
Protecting Backup Media with AES Encryption

Abstract:

Although most businesses scrupulously protect the personal customer information that they collect and store onsite, companies often do not consider the security issues involved when sending backup media to offsite storage for safekeeping. As recent news coverage has shown, offsite media can be lost or stolen while in transit, exposing sensitive information to potential misuse. By using AES encryption on backup data, a business can feel confident that sensitive customer information will remain safe and secure, even if the backups tapes are lost or stolen.

11/07/05

Copyright © 2006 EMC Corporation. All rights reserved.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC², EMC, and Retrospect are trademarks of EMC Corporation. All other trademarks used herein are the property of their respective owners. All other brand names are trademarks or registered trademarks of their respective owners.

[S70140106V1]

Protecting Backup Media with AES Encryption

Table of Contents

Introduction	4
Who Needs AES Encryption for Backup Media?	4
Learning the Hard Way.....	4
Regulatory Compliance.....	5
Health Insurance Portability and Accountability Act (HIPAA)	5
California Senate Bill 1386.....	5
Payment Card Industry (PCI) Data Security Standard.....	6
Other Regulations	6
Using Backup Software Certified for AES Encryption	7
How AES Encryption Works	7
Common Sense Guidelines for Pass Codes	8
Selecting a Strong Pass Code.....	8
Avoiding Weak Pass Codes.....	8
Guarding Your Pass Code	9

Introduction

Are you capturing sensitive customer information such as social security numbers, bank records, credit card information, or medical history? If you store this kind of information electronically, you need to take a serious look at how you protect your backups, especially if you store backup media offsite.

Who Needs AES Encryption for Backup Media?

Most organizations take considerable precautions to ensure the security of their computer networks. Physical access to the servers is limited. Networks are protected with cutting-edge technology. Access to data is restricted to authorized personnel. But these security measures protect data only when it is onsite.

Almost all backup strategies incorporate some form of offsite storage for disaster recovery purposes. Any entity that collects sensitive information—about customers, employees, business partners, or organization members—must closely examine how backup media is protected. How secure is your backup media when it goes out the door? Are you confident that your offsite data is protected if it falls into the wrong hands, or do you have a potential security breach waiting to happen?

If you are storing information on backup media that is not strongly encrypted, you could face damaging public disclosure, civil action, or even criminal penalties—not to mention public embarrassment and loss of confidence among customers—if offsite backups are lost, stolen, or accessed by others. It's amazing how easily tapes can disappear. The driver for a courier service forgets to lock the truck door, and a bump or a sharp turn in the road sends your tapes onto a city street. A forklift in a storage facility rips a hole in a storage carton, and your tapes tumble on to a loading dock.

Learning the Hard Way

In 2005, several high-profile financial institutions and corporations announced that backup tapes containing personal information about customers or employees were missing. The tapes were not encrypted and the personal information they contain remains in a potentially compromising position. Until the tapes are recovered, they could still fall into the wrong hands and the information they contain could be misused. The incidents were given extensive coverage in the news media. Time and effort were spent notifying individuals whose information was lost and ensuring that the lost information had not been used to gain unauthorized access to accounts.

Bank of America

Financial records of 1.2 million federal employees – including several U.S. senators – participating in a U.S. government charge card program were lost when Bank of America backup tapes disappeared en route to a backup center.

Time Warner Inc

Personal information on about 600,000 current and former employees of Time Warner Inc. disappeared when 40 tapes went missing while in transit to a storage facility.

Citigroup

Information on about 4 million Citigroup customers was lost when tapes disappeared while in transit to a credit bureau.

Ameritrade Inc

Four backup tapes fell out of a shipping package that was damaged in transit. Three of the tapes were found, but the fourth tape, containing account information for 200,000 Ameritrade clients, is thought to have been lost or accidentally destroyed.

Protecting Backup Media with AES Encryption

Regulatory Compliance

As more personal data is being stored electronically, public concern is growing about the security of that data. In response, federal and state agencies—and even industry associations—are implementing regulations and guidelines to guarantee the safety of digital information and guard against identity theft.

These regulations affect not just large financial institutions or corporations. Many larger companies and institutions are requiring their business partners, associates, and contractors to implement secure encryption practices as part of the conditions for doing business. As more companies rely on electronically stored customer information, privacy and security regulations will affect more businesses over time. By using AES encryption to protect backup media, you can make it easy to comply with current regulations as well as any future regulations.

AES encryption is the strongest and most reliable method for complying with regulations governing the confidentiality of personal information on backup media. It prevents unauthorized individuals from accessing the information if media is lost, stolen, or misplaced. AES is the encryption standard selected by the U.S. government after a three-year competition. SMBs can be confident that their backups are being protected by using a strong encryption technology such as AES 128-bit or 256-bit encryption, the strongest cryptographic technology currently available.

The following sections describe major regulations and industry guidelines that can be successfully addressed using AES encryption.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA applies to health care organizations or any entity maintaining medical or health insurance record for employees or members. HIPAA mandates that these entities implement a secure backup and disaster recovery strategy for electronically stored personal health information. HIPAA also requires entities to protect against any reasonably anticipated unauthorized uses or disclosures of information. Non-compliance can result in fines as high as \$25,000 per violation and could lead to expensive litigation by patients whose information was compromised.

HIPAA is broad and deep, affecting virtually all healthcare organizations – healthcare providers, health plans, public health authorities, healthcare clearing houses, and self-insured employers – as well as life insurers, information systems vendors, various service organizations, and universities. Health records also include “health transactions” such as health claims, health plan eligibility, enrollment, payments for care and health plan premiums, claim status, injury reports, and coordination of benefits.

California Senate Bill 1386

Sometimes called the California Database Breach Act, this California state law requires disclosure when the unencrypted personal information of California residents falls into the hands of unauthorized personnel. Disclosure may require public announcements, press releases, and advisories with widespread and embarrassing press coverage. The law applies to state agencies and thousands of companies who do business in California or with California residents. Other state and federal laws have been patterned after the California Database Breach Act.

The California Database Breach Act is far reaching. It applies to state agencies and companies in California, as well as the thousands of companies that store private information and do business in California (the fifth largest economy in the world) or have online commerce or content relationships with California residents. While the law doesn't specifically require companies to encrypt data, using AES encryption for offsite backups is the most trustworthy method for guaranteeing the security of backups that contain information on California residents.

Protecting Backup Media with AES Encryption

Payment Card Industry (PCI) Data Security Standard

PCI is designed to safeguarding sensitive data and prevent identity theft by establishing a compliance program for merchants and service providers that store, process or transmit credit card data. It is a collaborative effort between Visa and MasterCard that is endorsed by other credit card companies in the United States that have established compliance programs based on the standard for member merchants and service providers that store, process or transmit cardholder data. This standard affects tens of thousand of companies throughout the world. PCI recommends using encryption as the “ultimate mechanism” to protect stored data. Merchants that fail to comply with CISP can face financial penalties.

Visa’s program is called the Cardholder Information Security Program (CISP) and applies too retail, mail/telephone, and e-commerce payment channels. Merchants that fail to comply with CISP can face hundreds of thousands of dollars in penalties. This standard affects tens of thousands of companies, big and small, throughout the world.

Table 1 The following table provides information about important encryption-related regulations.

Regulation	HIPAA	California Senate Bill 1386	Payment Card Industry (PCI) Data Security Standard
Who’s Affected	<ul style="list-style-type: none"> ☛ Health organizations including doctors, dentists, vision care providers, medical centers, and hospitals ☛ Health plans, public health authorities, clearing houses ☛ Life insurers, information systems providers, self-insured employers, service organizations, universities 	<ul style="list-style-type: none"> ☛ State agencies and companies that store electronic information for any California resident ☛ Companies affected by copycat legislation in other states and at federal level 	<ul style="list-style-type: none"> ☛ Member merchants of Visa, MasterCard, and other credit card companies that store cardholder data ☛ Visa-specified retail, mail/telephone and e-commerce payment channels
Penalty for Non-compliance	<ul style="list-style-type: none"> ☛ Encryption is optional, but if a court finds safeguards inadequate, organizations can face <i>severe criminal and civil penalties</i>, and fines up to \$25,000 	<ul style="list-style-type: none"> ☛ Civil lawsuits for damages caused by disclosure (e.g. identity theft) ☛ Bad press, impact on revenues and customer satisfaction 	<ul style="list-style-type: none"> ☛ Visa merchants that fail to comply face hundreds of thousands of dollars in penalties
Solution	With AES encryption, offsite backup media cannot be accessed	If data is encrypted, no need to disclose lost or misplaced backup tapes	Encrypting backup data ensures compliance

Other Regulations

A number of other laws and regulations can also be partly of entirely addressed by implementing AES encryption to protect offsite backup media.

Sarbanes-Oxley Act

The Sarbanes-Oxley act requires corporations to keep detailed financial information and retain copies of communications that relate to business decisions. All this information needs to be backed up and stored.

Protecting Backup Media with AES Encryption

Although Sarbanes-Oxley does not stipulate that data be encrypted for protection, most companies will want to encrypt their backups to ensure that confidential corporate data is protected while in offsite storage.

Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act is intended to ensure the security and confidentiality of records and information for customers of financial institution. The law includes a Safeguards Rule, which requires banks, securities firms, insurance companies, and other companies providing financial products and services institutions to implement administrative, technical, and physical safeguards to protect customer information.

Federal Information Security Management Act

The Federal Information Security Management Act requires government agencies to have adequate security for information and information systems. The law is only applicable to the government sector, but it can affect contractors or other businesses that provide or managed information for government agencies.

Using Backup Software Certified for AES Encryption

Data can be securely protected by using backup and recovery software such as EMC Retrospect, which has built-in AES encryption capabilities to protect backup media stored offsite. AES encryption is the most powerful form of encryption available to the public. As of 2005, no successful attempts to crack AES encryption have been reported.

As noted by the U.S. government's Office of Management and Budget, AES will provide agencies with a new encryption method "designed to be secure for at least 20 to 30 years.... When suitably strong encryption algorithms are employed and implemented with appropriate assurance, encryption can prevent the disclosure of communicated or stored data to unauthorized parties."

By delivering the highest level of data encryption available, backup software that uses AES encryption can protect against embarrassing, costly, and legally sticky situations that can result if backup tapes are lost or stolen. Companies can feel confident their data is protected against unauthorized access if tapes are lost or stolen. Because the tapes are encrypted, personal data is never compromised and confidential corporate information is never exposed to public scrutiny. There is no need to notify customers. No additional money or time needs to be spent protecting accounts from unauthorized access.

The U.S. government's National Institute of Standards (NIST) has established Federal Information Processing Standards (FIPS) to ensure that software products meet U.S. government specifications for AES encryption. FIPS has also been adopted by the Communications Security Establishment of the Government of Canada (CSE) as the encryption standard for protecting electronic information in Canada.

In July 2005, EMC Retrospect 7 for Windows became the first backup and recovery software to receive FIPS Publications 197 certification from NIST for 128-bit and 256-bit Advanced Encryption Standard (AES) encryption, the strongest form of encryption available. Companies that store confidential information are increasingly turning to NIST and FIPS Pub 197 as the security standard for backup media. To view the official list of software, hardware, and firmware products with FIPS certification for AES encryption, visit the National Institute of Standards and Technology (NIST) Web site at <http://cs-www.ncsl.nist.gov/cryptval/aes/aesval.html>.

How AES Encryption Works

AES encryption uses two components to encode and decode information: an encryption key and the AES algorithm. AES key sizes are 128, 192, or 256 bits. The security of the data depends on the number of characters in the encryption key, with 256-bit encryption being the strongest form.

Protecting Backup Media with AES Encryption

The encryption key transforms plain text into code and reverses the process to decode encrypted material. Decoding information with a different key would result in nonsensical information. Most people will select a password—or more correctly a pass code—to use as an encryption key. AES transforms the pass code using a key-derivation algorithm, which adds random bits to the password to expand it to a 128-bit, 192-bit, or 256-bit key. A larger key size means that there are more bits you can use to scramble the data. Longer keys require more work to unscramble the data. A long enough key requires a lot of work to decode. AES encryption has not been broken as of 2005, and encryption experts believe that for years to come, computers will not have enough power to decode AES-protected data.

A larger key size also adds complexity to the AES algorithm. The algorithm creates a series of tables and populates the tables with the bytes of data being encrypted. The algorithm uses information contained within the encryption key to replace some data in the tables, shift data to new positions inside the table, and derive mathematical formulas for combining and transforming the values of the bytes within the table. Because the tables are blocks of information, AES encryption is known as a block cipher. It has a fixed block size of 128 bits. After the bits have been scrambled, they are exported as encrypted data, which can only be unscrambled by the same encryption key that was used to create the code.

Common Sense Guidelines for Pass Codes

Even the strongest encryption method can be bypassed if your pass code is vulnerable. Follow a few basic rules when selecting a pass code and make sure you protect your pass code so it does not fall into the hands of unauthorized persons.

Selecting a Strong Pass Code

The strongest pass code consists of a random series of characters, mixing uppercase and lowercase letters, numbers, and other keyboard symbols. The longer the password, the better protection is provided. In fact, taking full advantage of AES encryption requires a 32-character pass code for 128-bit encryption and a 64-character pass code for 256-bit encryption. It might not be possible to use the full 32 characters, because many applications limit the number of characters a user can enter for a pass code. Still, the basic concept still applies. Longer pass codes provide greater protection.

From a practical standpoint, a 64-character pass code of random symbols is difficult to remember—and you can't use a pass code if you can't remember it. A simple solution is to pick a pass code that has personal significance for you, which makes it easy to remember, but is highly unlikely to ever become public knowledge. For example, select your favorite line from a movie or book, and then add the price you paid for your car. The pass code will be easy to remember, but it is highly unlikely that anyone would discover or guess the pass code.

When creating a pass code, consider the sensitivity of the information you are protecting. A financial institution protecting customer accounts and sensitive personal information might want to use pass codes with the highest level of protection. If your company is backing up weekly sales and inventory figures that are not of a confidential nature, your employees are probably safe using shorter pass codes that are easier to remember.

Avoiding Weak Pass Codes

When selecting a pass code, a common mistake is to choose a weak pass code that can be easily broken. A single-word pass code provides weak protection, because code breakers often use existing lists of words, for example an online dictionary, to launch attacks on password-protected material. A short pass code can be easily broken by decoding programs that compile all possible combinations of short pass codes. Another common mistake is to continue using a temporary default pass code that was intended to be quickly

replaced by a permanent password. Many default passwords are public knowledge or can be easily guessed.

Weak pass codes can also be based on personal information that can be discovered by someone who knows you or who gains access to your personal information. For example, do not use your name, the name of a relative, birthdates, telephone numbers, addresses, a driver's license number, social security number, or similar information that could be guessed by someone who stumbles across your personal information.

Guarding Your Pass Code

Even the strongest pass code is useless if you treat it carelessly. A few simple precautions can prevent others from gaining access to your pass code.

- Do not divulge your pass code to anyone, even someone who appears to be trustworthy. Hackers have been known to call random telephone extensions within a company, pretending to be IT personnel. If someone claims to be calling from IT and requests your pass code, do not give them your information.
- Memorize your pass code. Make a record of the pass code only if you can store it in an absolutely secure location that can be accessed only by authorized persons.
- Make sure no one can see your hands when you type your pass code on your computer keyboard. If someone is standing behind you, they might be able to see the pass code being entered.

When you encrypt information, it is important to consider what might happen if you forget or lose your pass code. If you rarely use a pass code or you suspect you will forget it, make a copy and place it in a protected location where no one else can access it. Although pass codes need to be secure, in some cases they might need to be accessible to someone else who might need access to the encrypted information. For example, if the individual who performs daily backups at a company is the only person who has the encryption key for that data, how will the company access their backups if the individual unexpectedly dies or becomes incapacitated? With important corporate information, a number of trusted individuals should know the pass code or should have access to a locked office, safe, or safety deposit box, where the pass code can be stored.

About EMC

EMC Corporation (NYSE: EMC) is the world leader in products, services and solutions for information management and storage that help organizations extract the maximum value from their information, at the lowest total cost, across every point in the information lifecycle. Information about EMC's products and services can be found at www.EMC.com.

About EMC Retrospect

EMC Retrospect is part of the EMC Insignia line of software and hardware products, which enables small and medium businesses (SMBs) to store, protect, manage, and share vital business information. To learn more about EMC Insignia, contact your authorized EMC Velocity SMB channel partner or visit www.emcinsignia.com.