GO ANYWHERE®
Managed File Transfer

GUIDE *(Cybersecurity)*

Defending Against Data Breach

Developing the Right Encryption Strategy

"You are going to be hacked. Have a plan."
Joseph Demarest, Associate Executive Assistant Director
FBI Criminal, Cyber, Response and Services Branch

EXECUTIVE SUMMARY

No matter how secure your information systems appear and no matter how confident your IT staff may be, the risks of your company experiencing a data breach are real, and they continue to grow daily.

Information security breaches cost companies millions of dollars each year, and incidents continue to rise. While government and industry regulations have been implemented that penalize the company if their sensitive data is compromised, protecting against the threat of data breach is difficult. Take, for example, the multiple ways unauthorized access can occur: theft of portable devices, lost paper files and external storage devices, improper access by employees, network infiltration from outside entities, and more.

Data breach incidents are not a temporary statistical aberration, but instead represent a growing epidemic. Given the cost to both companies and their customers, it's critical that IT teams develop a solid strategy that utilizes the most effective tools.

This white paper has several objectives.

- Examine the problems that create a higher risk for data breach.
- Explore the regulatory landscape.
- Describe the technical hurdles facing both management and IT.
- Demonstrate how the right data encryption technologies can reduce the exposure of data theft without hampering efficient workflow.

Most importantly, this paper offers recommendations for how IT management can deploy strong security technologies to encrypt, monitor, and audit the access and use of sensitive information within an organization's system.

Data Breaches Wreak Havoc

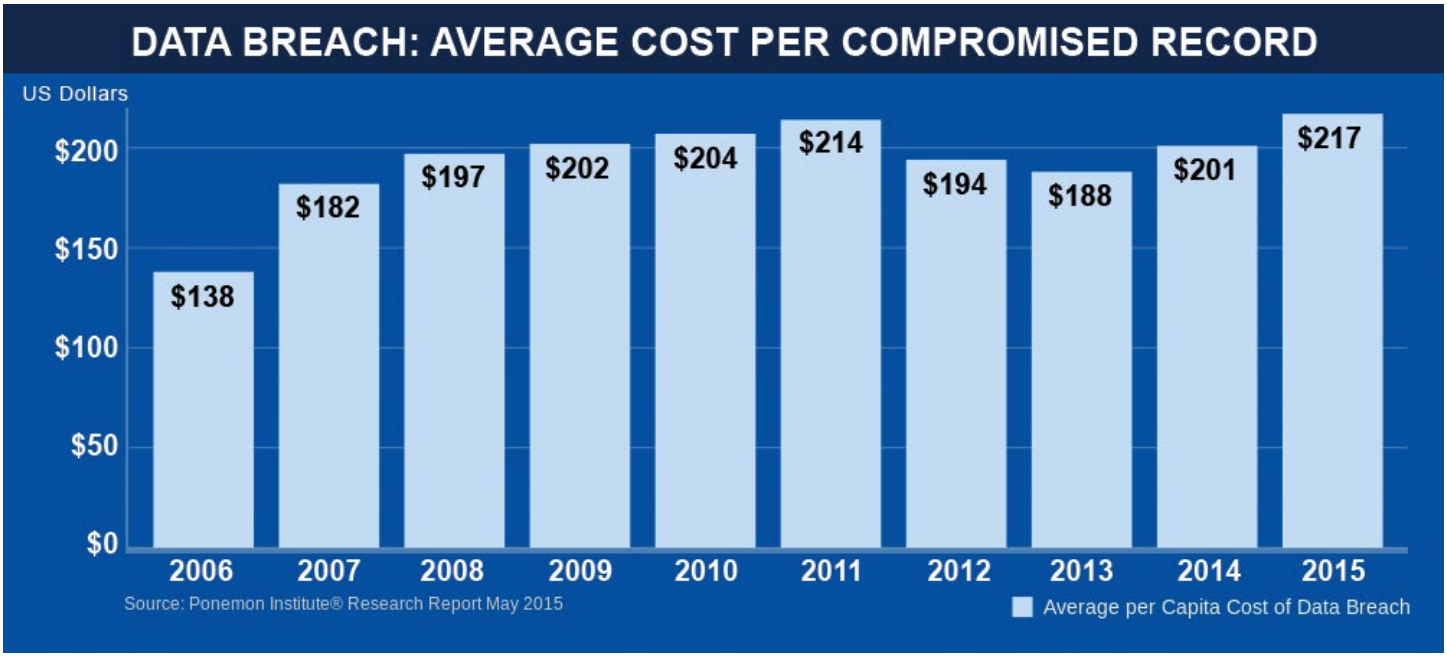
According to estimates published by the Ponemon Institute's "2015 Cost of Data Breach Study: United States," the average corporation that suffers a data breach will pay $6.5 million to resolve the issue. That's about $217 per record to cover legal fees, the cost of notifying each affected person, and regulatory fines, as well as lost employee productivity, stock price dips and indirect customer losses.

Anthem reported in February of 2015 that nearly 80 million records related to members and nonmembers were compromised in a massive data breach. Anthem, a US health insurance provider, said that cyber attackers targeted one of their parent company IT systems and obtained personal information dating back more than a decade.

Unencrypted information, including names, dates of birth, social security numbers, addresses, email, employment and income data were accessed – the perfect material for identity theft, fraud, or any number of criminal activities. While the projected cost seems to fluctuate as time passes, the potential liability to Anthem, using Pomenon's estimates could be substantial.

In 2015, there were several other reports of large data breaches in the news:

- Ashley Madison, the online dating and social networking site reported losing up to 37 million records.
- The Office of Personnel Management lost 25.7 million government worker records.
- The Identity Theft Resource Center (ITRC) reported more than 175 million records were exposed in 690 separate data breach incidents for the year.



Another clear trend is that not only is the number of incidents increasing, the cost per incident has also dramatically increased by more than 57% since 2006.

Where is this epidemic leading us, and how tolerant will the public be with the continued threat that their private information may be compromised?

Multiple Factors Impact Data Security

While most IT staffs are vigilant in the design and monitoring of their companies' computers, servers and networks, what used to define the parameters of data security has changed as more portable devices become common, and as hackers continue to gain sophistication.

Tackling the problems with data security requires examination from both a business management and an IT perspective. By integrating these two perspectives with a clear understanding of today's data security challenges, companies can begin taking proactive steps to minimize both exposure and liability.

Increased External Exposure

The overview of the data security environment begins by remembering that companies are connected globally like never before.

Not long ago, integrated information services were used only by the top tier organizations and automated interactions among business partners, clients, and customers were relatively rare. At that time, computing systems were islands of information, used primarily for internal accounting and database activities. Security procedures revolved around keeping internal systems safe and protected, without much concern for external penetration.

52% of Security Professionals expect to be hacked within the next 12 months.

SOURCE: CyberEdge Group 2015 Cyberthreat Defense Report North America & Europe

Today most companies' information systems are highly connected to other systems and are managing multiple workflows including:

- Interconnected supply chain management (SCM);
- Online ordering with credit cards;

- Integrated customer relationship management (CRM); and
- Enterprise resource planning (ERP).

The data a company network manages every day is expensive to collect but it's integral to an organization's success in today's competitive global marketplace. However, because this information is so valuable, IT information systems are primary targets for organized, highly sophisticated, and malicious attacks.

Open Standards

The paradox for companies doing business globally is that in order to compete and connect, they must be "open" – in the form of well published standards – to foster and expand the company's virtual services. IT departments have responded to the challenge by building the technical infrastructure necessary to enable these new information services to facilitate expansion to a wider audience of users and business partners. Yet in striving for more open access, incredible strains have been placed on the conventional methods of maintaining tight security around data and systems.

Access Control Security Limits

The most common approach to securing data has been to restrict who could see or retrieve services and information by assigning access privileges through a hierarchy of user profiles and classes. This method is referred to as access control.

Unfortunately, while access control is a proven technology for securing information systems and industry standards are robust, there are limitations when it is implemented as the sole form of protection.

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

Another challenge is the heterogeneity of platforms running within a single company's networks. Windows, IBM i, Linux, AIX, UNIX, and Mac OSx platforms all 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, increasing the likelihood that data could be exposed to potential misuse and theft.

While access control security schemes are good for keeping unauthorized people from obtaining access to protected data and services, they can fail, leaving file contents vulnerable.

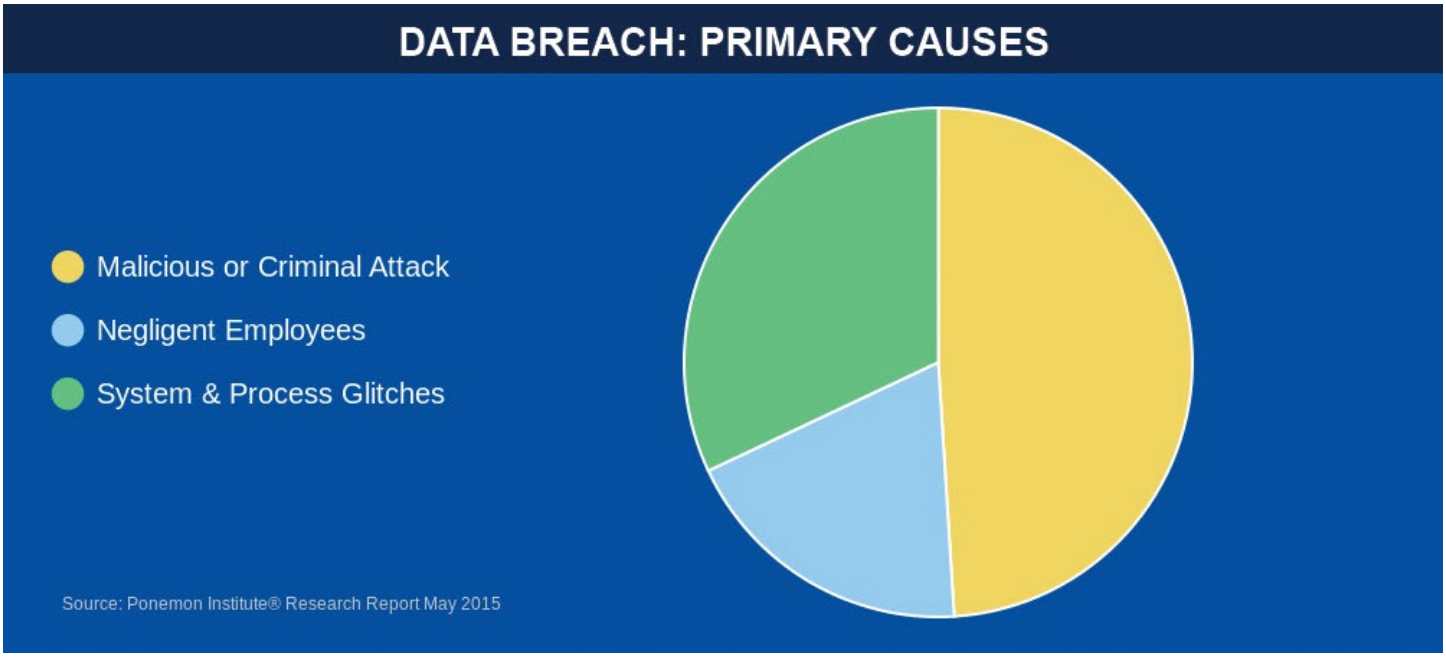
Expanded vs. Restricted Access

So back to the paradox of becoming more open while protecting networks and data from increasing security threats. On 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 control the levels of user authorization and enforce limits on what authorized users at all levels can see and how they can use the content of the data itself.

Adding to the pressure is technical analysts' belief that any network can be hacked; any password to a user profile can be stolen; any laptop PC or mobile device can be lost.

Even off-site disaster recovery services and portable devices are exposures that IT must address. Everyone knows a backup tape can be misplaced or stolen, and a USB thumb drive, a PDA, or a 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.

As files move from system to system, there is no guarantee the access control scheme of a copied file will be sustained.



These issues must be addressed by both IT and management, since a security breach by any of these methods may result in serious financial repercussions for the entire organization.

The Management Crisis

If a burglar breaks into an office and rifles through files and desk drawers, most people know what to do: notify the police, file a complaint, inventory the items that may be missing and change the locks. It's a tedious process, but at least it's well-understood.

Unfortunately, when an intruder hacks into your network or steals your data, the procedure for reporting and inventorying the damage is much less clear. Law enforcement jurisdictions are not well-established and the recourses available to the organization are limited.

Assessing The Damage

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 every customer, vendor, employee and partner 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 tarnishes the reputation of the organization itself.

Perhaps just as disturbing is that companies that have been victimized by data theft often struggle to identify exactly 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. If a hacker penetrates the network, merely tracking his virtual trail can take weeks. 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 compromised? Even if management has a comprehensive plan for notifying both authorities and clients, what are the implications for the organization? Is the company subject to legal recourse? More importantly, how does management prevent future theft from occurring?

Choosing The Right Tools

Many organizations do not have the proper tools to protect

or control how their data is being used, nor do they have comprehensive auditing and reporting options. The best management at these organizations can hope for is that a network intrusion generates a basic report that identifies which files have been accessed. Yet if a user profile has been compromised, management often has no way to learn how that data may be misused, and difficulty evaluating the level of the threat that any breach represents.

Legal Requirements

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

- Forty-seven 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. However, these standards do not address the security of important information that may be contained in other files.
- The U.S. Treasury has specific requirements to ensure the security of electronic funds transfers. 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.
- HIPAA, 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 27002 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 specific technical underpinnings of preservation.

Since 2010, criminal attacks on healthcare organizations have increased 100%.

SOURCE: Ponemon Institute, LLC 4th Annual Benchmark Study on Patient Privacy & Data Security

Sorting through these requirements takes considerable time. Interpreting and implementing them can be tedious. And yet, ignoring them can lead to serious liabilities for the company. Worse yet, even when a company is striving to meet these requirements, management often lacks the tools to prove its compliance.

Regulation Trends

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

For instance, Congress passed the "Identity Theft Enforcement and Restitution Act" in 2008 which aims squarely at identifying the liability standards to which companies will be held accountable, and the punitive consequences should their data be lost or stolen.

In addition, continuous data theft incidents have created concerns that company executives can become personally liable if their organization's data is compromised.

Business As Usual vs. Data Asset Protection

Business managers are facing the same conundrum that IT battles. How do they build information assets that can be readily exchanged to drive business while still protecting the information assets in a way that shields the organization from lawsuits and liability?

Quite simply, once management "locks" the contents of a file containing sensitive information (identity, financial data, credit

Continuous data theft incidents have created concerns that company executives can become personally liable if their organization's data is compromised.

card data, or trade secrets), business and legal requirements demand that the lock cannot be broken.

Data Encryption is Part of the Solution

Data encryption helps organizations keep sensitive information out of the hands of thieves. Data encryption uses mathematical algorithms to obfuscate the "plain text" data so that it appears as a nonsensical string of 1s and 0s called "cipher text." The data can only be decrypted using "cipher code" key(s) that enable a decrypting algorithm to return the information back into plain text. These algorithms are complex and offer strong protection. For instance, AES encryption can utilize keys of up to 256 bits in length, creating extremely robust encryption security.

AES is a symmetric encryption standard because it utilizes a single key that can both encrypt and decrypt data. Symmetric encryption is often called a secret encryption standard because the encryption keys must remain secret to prevent data theft.

Today, IT departments regularly use symmetric data encryption schemes such as AES or 3DES to protect internal databases and backup tapes.

Limitations of Common Encryption Deployment Techniques

Historically, organizations have relied upon two approaches when using symmetric encryption: 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 primary disadvantage of full-disk encryption is that while it can minimize the risks if the physical disk drive is stolen, this method cannot protect an organization from an online attack by a hacker or rogue employee. Once a hacker gains access to the system, all data will be automatically decrypted regardless of which application (or tool) is running and regardless of the user's credentials. Another downside of full-disk encryption is that it requires increased 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

An approach that's gaining popularity is data field encryption which 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 encrypts only specifically identified fields within a database, turning the contents of those fields into protected resources.

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. 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 memory of the computer.

Data field encryption is a more resilient technique for securing targeted fields than either full-disk or file/folder encryption.

Management can choose a number of different encryption standards to secure the data, and can generate separate, unique keys for encrypting these individual fields. This creates the opportunity for a security hierarchy that management can structure and control.

For instance, one key can be used to protect fields containing Social Security numbers, and a different key can be used for fields containing salary information. Meanwhile, if the file is lost or stolen – or even copied to another system – the encrypted fields remain secure until they are presented with the appropriate key. Even if the key for one data field is compromised, the other encrypted fields are still locked.

Managing Encryption Keys

The opportunity to use multiple encryption keys does come at a cost, however. One of the major problems with many encryption systems is the basic management of the security keys themselves. 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.

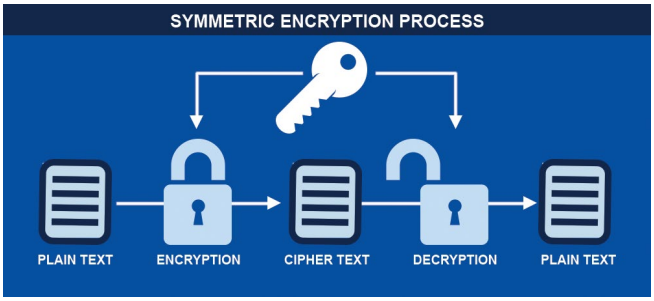
Many companies treat encryption key management as a responsibility of the IT department, and therefore it is never fully addressed by the organization itself. Sometimes keys are even hard-coded within the application code itself. This may result in a more efficient operation – hiding complexity from 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 software applications. These key management systems can require substantial operator training and can result in disruptions and slowdowns in daily workflows. Moreover, they are subject to theft themselves if not adequately protected.

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

Implementing Best Practices for Data Field Encryption

In order to provide true security for data field encryption, there are a number of significant features that the key management system should provide.



- **Inherent security:** Protects the encryption keys themselves, preferably using some method of master key encryption.
- **Authority-based:** Identifies the users who can create and manage encryption keys.
- **Policy-based:** Establishes a policy structure for creating and utilizing encryption keys.
- **OS-based security integration:** Integrates the inherent security of the management system with the access control security schemes of the base operating system.
- **Generation methodology:** Automates the generation of strong encryption keys using strong random-number algorithms.
- **User transparency:** Restricts the retrieval of the actual value of the encryption keys, yet delivers the keys transparently and secretly to the appropriate application.
- **Key management utilities:** Organizes and maintains keys in one or more key stores.
- **Auditability:** Produces detailed reports about what applications and users have accessed and used the security keys to gain access to the protected data fields.

Each of these essential features should be designed and implemented to protect the information assets of the company while providing the most operationally neutral and integrated solution for encryption and decryption of data. The best solution remains invisible to the user, but offers management a secure, expandable and configurable tool for controlling and preventing data theft.

Most importantly, the ideal data protection tool should

The best solution remains invisible to the user, but offers management a secure, expandable and configurable tool for controlling and preventing data theft.

provide rigorous auditing features so that when data is lost, management will know who has accessed the sensitive information, and by what means. Without such auditability, the organization has very few options to assess and recover from the damage inflicted by a data security breach. When the right data protection tool is employed, management can identify not only the exposure, but also the steps necessary to prevent further damage from future breaches.

CONCLUSION

A Pathway Out of the Data Theft Nightmare

Customers, clients, and business partners are understandably anxious that the safety of the sensitive information they have placed in trust with companies 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.

Organizations have made progress, but the costs are still too high and the liabilities to the companies are still rising. Both IT and management teams are in a continual search for better tools and techniques to drastically reduce or eliminate the organization's exposure to data theft – to preserve their reputation, protect those customers and others who would be affected, and avoid the repercussions of fines and notification costs.

A comprehensive system of data encryption – if properly designed and judiciously deployed – is one pathway out of the security dilemma. IT departments can use advanced data field encryption technologies that thoroughly integrate with the current application and operating system software. The right system can provide better management with stronger accountability, auditability, and better assurances that the data stored in the organization's system is under a stronger and more resilient lock and key.

Automated Field, File and Backup Encryption Solutions for the Enterprise

Crypto Complete™ protects sensitive data using strong encryption, integrated key management and auditing on the IBM i operating system. Crypto Complete allows organizations to encrypt database fields, backups and IFS files quickly and effectively with its intuitive screens and proven technology.

GoAnywhere® MFT is an enterprise-ready managed file transfer solution which streamlines and encrypts the exchange of data between your systems, employees, customers and trading partners. It provides a single point of control with extensive security settings, detailed audit trails and reports.

Learn more about the GoAnywhere Managed File Transfer solution at www.GoAnywhere.com.

HelpSystems
103 S 14th St
Ashland, Nebraska 68003
(402) 944.4242
(800) 949.4696
goanywhere.sales@helpsystems.com
www.GoAnywhere.com

helpsystems

www.helpsystems.com

About HelpSystems

Organizations around the world rely on HelpSystems to make IT lives easier and keep business running smoothly. Our software and services monitor and automate processes, encrypt and secure data, and provide easy access to the information people need.