

December 2006
Volume 4, Issue 4



December Social

Thursday

December 14, 2006

1:30 p.m.

Archibald's Restaurant

1100 West 7800 South, West Jordan

Inside this Issue

President's Message	2
DocNet Ad	2
2006-2007 Board of Directors	3
2006 Arma Conference	3
Iron Mountain Ad	4
Best Practices for Protecting Private Information on Back-up Tapes	5
Best Practices for Protecting Private Information on Back-up Tapes... Continues	6-8
File Center Ad	9

PLEASE CHOOSE ONE MEAL CHOICE:

▪ **Chicken Florentine:** A fresh, boneless chicken breast broiled and smothered in a rich mushroom and spinach cheese sauce and served with rice pilaf and chef's vegetables

or

▪ **Baron of Beef:** Tender and moist Baron of Beef with a fresh mushroom bordelaise sauce, mashed potatoes and chef's vegetables

All meals include fresh-baked sourdough bread and butter, tossed green salad with house ranch dressing, dessert and beverage.

PLEASE RSVP WITH MEAL CHOICE BY

WEDNESDAY, DECEMBER 6, 2006

To Rori Clark, Midvale City Recorder at

rclark@midvale.com



"To Advance the Professional Practice of Records and Information Management"

President's Message

By Daryl R. Downs
Chapter President

In August 2006, we established a goal to "More Efficiently Share Chapter Information" as part of our strategic plan. That goal included the integration of our chapter newsletter and other appropriate content into our chapter website. The date for that integration has arrived. The December 2006 issue of the ARManagement Newsletter will be the final edition.

As we end the publication of our newsletter, I extend my sincere thanks to Michelle Marsh who has contributed both her time and her professional design and editorial skills to make our newsletter a success. I am certain that very few of us appreciate the effort required to produce our monthly news-

letter. Michelle has fulfilled her assignment admirably. Thank you, again.

I also extend my thanks to each chapter member who has ever worked on the newsletter or contributed content for the benefit of others.

As we integrate all our chapter content into our www.armautah.org website, it will become more important for each chapter member to use the website often. When you would like to know what programs or events are coming, check the Calendar.

The best way to learn how to navigate the website is to use it. We have tried to keep it simple, and we are always open to suggestions that will improve your experience when you use the website. If you have suggestions, tell

use about them at About Us / Leadership/Contact Us.

We have also tried to select useful Internet links that may relate to your records management assignments, employment, and current RIM issues.

As your Utah-Salt Lake Chapter President, I recognize a real need to provide you with useful information. The move to a web-based information repository is part of our larger strategy to improve both the quantity and the quality of the information available to you through our chapter. We look forward to our members being both beneficiaries and providers of that improved content.

Take the Pain Out of Document Management

Managing information is time consuming and costly. Filing and retrieving paper, searching for and reproducing missing documents, and keeping private information secure diverts employees away from revenue producing activities.



DocuNet's unique information management solutions will minimize inefficient practices and will enhance productivity.

- ◆ Reduce Operations Costs
- ◆ Increase Data Accuracy and Accessibility
- ◆ Increase Information Security
- ◆ Decrease Document Storage Costs

(801) 977-8400

www.docunetusa.com

Document Scanning

Custom PDF Formatting

Records Management

Records Storage



San Antonio Conference One of the Best Ever

More than 4,500 people were in San Antonio, Texas, for ARMA International's 51st Annual Conference and Expo Oct. 22-25, where they had access to more than 90 educational sessions featuring trends such as compliance, e-mail management, and electronic (digital) archiving. Attendees also had the opportunity to visit more than 200 vendors on the nearly 200,000 square foot show floor. A number of new products were unveiled to attendees, including the world's first-ever mobile scanning facility.

ARMA also added a technology sponsor - Microsoft - to this year's show.

Another first was the offering of post-show podcasts of technology sessions, interviews with industry experts and leaders, and conference reaction from attendees. If you missed the 2006 Conference and Expo or you just want to re-live Judge Shira Scheindlin's keynote Q & A session, get up-to-date by listening to the podcasts at www.arma.org/podcast. You'll find interviews presented in .mp3 format. Use your browser's audio plug-in for .mp3 files, or download them to your desktop and use your favorite .mp3 player application.

ARMA International's 2006 Podcast is brought to you by NextPage, providing desktop document retention, and ARMA International, the authority on managing records and information.

Mark your calendars for ARMA 2007 in Baltimore, Maryland, on Oct. 7-10.

Courtesy of www.arma.org/news

Happy Holidays



Utah Salt Lake Chapter Board of Directors 2006- 2007

Immediate Past President – Sonya Kintaro
801.535.6225 / Sonya.kintaro@slcgov.co

President –Daryl Downs
801.240.6773 / downsdr@ldschurch.org

President Elect – Rori Clark
801.567.7207 / rclark@midvale.com

Secretary – Pat McFerson
801.825-8976 / pmcferson@weber.edu

Treasurer – Daye Abbott
801.535.6343 / daye.abbott@slcgov.com

Historian – Tom Benson
801.323.3470 / tbenson@rqn.com

Editorial Committee – Michelle Marsh
801.774.8676 / michellek68@yahoo.com

Hospitality Com,itte – Daryle Bartholomew
801.851.8215 / daryleb@utah.gov

Corporate Liaison – Tom Benson
801.323.3470 / tbenson@rqn.com

Membership Director – Craig Young
435.864.6444 / craig-y@ipsc.com

Publicity Committee – Paulette Thurber
435.654.0757 x13 / pthurber@ciherber.ut.us

**Education Committee/CRM Director–
Bruce Bailey, CRM**
801.545.5700 / bbailey@utah.gov

Webmaster – Chris Calton
801.226.7146 / chris@cuwcd.com

Governement Liaison - Brent Egbert
801.365.4639 / begbert@extrspace.com

“To Advance the Professional Practice of Records and Information Management”



Meet your new best friend.

As the world's trusted leader in protecting, storing and managing business records, Iron Mountain offers an unrivaled choice of solutions that let you instantly access and retrieve records right from your desktop. Iron Mountain Connect™ is an innovative web-based tool that can reduce costs, increase control, and ensure ongoing compliance of your records management program. To learn more about our wide range of products and services, call us at (800) 800-IRON or contact your Iron Mountain representative.



www.ironmountain.com

RECORDS MANAGEMENT / SECURE SHREDDING / DIGITAL SERVICES / COMMITMENT

©2015 Iron Mountain Incorporated. All rights reserved. Iron Mountain and the design of the mountain are registered trademarks of Iron Mountain. Connect is a trademark of Iron Mountain Incorporated.

IRON MOUNTAIN - WHITE PAPER

Best Practices for Protecting Private Information on Back-up Tapes

INTRODUCTION

Data protection is critical insurance against loss of data that could cripple a business. It is estimated that three out of five businesses that experience downtime of 48 hours or more will be out of business within 3 years. Creating a successful disaster recovery and data protection plan requires people, process and technology in the right recipe to be successful. It is not easy work, but it is essential work.

Protecting private information is becoming increasingly important and is being mandated by state and federal legislation. Private information can be defined as non-public personal information such as name, address, credit card number, Social Security Number; and company-sensitive information including nonpublic financial data, customer lists, intellectual property and trade secrets.

In recent months, the two worlds of privacy protection and disaster recovery via tape backup have intersected, providing key indicators that businesses need to redefine their approach to backup to address these new concerns. Enterprise Strategy Group summarizes this best in a recent research report. These regulations mean that data security decisions must be made in the context of corporate governance, not simply technology operations (ESG Research, The State of Backup Encryption, March 2005).

REDEFINING BACKUP

Historically, backup success has been measured by meeting the goals of information recovery. Typical concepts include recovery time objective, recov-

ery point objective and off-site storage of tapes to ensure the data is available in a backup location in the event of a disaster. These items, and the need to complete backups within a certain timeframe ("backup window"), have historically driven IT spending as it pertains to data backup and recovery. In addition, they are the primary metrics by which an IT organization is measured in terms of meeting their backup objectives.

In today's world of heightened awareness and increasing regulations regarding the protection of private information, backup practices need to be modified in consideration of these new requirements. The traditional definition of success needs to be expanded to ensure that critical information cannot be accessed by unauthorized parties. This means thinking about data protection in different ways, including making the data storage security of backup tapes, regardless of location or type of storage device, an integral part of the company's overall security policies and procedures.

ENCRYPTION

One of the best practices to prevent the unauthorized access of information is to use encryption technology. Encryption is well-known for the protection it provides in the transmission of data across public networks (SSL, tunneling or secure web pages, for example). Encryption scrambles information so that unless you have the key, you will not be able to decipher and unlock it to be read. When information on a tape is encrypted, it is essentially unreadable without the key. Encryption has typically not been applied to backup data because they are usually

transported via a secure physical chain of custody. While Iron Mountain has a 99.999% reliability rate in transporting backup media, and extensively uses training, technology and process to ensure security of the end-to-end transportation process of backup tapes, human error can occur and tapes can get lost. Though it is difficult to reconstitute the information on an unencrypted backup tape without the precise hardware, software and system components, it can occur. Encryption of the data on backup tapes is the only effective means of making certain that others cannot read the information on the tapes in the event they are lost.

According to a 2004 survey by Enterprise Strategy Group, over half the respondents in all categories (large and small business, financial services, government, healthcare and manufacturing) do not use encryption technology to protect their backup information in this manner.

Adding encryption to your backup environment isn't an easy task, but it is vi-



able. It adds several layers of complexity to an already difficult backup and recovery process. It requires specialized hardware and/or software to accomplish the encoding, plus keys to unlock the encoded data when it's needed for disaster recovery. Issues of protecting keys, ensuring key availability during disaster recovery, and ensur-

“To Advance the Professional Practice of Records and Information Management”

Best Practices for Protecting Private Information on Back-up Tapes

ing encryption hardware and software is available at the disaster recovery site significantly increases complexity. Encryption capability has been available within enterprise-class backup solutions for some period of time. Organizations have rarely taken advantage of this capability because it has been difficult to integrate into the backup and disaster recovery process and still achieve the backup window and recovery time objectives.

There are several options for implementing encryption that can balance backup objectives with the emerging need to ensure the protection of private information.

These include:

- **Application Data Encryption:** Under this solution, the business application writes the data to the hard drive in an encrypted format; therefore the backup software copies encrypted data. In this approach, data compression techniques cannot be used once the data has been encrypted. With the lack of compression, more media and a longer backup window are required.
- **Storage Software/Backup Software Encryption:** Most enterprise-class backup software includes an option (some at a fee) for encryption. This has the benefit of low impact on infrastructure changes, but may not be the right choice for high-volume data encryption. Adding a step to the backup process may increase the time needed to successfully complete the backup (“backup window”), as well as prohibiting the use of



compression and potentially increase the media required to complete the backup. Increasing amounts of data and increasing backup windows can impact the success of the backup process.

- **Appliance Model:** Appliances promise a high throughput, low impact configuration, allow use of compression and require lower management overhead. These devices typically sit “in line” with your backup process—either as a physically attached device or a combination of a device and “agent” software.
- **Combination Approach:** Send backup data in an encrypted form over the network to a secure “disk” vault—then this information, which is encrypted, is moved to a backup tape for off-line secure storage.

In addition to encrypting your information, there are best practices surrounding encryption key management. Putting your keys on a tape and placing them in the same control environment is not a good practice. Keeping them separate and properly archived is a best practice.

CONTINUED ASSESSMENT

At a high level, the main topic presented here is that company practices around backup and information protection need to evolve to meet the new requirements for protection of private information. Technology alternatives exist. Companies need to start the process of re-thinking their backup practices. Backup needs to become part of an overall security process that reviews access to cus-

tomers and employee information and any other company-sensitive data. The key point is this requires the adoption of a sustained process, not sponsorship of a special event. Each organization may have its own approach, but as with Sarbanes-Oxley compliance, what started in many companies as a project to “pass the test” in the first year is now being institutionalized as part of normal business processes.

Additionally, performance of a risk assessment requires that the individual responsible for information security at the company take into consideration all portable media devices, including backup tapes, laptops, USB drives, etc. Understanding the value of the information inside your company and how it is—and should be—protected will most likely substantiate such a change in approach to managing and protecting it. What’s most important is to start the process.

FREQUENTLY ASKED QUESTIONS ON TAPE SECURITY AND ENCRYPTION

How difficult is it to get data off an unencrypted tape?

Even if your tapes have been “stolen”, getting data off of these tapes is not easy. One would need to have:

- The right make and model of the tape device in which to put the tapes
- The right version of the backup software
- The right operating system to recover the information
- The precise configuration of the system including server names

If you think about how difficult it is just to recover data when it is your own, the above process can be a very large

Best Practices for Protecting Private Information on Back-up Tapes

science project for a person without the right recipe and ingredients. This is not to say that encryption is not necessary; however, when segmenting your data, and having to make choices, these things are important to remember.

Why is this important to me?

Based on recently passed legislation, and legislation pending in Congress, all personal information needs to be safeguarded because in the event of a loss, the individuals whose information was on the tape must be notified. Companies that have specific customer information such as credit card information, names, addresses or Social Security data of consumers are obligated, by law, to protect that data from inappropriate access or deletion, and in many cases disclose any potential inappropriate use or access.

What are the risks and consequences of not encrypting my data?

There is a significant business risk to allowing personal information to fall into the hands of a competitor or unscrupulous individuals who may use that data in a criminal fashion. In the current era of identity theft this is a significant risk. Irreparable damage may be done to your company or your customers by not appropriately protecting your data.

Is data encryption appropriate for all of my data?

Usually it is not appropriate for all data. There are many different kinds of business data that require different levels of classification and, therefore, protection. The important thing is to perform a security assessment to identify the

data with the highest exposure risk and develop a plan for encrypting this information.

What are the costs?

Generally the costs are not prohibitive. There may be server overhead as well as staffing required to support key management and protection. Generally, the cost will be small in comparison to the business risk of having personally identifiable information fall into the wrong hands.

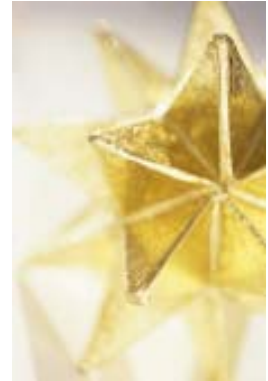
What are some of the options?

There are several options available in the marketplace. Generally the options will fall into a few categories: one will be appliance based, the other software based. Some options can insert the encryption process between the computer host and the disk; other processes insert the encryption process between the disk and tape drive, usually using the backup server to implement this process.

IRON MOUNTAIN WHITE PAPER
If encryption is an option in most backup packages, why don't people use it?

Generally, once a backup process is established and working, a backup administrator is not going to add a layer of complexity simply to enable an additional option without a sound business reason. Most companies have judged the success of the data protection process on how quickly and confidently they can recover their data for business purposes, they have not considered the security and/or privacy implications of making a copy of the data. In addition, in most cases it doesn't make sense to turn the encryp-

tion option on globally. Not all data contains private information and this would result in a large increase in computing needs and time to complete backups. It also would create larger backups and increased tape usage as encrypted information cannot be compressed by tape drives.



Does it work for SAN, NAS, DAS, Tape?

Most software and appliance solutions can be implemented in all storage infrastructure configurations. Implementation options need to be considered based on the sensitivity of the data, whether or not removable media is used, and the risk tolerance of the business. In general terms most companies considering encryption today are focused on removable media.

Does it impact my backup processes?

There could be a measurable impact on the backup process if encryption is implemented with a high level of granularity and not well thought out. There is a potential impact on the computing resources consumed by the backup server, the length of time the backup processes run, and the complexity of ensuring the keys and encryption hardware and software are available for disaster recovery needs. In general terms, there should be minimal changes required to the backup environment to support encryption provided that the process is well thought

“To Advance the Professional Practice of Records and Information Management”

Best Practices for Protecting Private Information on Back-up Tapes

through and performance considerations are understood and managed.

Is key management an issue?

Managing encryption keys is a process that needs to be understood prior to implementing encryption. Generally this is not a significant issue when implementing an appliance solution. One of the features of the appliance model is generic key management in a "black box" manner. The appliance will manage all of the key components based on defined policies. In a software implementation, processes need to be developed and managed to ensure that the encrypted data and required keys are sent offsite, separately, to protect the data but are available together in the event of a required restore process.

Who is responsible for encryption?

Typically, it is the Chief Security Offer or the individual who is responsible for information security at a company. These people should be identifying what data is considered private information and defining the security process. The next person in the process is the backup administrator.

© 2005 Iron Mountain Incorporated. All rights reserved. Iron Mountain and the design of the mountain are registered trademarks of Iron Mountain Incorporated. All other trademarks are the property of their respective owners.



New Year's Recipe

Shrimp Scampi Cheesecake Appetizer

"Rich cheesecake with a seafood surprise. Decadent and smooth for adult tastes."

Original recipe yields: 12 servings

Prep Time: 45 Minutes

Cook Time: 25 Minutes

Ready In: 1 hour 10 minutes

INGREDIENTS

- 1 tablespoon olive oil
- 1 onion
- 6 teaspoons mince garlic
- 1 pound fresh shrimp peeled and deveined
- 12 shells puff pastry, baked
- 4 tablespoons butter or margarine
- 3 (8 ounce) packages cream cheese, softened
- 4 eggs
- $\frac{1}{2}$ cup heavy cream
- 16 ounces smoked Gouda, grated
- 2 teaspoons salt

DIRECTIONS

1. Preheat oven to 350 ° F (175° C).
2. In a large skillet over medium-low heat, warm oil and sauté onions and garlic until onions are translucent; set aside to cool. When cool, pour off liquid reserving garlic.
3. Cut shrimp into $\frac{1}{2}$ -inch pieces, reserving 12 uncut for garnish. In a large skillet over medium-low heat, melt butter and add reserved garlic and all shrimp; cook shrimp for 2 to 4 minutes or until done.
4. Remove center circle and a small portion of inside of cooled puff pastry shells.
5. In a medium bowl, beat cream cheese until creamy; add one egg at a time and beat until well mixed. Add cream, Gouda, onions, shrimp and salt.
6. Spoon filling into puff pastry shells.
7. Bake in preheated oven for 20 to 25 minutes or until filling is browned on top. Garnish with whole shrimp and chopped chives; serve.

**"To advance the professional practice of
Records and Information Management**

*ARMA
P.O. BOX 2160
Salt Lake City, UT 84111-2160
Address Correction Requested*

We're on the Web!
www.ARMAUTAH.ORG

FILE CENTER, INC
RECORDS STORAGE & MANAGEMENT

Introducing "Web Based" records management.
File Center, Inc. now offers a direct link with your off-site records via the RSWeb Internet enabled interface. The index of your stored records is only a password away.

Call File Center or visit our website today
801-979-1233
www.filecenterinc.com

"We'll barcode anything"

NEWSLETTER INFORMATION

Comments, submissions and advertisements are welcome. For more information, please contact the Newsletter Editor/Publisher Michelle Douglas 801.774.8676 or MichelleK68@yahoo.com

This Newsletter is mailed monthly to over 60 records and information management professionals in the Utah-Salt Lake Chapter area, as well as professionals in other ARMA Chapter areas. Opinions are those of their authors and do not necessarily reflect the official policy or opinions of ARMA International or the local chapter.

Contributions or gifts to ARMA International are not deductible as charitable contributions for State or Federal income tax purposes.