AES Encryption Strategies

A White Paper for the IT Executive

THIS PAPER IS FOR THE CIO AND IT EXECUTIVE who makes decisions about data security on their Enterprise server platforms. Many IT executives are now faced with the urgent need to secure sensitive data on their computing systems in a very short period of time. Decisions need to be made on what data security solutions to use, which projects need priority, and how to make the best use of available resources. The need to deploy better data security has arisen quickly and many IT executives feel the need for more information. This paper will try to provide helpful information and suggestions for a plan of action.
Data Security - Everything Changed on February 15, 2005

On February 15th, 2005 Choicepoint announced a significant loss of private data due to criminal activity originating outside the company. This day marks the point at which a sea change in attitudes about data security began. The loss of data by Choicepoint was followed by announcements by several other companies of significant data losses. Bank of America, DSW, Citigroup, MCI, CardSystems, and many others experienced the loss of employee and customer data. It is likely that there will be many more losses in the days and weeks ahead.

Many of the companies who have experienced data loss are not negligent when it comes to security. Some have teams of qualified security experts trying to prevent unauthorized access to their networks and internal systems. The problem is this: criminals have become more adept at exploiting the weak points in a company’s security plan. When they can’t get access to internal networks, they steal archival tapes. When they can’t get access to a mainframe database with millions of records, they steal a laptop with a large extract of that data. When they can’t get access to the central database, they get access to a PC and use FTP or ODBC to steal data. Our Enterprises did not get worse on the issue of security, criminals got better at what they do.

The reaction on the part of the public and regulatory bodies has been dramatic. Card issuers such as Visa and Mastercard rushed new rules into effect, and imposed very short deadlines for merchants to meet the new security requirements. States have moved forward very rapidly with new notification requirements modeled after the California privacy notification law. Sarbanes-Oxley rules have tightened about system security and data security. And the federal government is moving towards new regulation.

One Thing Is Certain:
Everything changed on February 15th. From this point forward all systems must be developed with data security as a key component. Existing systems without adequate data security must be replaced or modified to incorporate data security to meet regulatory compliance.

The IT manager is faced with new demands from senior management to limit the risk of data loss, and to meet Visa PCI security requirements. With very little lead time, decisions have to be made, and resources committed, to remediate data security problems in core applications. In many cases this looks like a daunting task similar in scale to the Y2K problem, but without the time to prepare. A large Enterprise may have hundreds or even thousands of applications that are affected. The impact may be severe.

Key Issues in Data Security

The data security solutions you select now will be in use for many years to come. Over time, these solutions will be integrated into almost every major application in your IT environment. Selecting the right solution now is an important first decision, whether that decision is to develop data encryption capability in-house, or to work with a data security solutions provider.

Here are some key questions to consider when making this decision:

Who will be able to provide us with mature guidance on the appropriate use and implementation of encryption?

Encryption is a complex technology - do we have the expertise and resources to do this on our own?

Data security is incorporated into a number of regulations that control our Enterprise, are we using the right technology to satisfy these regulations? And will our solution help us minimize legal liability?

Will our data security solutions easily extend to new requirements? We need to secure credit card numbers today. What about tape encryption, spool file reports, and IFS files? Will our data security technology lend itself to new uses?

We transfer data between diverse systems in our internal network, and between customers, suppliers, and employees. Will our solutions meet all of these needs?

In this paper we’ll look at these questions and suggest some ways to arrive at an answer you can live with today and into the future.
Data Encryption Technologies - What You Need To Know

Selecting the right encryption technology is important. Some encryption technologies, such as DES, do not provide enough security now that computers have become so powerful. Other encryption technologies are secure today, but will soon not meet the minimal requirement for security due to the advancing power of computers. Triple DES falls into this category. Other encryption technologies are secure, but do not satisfy federal and international standards. Twofish, RC2 and RC4 are examples of this type of encryption technology.

Only one encryption technology meets all of the requirements for strength, longevity, and regulatory approval – the Advanced Encryption Standard (AES). AES has been adopted by the federal government as an approved encryption technology under the FIPS-197 standard. AES is accepted by the Health Insurance Portability and Accountability Act (HIPAA), and is accepted by all credit card issuers for data security including Visa, Mastercard, Discover, American Express, JCB, and others. AES has also been incorporated into Pretty Good Privacy (PGP) encryption which is used by banks, insurance companies, benefits providers, and most major financial institutions.

Selecting a data security solution based on AES is a safe and wise decision. It provides the best encryption security, the best regulatory coverage, and the best position for future development.

Choosing the Right Partner

When you look for a partner for data security solutions you will want someone who has a mature set of solutions and a history of support for your server platforms. They should be able to provide you with a wide range of solutions. Data that is encrypted on one server must be able to be decrypted on another server with a different operating system. The right partner will have faced these issues and it will show in their product suite.

Little Known Fact:
Did you know that strong encryption can be rendered useless by an incorrect implementation? It's true – when you encrypt fields in a database with a strong encryption method like AES, you have to take care to use the right AES mode. Using AES encryption in Electronic Code Book (ECB) mode with the same key for each record may provide weak security. The right implementation uses AES in Counter (CTR) or Cipher Block Chaining (CBC) mode resulting in strong encryption on even very small fields.

The right partner will also have a firm grounding in the Enterprise application server world. Each computing platform has particular requirements and best practices. A security product needs to be tuned to the requirements of a specific platform. For example, installation on UNIX is different than Windows which is different than Linux. Your data security solution must incorporate platform knowledge in order to provide a truly secure approach to data security.

Identifying Data Security Needs

Some of your data security needs will be easy to identify. If you store credit card numbers in a database, these will have to be secured with strong encryption. However, there are probably many places in your applications, reports, and processes that need data security.

Consider starting with a list of all potentially sensitive data in your systems. Do you store the following information?

- Credit card numbers
- Social security numbers
- Date of birth
- City of birth
- Drivers license number
- Zip code
- Maiden name
- Prompt for lost password (favorite pet?)

Develop a Strategy That Insures Some Early Successes

CIOs and IT Managers are under pressure to show quick progress on data security. Getting some early wins can be important to consolidate the support of upper management, and build confidence among members of the IT team. For this reason we suggest that you develop a list of data security needs and put priority on some tasks that can be
completed quickly. For example, encrypting archival tapes may be a task that you can complete very quickly. Or, securing the transfer of payroll data to your outside vendor might be a very quick win.

It is probable that encrypting data in your database files will have application impacts that take time to resolve. If you make this your first achievable goal, you may put your first success too far out in the future, especially if you have a number of applications that need changed. You can prioritize your data security initiatives to get early successes.

Securing Tape Archives

There are two basic ways you can secure tape archives:

- Use hardware encryption devices
- Use software encryption solutions

Each method has advantages and disadvantages. Hardware encryption may take longer to implement, have larger initial acquisition costs, be susceptible to hardware failure, and disrupt existing data recovery plans. Hardware encryption solutions may provide faster backup than software solutions.

Software solutions have the advantage in fitting well with your business recovery plan, allowing for selective encryption of saves, cost less, and be faster to deploy. Additionally, software solutions often incorporate audit trails that are important for regulatory compliance. Software solutions are typically more extensible, and software vendors provide updates to increase the value and scope of their offerings.

Hardware Tape Solutions, Consider This:
Hardware encryption devices will not integrate easily with your High Availability software, and will not provide security for data that is mirrored to an HA system. You will still need to secure data at the file level using software encryption, and the result will be double encrypted data that multiplies the chance of key loss.

You can expect that securing your archive tapes will be a relatively quick process. If there are application impacts they are usually limited to your nightly backup and restore processes. In most cases the application impacts will be minimal.

Securing Tape Transfers to Vendors and Suppliers

If you are sending sensitive data to a customer or supplier via tape, be sure to secure that data on the tape. The requirement for securing this type of tape data has the additional requirement that your trading partner needs to be able to decrypt the data. The de facto standard for exchanging data securely with trading partners is Pretty Good Privacy (PGP). PGP is implemented on a wide variety of platforms and is widely used by banks, insurance companies, and benefits providers. Consider using PGP for this type of data exchange to insure the best cross-platform support for encryption and decryption.

Important Compliance Note:
If you use PGP for data encryption, be sure your solution supports Additional Decryption Keys (ADK). ADK is an important component of regulatory compliance and audit. Without ADK you will not be able to verify the data contents of an encrypted transfer. Not all encryption solutions support ADK.

Securing Internet Data Transfer

If you are transferring data to your customers or vendors using the Internet, be sure to secure the data or the connection. The most common way of securing the data is with PGP encryption. PGP is an open standard for encryption, and is supported on many different platforms including Windows, UNIX, IBM mainframe, Linux and the IBM iSeries. It is the most common way of securing files before transfer over the Internet.

You can also secure the actual connection to your trading partner by using a secure connection technology such as SSL. If you transfer data with File Transfer Protocol (FTP) you can use the SSL FTP connection type to encrypt the data during the connection. If you transfer data using a web connection technology such as HTTP, you can secure the connection with SSL using the HTTPS (secure) connection method. For email transfers you can enforce data security by using a policy-based security solution such as PGP Universal. If you use one of these secure connection methods, be sure that your trading partner has adequately secured the data after receiving it. Data may be secure during the transfer, but exposed after the session is complete.
Securing Fields in Database Files

The most critical data security issue for Enterprise customers is to get sensitive data encrypted in their database files. Once field, or column, level encryption is implemented the risk of significant data loss is minimized. Encrypting at the field level will exempt your company from privacy notification requirements, and greatly improve overall security.

Encrypting at the field level may be the most difficult part of securing your sensitive data. For most users field level encryption requires changes to their existing applications. And if the data is shared with applications on different platforms, solutions must be found for distributed encryption and decryption services. How extensive the changes to your applications are depends on a number of factors. In the next section we discuss the typical issues you will face when making these application changes.

There Is No Magic Bullet:
It may be tempting to consider using stored procedures to implement field encryption to avoid modifying applications. You should avoid using these types of solutions. They reduce data security by automatically decrypting data in normal copy functions and FTP transfers, and they can have severe performance impacts on your batch applications.

If you are faced with the requirement for near term PCI credit card security compliance, you should work on the applications that store and access credit card information first. Be sure to use a methodology that will also support Sarbanes-Oxley compliance even if you do not have to meet these requirements now. If you have any customers who are subject to Sarbanes-Oxley it is likely that you will also need to be compliant at some future time.

Application and Database Impacts

While you are likely to have to make some changes to your database files, using the right technology will help minimize these impacts. You should use an encryption technology that does not require expanding the size of a field when encrypting. And the use of field level encryption routines should be simple and well documented. When implementing field level encryption in your database, you can expect to encounter issues in the following areas:

- Indexes using sensitive data will become unusable, forcing application changes that use these indexes.
- Application programs will need to be changed to encrypt and decrypt sensitive data.
- Sensitive data stored in numeric fields may become invalid after encryption.

For credit card lookup you may have an index over your database by credit card number. Once you encrypt that credit card number the index will be useless. This means that your applications will need to use a different method of locating credit card transactions. You can locate credit card transactions by customer name, date range, zip code, or other mechanism. But this will mean changing your index and application code.

Applications that store or retrieve and use encrypted data will need to be changed to perform the actual encryption and decryption tasks. Any application that inserts new records into the database will need to be changed to encrypt the field before the new record is added to the file. Any application that uses the encrypted data must be changed to decrypt the data before it is displayed, printed or exported. You should not have to change an application that retrieves a record with encrypted data, but does not use the encrypted field. There is no requirement to decrypt a field if it is not used.

Numeric database fields can present a challenge for encryption. The act of encrypting a numeric field will make it invalid and result in database errors in your applications. For this reason most customers convert numeric fields to character format before starting their encryption project. Since you don’t normally need to perform mathematical operations on sensitive data, this is often a simple change.

Point of Sale Systems

Retail and distribution customers with point of sale terminals face an extra challenge. Data must be secured at the point of sale terminal, secured during transfer to the central server platform, and secured when stored in a database file.

In most cases the vendor of the retail software will provide the encryption solution for storage of data on the POS system itself. If you maintain your own POS applications you will need to modify them to perform this task.
On a daily basis, the POS transaction journals and settlement transactions are transferred to the central server for processing into back end systems. The data must be encrypted during the transfer process. This means that an encryption method must be found that is compatible with the solution you use on the central server platform. Your encryption software vendor should provide you with guidance on how you can accomplish this requirement.

Business Data Integration & Cross-Platform Considerations

In the modern Enterprise it is common to find applications on a variety of platforms including Windows, UNIX, Linux and IBM i and z mainframes. These applications share data in order to provide application services on the platform that is best suited for them. When sensitive data is shared across these systems it is necessary to find a way to encrypt and decrypt data across a platform boundary.

The most common way for real time applications to work with encrypted data is to use the services of an encryption server. An encryption server can securely store encryption keys, provide real-time encryption and decryption services, and scale to handle larger volumes of transactions. When you acquire a data security solution be sure to understand how your software vendor will help you meet this requirement.

When applications share data over a platform boundary, but do not need to encrypt or decrypt data in real time, you can use standard file encryption techniques for data transfer. For example, an Windows application might use WinZip to encrypt an entire file before transferring it to another server. An application on the Windows server can decrypt the data before processing it into the Windows application. You could also use PGP encryption for this type of transfer.

Audit Trails for Regulatory Compliance

You may need to meet regulatory compliance requirements to identify all users who have access to sensitive data and provide reports of actual access to specific information. This means that your encryption solution should provide you with the ability to automatically collect user and job information and to report that information to authorized security administrators. Of course, information collected about access to sensitive data must also be securely stored in the audit file. Since some sensitive data may require access logging, while other sensitive data does not require access logging, your encryption solution should allow you to implement this under your control. Access logging adds additional overhead to your encryption solution and you will want the maximum flexibility in how you deploy your solutions.

Imagine Being Asked This Question:
Who on our system has looked at credit card number 1111 2222 3333 4444 between February 2nd and February 21st? What job were they running, and what was the date and time of their access? Can your data security solution help you answer this question?

The Resource Impacts of Data Encryption

Data security comes with a price. In addition to any initial implementation costs, you will incur system resource costs. Your CPU utilization will increase as you encrypt and decrypt data. There is no strong encryption solution that will not make additional demands on your system. Fortunately, many server vendors are adding encryption support in hardware. But you will still need to do performance analysis and capacity planning as a part of your development process. Be sure your software vendor provides you with the tools you need to assess the impact on your system. The only way you can accurately assess the impact on your system and applications is to actually use the encryption software on your system. Be sure your data security software provider provides a means of real impact assessment on your system through a functional trial of the software.

Review HR Processes for Proper Background Checks

Unfortunately, a number of companies have experienced data loss through criminal activities of their employees. A customer support representative might have access to sensitive data as a part of their normal job. A programmer might have access to large amounts of data. If your company handles sensitive information be sure to review pre-employment practices for adequate background checks. Rectify oversights in this area by getting current background checks. You should expect your employees to understand and comply with this requirement.
Review Customer & Vendor Data Exchanges

Are you exchanging sensitive data with a supplier or customer? You have a right to expect your trading partners to insure the security of data on their systems. Implement a data security mechanism such as PGP for data exchange, and ask your trading partner to meet the same data security goals that you set for your own organization.

Townsend Security

Despite an organization’s best efforts, their data will get out. The best way to secure critical information is with strong encryption and key management.

Townsend Security provides NIST-certified encryption and logging solutions for the Enterprise. Our encryption, key management, tokenization, and logging solutions protect sensitive data from loss, whether it rests within, or is transmitted outside, of your organization.

Our certified database encryption and key management solutions are guaranteed to meet the encryption and key management meet or exceeds the standards in PCI, HIPAA, HITECH and more. Organizations worldwide rely on Townsend Security for their data privacy needs.

Web: www.townsendsecurity.com
Phone: (800) 357-1019 or (360) 359-4400
International: +1 360 359 4400
Email: Info@townsendsecurity.com