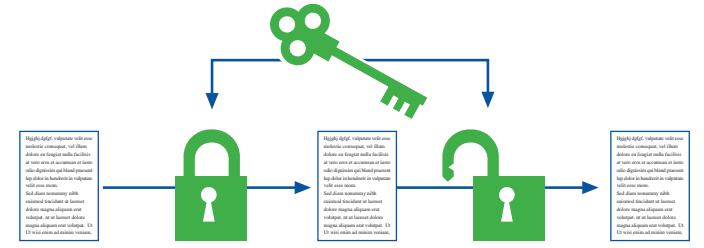
Today many organizations have begun using data encryption to keep sensitive information out of the hands of thieves. Data encryption uses mathematical algorithms to obfuscate the "plain text" data in such a way that it appears as a nonsensical string of 1 and 0s called "cipher text." The data can only be decrypted using "cipher" key(s) to enable a decrypting algorithm to return the information back into plain text. These algorithms are complex and offer strong protection.

Data encryption has been available for decades. The Data Encryption Standard (DES) was first introduced in 1976, and was enhanced for the electronic payments industry by IBM in 1978 with a stronger standard called Triple DES (TDES).

In early 2001, these and other security algorithms were technically overtaken by the Advanced Encryption Standard (AES) – the standard approved by the U.S. National Security Agency for encrypting top secret governmental information. It was not until 2002 that the Advanced Encryption Standard (AES) became readily available to business users. Today, AES is the most widely used method of encrypting data.

AES is a Symmetric Encryption Standard because it uses a symmetric key that can both encrypt and decrypt data. Symmetric Encryption is often called a secret encryption standard because the encryption

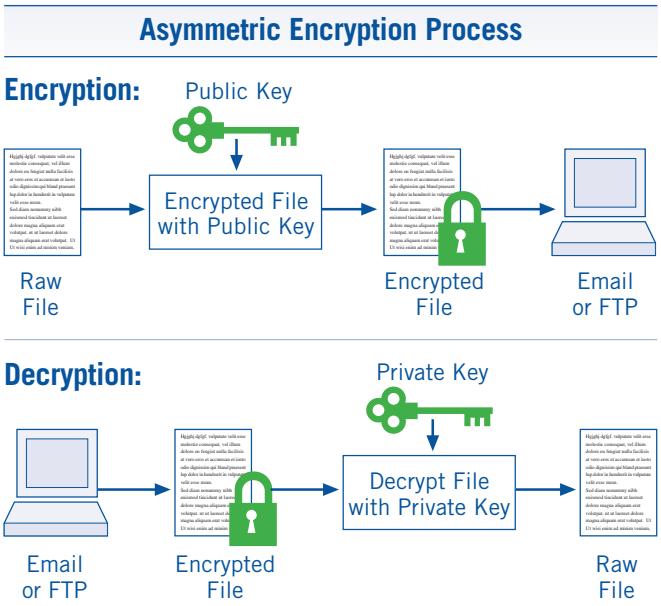
Symmetric Encryption Process



… the harshest of penalties being discussed by the Ministry of Justice in the United Kingdom is a two-year prison sentence for the most serious of offenses. All it would take is one case in one country to enact a penalty such as this, and we would likely see other countries following close behind with their own laws.

Source: "Windows in Financial Services", Microsoft Corporation, Don Canning, November 2006

keys must be kept secret to prevent data theft. IT departments today regularly use Symmetric Encryption schemes to protect internal databases and backup tapes.



Asymmetric Encryption Standards – also called "Public-Key" encryption, utilizes two keys: A public key to encrypt and a private key to decrypt data. Asymmetric Encryption Standards, along with digital signatures, are used in email communication and Internet transactions (i.e. FTP) where the sender needs to ensure the confidentiality of a communication, and/or the recipient needs to validate the identity of the sender.

IBM and other operating system vendors have incorporated some of these data encryption standards as a set of services for programming applications, though they do not provide easy methods of implementation.

Yet, to be effective against data theft, data encryption systems need to be integrated with the application software that runs our enterprises. Today this integration is lagging behind in many organizations.

With Data Field Encryption, the **database itself is accessible** by normal operating system functions, such as read, copy, backup, or recovery, even though the **individual fields are encrypted.**

Limitations of Common Encryption Deployment Techniques

Historically, organizations have relied upon two approaches when encrypting information: Full-disk encryption and File/folder encryption.

- Full-disk encryption protects everything on a hard disk volume or storage pool.
- File/folder encryption encrypts individual files and/or folders that have been identified as security risks.

Both techniques have advantages, but both create potential areas of concern. The downside of Full-disk encryption is that it requires user training to access the information while substantially decreasing the performance of the information system. The downside of File/folder encryption is that – once decrypted – it leaves an unencrypted copy that is unprotected and which may be copied and misused. File/folder encryption often places too much responsibility upon the authorized user who has decrypted the file or folder.

Data Field Encryption

More recently, a newer approach – called Data Field Encryption – has been successfully deployed by an increasing number of organizations for protecting relational database systems. Instead of encrypting the entire disk, folder, or file, Data Field Encryption will

encrypt only specifically identified fields within a database, turning the contents of those fields into protected resources.

Data Field Encryption is a significantly stronger and more resilient technique for securing targeted fields than either Full-disk or File/folder encryption. Data Field Encryption minimizes the performance issues associated with Full-disk and File/folder encryption while placing rigorous protection on fields such as social security numbers, credit card numbers, etc.

With Data Field Encryption, the database itself is accessible by normal operating system functions, such as read, copy, backup, or recovery, even though the individual fields are encrypted. The decryption process for the individual fields can be activated through functions/procedures (APIs) that are implemented within the organization's applications.

Data Field Encryption prevents copies of the decrypted resource from being left in the open: When the accessing program terminates, the decrypted image of the field resource is automatically destroyed in the computer's memory. Meanwhile, if the file is lost or stolen – or even copied to another system – the encrypted fields remain secure until they are accessed with the appropriate decryption key.

Data Transmission Encryption

Unless otherwise protected, all data transfers, including electronic mail and FTP, travel openly over the Internet and can be monitored or read by others.

Given the volume of transmissions and the numerous paths available for data travel, it is unlikely that a particular transmission would be monitored at random. However, hacker tools, such as "sniffer" programs, can be set up at opportune locations on a network to simply look for and collect certain types of data (e.g. user ids, passwords, credit cards numbers, social security numbers, etc).

Potentially, the open architecture of the Internet can allow those with specific knowledge and tools to alter or modify data during a transmission. Steps must be taken to ensure that all data is maintained in its original or intended form.

Technologies are available so the Internet may be used for secure electronic commerce transactions. Recommended encryption standards for securing data transmissions include Open PGP, SFTP (FTP over SSH) and FTPS (FTP over SSL). These encryption standards utilize asymmetric keys for authenticating the sending and receiving parties.

Because encryption renders information unreadable to an unauthorized party, the information remains private and confidential while in transit. Furthermore, encryption technology can provide assurance of data integrity as some algorithms offer protection against forgery and tampering.

Encryption Keys: The Management Issue

For each data field or transmission, management can choose the appropriate encryption approach and a unique security key. This creates the opportunity for a security hierarchy that management can structure and control.

Unless otherwise protected, **all data transfers,** including electronic mail and FTP, travel openly over the Internet and **can be monitored** or read by others.

For instance, one security key can be used to protect fields containing social security numbers, and a different security key can be used for fields containing bank account numbers. Even if the decryption key for one data element is compromised, the other encrypted data will remain locked.

The opportunity to utilize multiple encryption keys can become chaotic, however, if it is not planned and managed properly. One of the major problems with many encryption implementations is the lack of good key management. How these keys are created, how they are managed, and who is permitted access to the keys can present serious security and operational problems that organizations must address.

Today, some organizations treat encryption key management as a technical IT problem that is never fully addressed by the organization itself. Sometimes decryption keys are even hard-coded (in the clear) within the application code itself. This may result in a more efficient operation – hiding complexity from operators, but is hardly a secure practice.

Some IT teams rely upon stand-alone packaged key management systems that do not fully integrate with the company's encryption solution and business applications. These key management systems can require substantial training and can result in disruptions and slowdowns in daily workflows. Moreover, they are subject to theft themselves if they are not adequately protected.

Still other IT teams decide to build their own home-grown systems to create and manage key resources. Yet building a custom key management system is a complex undertaking that can be costly and is prone to its own security problems.

Implementing Best Practices for Effective Key Management

In order to provide true security for the encryption solution, there are a number of significant features found in effective Key Management Systems:

- Inherent security: A mechanism to protect the encryption keys themselves, preferably using some method of Master Key encryption.
- Authority-based: A mechanism that identifies the users who can create and manage the encryption keys.
- Policy-based: A mechanism that establishes a policy structure for creating and utilizing the encryption keys.
- OS-based security integration: A mechanism that integrates the inherent security of the management system with the Access Control security schemes of the base operating system.
- Random key generation: A secure mechanism that automates the generation of strong encryption keys using random-number algorithms.
- User transparency: A mechanism that restricts the retrieval of the actual value of the encryption keys, yet delivers keys transparently and secretly to the appropriate application.
- Key management utilities: A mechanism that organizes and maintains keys in one or more key stores.
- Audit-ability: A mechanism that produces detailed reports on what applications and users have accessed and used the security keys to gain access to the protected data.

Key Management System Features:

- Inherent Security
- Authority-based
- Policy-based
- OS-based Security Integration
- Random Key Generation
- User Transparency
- Key Management Utilities
- Audit-ability

All of these base features should be implemented with the purpose of protecting the information assets of the company, while providing the most transparent, operationally neutral and integrated solution for encryption and decryption of data. The best solution removes the details of encryption from the visibility of the users, while offering management a secure, expandable, and configurable tool for controlling and preventing data theft.

Most importantly, the tool which IT deploys should provide rigorous auditing features, so that when data is compromised, management will know who – and by what processes – sensitive information has been accessed. Without such audit-ability, the organization has less recourse for controlling the damage inflicted by a data security breach. With such a tool, management can identify not only the exposure, but also the steps necessary to prevent further damage from future breaches.

A Pathway Out of the Data Theft Nightmare

Information systems are on notice: Customers, employees, and business partners are justly wary that the safety of the sensitive information they have placed in trust with the organization may be compromised. Regulators and law enforcement officials have shown that their first recourse after a data breach is to penalize the companies that are careless with their data resources. The industry trends in data theft and security breaches support these concerns and their oversight.

IT and management teams are both appropriately concerned. They are in search of better tools, better systems, and better techniques that can address these serious flaws in security, and are looking for ways to plug the organization's exposure to data theft. They are also obviously seeking ways to avoid the repercussions of serious breaches in the security of the information system.

A comprehensive system of data encryption – when properly architected and judiciously deployed – is one pathway out of the security dilemma. Using advanced data encryption technologies that thoroughly integrate with the current application and operating system software, IT can provide management with those better tools, with stronger accountability, audit-ability, and better assurances that the data in our systems is under a stronger and more resilient lock and key.

A comprehensive system of data encryption – when properly architected and judiciously deployed – is one pathway out of the security dilemma.

About Linoma Software

Founded in 1994, Linoma Software provides innovative technologies to consistently meet evolving needs for encryption, data transmission and application modernization. Linoma Software has a diverse install base of over 3,000 customers around the world including Fortune 500 companies, non-profit organizations and government entities.

For more information about Linoma Software products and services, visit our website: www.LinomaSoftware.com or call us at 800.949.4696.

Electronic Contact Information

Sales: sales@linoma.com

Support: support@linoma.com

Website: www.LinomaSoftware.com

Phone Numbers

Toll-free: 800.949.4696

Outside USA: 402.944.4242

Fax: 402.944.4243

Address

Linoma Software
1409 Silver Street
Ashland, NE 68003 USA