

RIM VIEW



ARMA International
Southern California Inland Empire Chapter

Vol. 8, Issue No. 4, Spring 2011



Silver Lining 25 years of RIM Education

In This Issue

President's Address	1-2
Ron Harrington first Inductee into SCIE ARMA Chapter Hall of Fame	3
A Quick Guide to Records Retention.....	4-5
Chapter Announcements/Calendar of Events.....	6
Ask the RIM Lawyer	7-8
CRM Study Questions.....	9
Is Your Resume' Hurting or Helping You Get that Interview?	10-11
Archives & Record Management Graduate Degree offered at San Jose State.....	11
Carmel Valley eDiscovery Retreat.....	12
AIEF Foundation Highlights.....	13
The Evolution of E-Discovery Sanctions.....	14-17
Removable Media Best Practices.....	18-21
2011 Annual RIM Seminar.....	22
ICRM News	23
Ex-Employee, Social Media and a Security Breach: Oh My!	24-25
2010-2011 Chapter Year in Pictures.....	25
25 th Anniversary Celebration at Mission Inn Riverside on May 12, 2011.....	26
2010-2011 Sponsors	27



Chapter President's Farewell Address

It has been a pleasure and honor serving as your Chapter President from (2008 – 2011). This has been an extraordinary year for the Southern California Inland Empire ARMA Chapter. We reached all chapter goals this year --- Launched New Chapter Website, New Chapter By-laws, Quarterly Newsletter Publication, Chapter Outreach and Increased Membership.

The chapter was well overdue for a newly refreshed and updated website. We were very fortunate to have Kylene Sotelo - City of Chino Hills strong interest at assuming the role as our new Webmaster. The board decided our current host was not capable of doing what the membership wanted from the website and changed host. The website was officially launched on September 24, 2010 and ironically the same day as our official Chapter's 25th Anniversary. All viewers are now able to see the history of the chapter, pictures, Chapter Announcements (ARMA, AEIF, ICRM and other Chapters), power point presentations and ability to pay by credit card with PayPal.

One of our greatest achievements as your Chapter Board was reviewing, rewriting and approving the Chapter By-laws. The chapter by-laws had not been reviewed in a few years. The Chapter President submitted [DRAFT] Chapter By-laws to the Chapter Board for review on Thursday, August 12, 2010. The board reviewed the Chapter By-laws and after 8 versions approved the new Chapter By-laws in record time on Thursday, September 16, 2010. The By-laws were submitted and approved on the same day by ARMA International. This was a clear sign that we had a great collaborative working board and it was going to be a wonderful year.

Our Chapter had two community outreach projects this year to educate others' about Records and Information Management and ARMA International. The first one Debora Thomsen, Secretary/Past-President, Traci McGinley, Treasure and Brandon Reeder, President coordinated and staffed the booth at LegalTech 2010 – Los Angeles Convention Center on behalf of ARMA International. There was an extremely high interest of those whom attended in becoming ARMA members.

The second community outreach was a One Day Event with Project Management Institute (PMI) California Inland Empire Chapter. The event was called "Project Management & Organizational Transformation – What you need to know for the next ten years". Debora Thomsen and Brandon Reeder managed a booth answering questions about ARMA and distributing ARMA International and Chapter literature. The Chapter supplied a raffle prize of an iPod shuffle for the event.

In the earlier part of 2010, I was attending an AHIMA (American Health Information Management Association) meeting at Loma Linda University. The presentation was given by Monica Ellis, Vice-President of the Orange County Chapter and formerly of Munters Corporation on recovering damaged documents. I met Charmaine Davis from Kaplan College at this meeting. She extended an invitation for me to be part of the Health and Information Technology (HIT) Advisory Board. This was a great opportunity for our Chapter to reach directly out to a new area and share the knowledge or RIM within our local Health and Information Management community. In turn, Kaplan has provided us a wonderful facility for us to meet for our CRM study group. Thus, the official SCIE ARMA CRM Study group was officially born in 2010. We hope that our first group of CRM Candidates will receive their CRM in the next year or two.

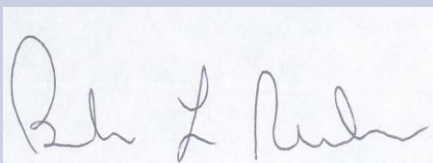
Our chapter began the year with 46 Chapter members in August 2010 and ended with 51 Chapter members in May 2011. There were two members that left the RIM profession and two others whom retired and decided not to retain their ARMA Membership. We were able to increase our Chapter membership by our community outreach and active recruitment by our Membership Director, Brenda Hutchinson to 9 new members. There has been a dramatic shift in years of active ARMA Membership with 49 percent of the membership with less than 5 years and 76 percent with less than 10 years. Our most senior Chapter Members are Hall of Fame Inductee No. 1 - Ronald Harrington, Mary Cox, Steve Gray and Brenda Hutchinson. These long-term members have truly been an instrumental part in success this year and in the past 25 years.

We concluded our year with our 25th Anniversary Celebration at the Mission Inn on May 12, 2011. You can find more information about this event on page 25 of this newsletter.

I want to personally thank the “2010 – 2011” Chapter Board for all their contributions and dedication to the chapter and making it a very successful year.

- Debora K. Thomsen, Past-President, Chapter Secretary
- Rhonda Basore, Vice-President
- Traci McGinley, Treasurer
- Brenda Hutchinson, Membership Director
- Justin Lee, Hospitality Director
- Kylene Sotelo, Webmaster

I've decided to continue my leadership path and represent our great chapter at the ARMA Pacific Region level. My new role is ARMA Pacific Region Sponsor Coordinator and any other duties asked by the ARMA Pacific Region board. I will remain in that role until a Region Coordinator position opens. However, I will continue to remain on the Chapter board as your Membership Director, Newsletter Editor and Past-President. I wish the future president and incoming board another successful year in 2011 – 2012.



Brandon L. Reeder
SCIE ARMA, Chapter President

***RON HARRINGTON, CRM – CHAPTER CHARTER MEMBER
& CHAPTER PAST-PRESIDENT INDUCTED AS
SCIE HALL OF FAME INDUCTEE NO. 1***

By Mary Cox, CRM

As one of the founding Charter members of the UIEC chapter Ron was instrumental in keeping the chapter going during those first years. I remember when I joined the chapter in 1988; Ron was my first contact and was always encouraging me to be active in the chapter. Ron was also responsible for much of my early education in Records Management due to the great speakers and topics he arranged for the chapter meetings. Ron was also willing to spend time sharing his records management experiences.

Of course Ron really got me involved in the chapter when he persuaded me to be chapter president. I remember that telephone call as if it were yesterday. By this time Ron had been single handedly keeping the chapter going and he told me that if he could not find someone to be president the chapter may have to fold.

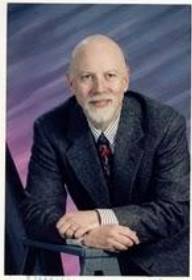
In the mid 1990's Ron started working at the County of Riverside. He first worked for the Clerk of the Board and then RMAP. Ron worked for the County for 10 years before going to the City of Ontario and then the National Archives.

While at the County Ron was primarily involved with establishing standards in the newly formed Records Center, creating retention schedules for the County Departments and providing education to the County Departments. Many of the procedures are still being used in the County's Records Center. Whether it is how to take a records inventory or how to properly stack boxes on a pallet were the result of Ron's expertise and experience. Prior to the County, Ron worked at the Sunkist Records Center so he had a lot of knowledge in that area.

One of the most successful avenues for educating not only the County but many in the local government agencies was the annual expo that was put on in Riverside co-sponsored by UIEC, County of Riverside RMAP and the Southern California City Clerks Association. Ron always did an excellent job working to get quality speakers at this event and being a vital member of the expo committee.

At that time back in the early 90's ARMA was relatively small – everyone knew everyone. But Ron knew EVERYONE and persuaded them to come out to the Inland Empire either as a chapter speaker, an Expo speaker or at the County for one of the Records Management Group Meetings. Ron not only attended the UIEC meetings but often attended the Orange County and Los Angeles Chapter meetings.

Suffice it to say that without Ron there would not be a Southern California Inland Empire ARMA Chapter and that Ron deserves to be the first one inducted into for the SCIE ARMA Hall of Fame.



A QUICK GUIDE TO RECORDS RETENTION

By Gordon E.J. Hooke, CRM

Gordon is a Senior Records Management Analyst/Consultant and a member of Twin Cities Chapter of ARMA. He won the *AIIM International* Distinguished Service Award in 2009.

Traditionally, records retention was an exciting as a bowl of thin gruel. In the 2011 evolution of records and information management, retention is the main course, the meat and potatoes. Organizations find great satisfaction and sustenance in retention: identifying and organizing information as it enters their reach and maintaining its availability as long as it has use.

Surely there are other leaders in ARMA International's Generally Accepted Recordkeeping Principles, including protection, accessibility and disposal. Retention, however, is the heart and soul of records management. Retention instructs an organization what to keep and how long to keep it. Retention tells where a record is stored and who the record's serial custodians are as it progresses through workflows. A retention devotee might say that all the other principles are peripheral.

The Retention principle's key commandment, "Know what you have and where you have it," carries two implications. First, without following the dictum, the records saved are largely lost and useless. Partial knowledge of inventory and location is hardly better than any knowledge at all. Searching for known records amongst many unknowns is like searching for the proverbial needle in the haystack.

The second implication concerns the data map. Since rules and guidance regarding electronic records were added to the Federal Rules of Civil Procedure in 2006, opposing attorneys discuss the records at the beginning of civil litigation. They trade data maps, essentially inventories of records, along with information about the records' location and storage media. Data maps answer the question, "What do you have and where do you have it?" Without a data map, a party to a suit may be deemed "in bad faith," and the party's legal standing may be compromised.

Although the definition of a record—the smallest unit of recorded information that affects an organization's function—is widely circulated, relatively little attention is given to the torrents of recorded information that do not affect an organization's function. These include "convenience" copies beyond their time to pick up milk on the way home, junk mail and much more. Distinguishing records from non-records can be critical. Long after the retention period of the original, a non-record copy is still subject to subpoena, as are any other non-records, whether they exist on derelict collaboration sites, on the hard drives of office multifunction devices or on a retired salesman's laptop.

Declaring and retaining records is vital to an organization's survival, but recognizing that non-records also have legal standing can be invaluable. Retention rules must address non-records.

It may be inaccurate to say that most corporate counselors advise their firms to keep all records forever, although certainly many do. However, it *is* accurate to say that few corporate counselors have ever studied the age-old discipline of records management. If they did, they would see the folly of their over-retentive advice.

Over-retention is wrong for a raft of reasons, among them:

A Quick Guide to Records Retention (continued)

- Storage is costly, some forms more than others.
- Too many records slow searches and retrievals.
- Unneeded records are legally risky.

The rule of thumb is to dispose records as soon as they have met all legal, regulatory and operational needs. Records with historical significance trump the rule. All records disposed of according to a compliant, published retention schedule are exempt from subpoena, so they carry no risk. All extant records may be required in court, even if they could have been disposed of but weren't. Keeping fewer records equates to lowered risk.

Every record must have a *raison d'être*. A recording of information without a reason or justification is not a record. That reason may be to meet a legal requirement, to fulfill a regulation, to perform an operational function (including recovery from a disaster) or to provide a historical resource in the future. Especially in business, there is no justification for retaining a recording of information without a valid reason. This varies from the art world, where information may be retained for its beauty or esthetic value. There, the justification, "I like it", is reason enough. Not so in business.

"How long should I keep records?" is the most frequent question records managers hear. And after the "forever" nostrum addressed above, we often hear the figure "seven years." This is generally unsubstantiated. It may be seven years, but it may just as likely be three years, six months, 12 years or some other period. The real answer to the question is, "Keep records as long as the retention schedule says to keep them."

Here's the shorthand: Create a data map and organize like records into appropriate record series. Then assemble all the people who have a stake in records retention and see how long they will need each series so they can do their work. (Include those responsible for legal and regulatory compliance.) In the retention schedule for each series, enter the longest period reported to be needed. When the period expires, there is no justification to retain the records in the series, unless a legal hold suspends the retention schedule.

For simplicity's sake, a records program may lump together records that need to be retained over a range of times. Simplicity is generally good, but there is a trade-off. If records that need to be retained for six months are lumped together with records that need to be kept for nine-month interval has passed. The records that could be disposed of legally after six months remain for an extra three months. Keeping records beyond their required period can create risks, as discussed above.

Implicit in the Retention Principle is its counterpart, disposition. To reiterate, disposing of unneeded records can be as important as keeping needed ones. Disposing of records always creates a declaration/certificate of destruction. The certificate is, essentially, metadata about the destroyed records; these certificates create their own records, with record series and retention periods. As Kurt Vonnegut said, "And so it goes ... There is no end in sight".

Although there is no end to the need for retention, neither is there an end to its benefits. No matter how satisfying the dinner, the diner needs more the next day. No matter how superb the retention practices, the need will reappear—somewhat evolved—the next day. Fortunately, practicing retention well brings great satisfaction, peace of mind and profit. Retention, indeed, is the meat and potatoes of records management. Like a hearty meal, good records retention brings great rewards.

Article originally published at <http://www.informationmanagementcompare.com/> on 1/10/11

CHAPTER ANNOUNCEMENTS/CALENDAR OF EVENTS

2010/2011 Chapter Calendar

July 14 (evening) – July 16, 2011

ARMA PACIFIC REGION LEADERSHIP CONFERENCE

Sainte Claire Hotel – San Jose (\$116/night)
302 South Market St.
San Jose, CA. 95113

<http://www.larkspurhotels.com/collection/sainte-claire>

For a relatively small chapter investment, you can immerse your leadership and communal educational environment that strives to build and maintain your chapter attitude, momentum, and membership. Think about sending as many board members as possible. Sending and sponsoring Chapter leaders to the Leadership Conference serves as incentive to become more involved in chapter activities.

Featured Speakers



Dale Mask, founder of Alliance Training and Consulting, Inc. an international company providing corporate training services. Using instructor-led, e-learning, and blended learning options, Alliance develops programs helping organizations meet specific training objectives. He has facilitated over 2,500 Leadership and management training sessions, including prior Pacific Region Leadership Conferences.



Trevor Mitchell, Director of ARMA International Member Services



Sean Tanner, PMP, ARMA International Outside Director & ARMA International Board Member

SCIE/ARMA Membership July – Sept 2011 Anniversaries

Diane R. Gladwell	14 years
Cynthia A. Simmons	13 years
Debora K. Thomsen	13 years
Olivia R. Flores	11 years
Christopher D. Ellis	10 years
Sadbi Espinoza	9 years
Anna Grandys	6 years
Cheryl Love	3 years
Alexandra Rackerby	2 years
Dale Jonasson	1 year
Rebekah Marshall	1 year
Regina Lynn Patterson	1 year
Eliseo Perez	1 year

WELCOME NEW SCIE ARMA CHAPTER MEMBERS

Twila Case – Catalyst Repository Systems

Lisa Williams – Merrill Legal Solutions

John Isaza, Esq. is a California-based attorney and partner of Howett Isaza Law Group, LLP



ASK THE RIM LAWYER

This is a continuation of the syndicated column I am doing for ARMA chapters, including your SCIE ARMA Newsletter. My column is devoted to answering information governance, records management and related legal questions from Chapter Members. As you read my responses, please note that although I am an attorney specializing in these areas of law, these are my opinions only based on very limited knowledge of the Member's particular circumstances. My opinions should not be construed as legal advice. Kindly consult with an attorney for more formal advice.

Now that we have all the legalese behind us, I must confess that I have not received any questions from any of you during the past two months. As the Great Justin Bieber says, "Is anyone out there?" (Ok, I think he says, "Is she out there," but I will duke this one out with my daughter later.) But I digress, since I have not heard from you, and I have publication deadlines, I am writing about one of my current favorite topics – Metadata as a Record. For the next installment, please send me questions regarding Cloud Computing, which is another one of my new favorite topics. Contact me at: Jisaza@HiLawGroup.com.

1. **Why should you care about Metadata?**

When it comes to declaring electronic records, information governance professionals have been struggling for some time with the issue of what metadata to preserve. Stated simply, metadata is data about data. ARMA International defines metadata as "[s]tructured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource." *ARMA Glossary of Records Management and Information Terms*, 3rd Edition (ARMA International 2007) In any event, when it comes to declaring records and their related metadata, it may not be as much of an issue with native files (documents living in their original format or application) so long as they are preserved intact upon creation. Also, when it comes to data stored in various and sometimes sophisticated platforms such as back-up or archival systems, as well as other enterprise systems that may automatically store all metadata in native format, the preservation of metadata may not be as challenging. Native format is, in fact, the preferred mode of production currently advocated by some counsel and courts. Unfortunately, when it comes to preservation of documents generated by common business applications (often unstructured data such as emails, WORD documents, Excel spreadsheets, Power Points and documents on shared drives found in both large and small organizations) for records management purposes, the question becomes more difficult. What metadata fields are considered usable or relevant in determining what to capture at the end of the day if a record is or has been migrated to another format?

(ASK THE RIM LAWYER CONTINUED)

Similarly, when it comes to discovery in litigation, organizations struggle with the scope of how much metadata to preserve for pending and anticipated litigation or agency investigations. Organizations now more than ever are being exposed to “spoliation” sanctions for the destruction of documents in litigation. Sanctions could range from financial penalties, to legal instructions that could affect a jury’s outcome, and even to jail. In 2004 and in 2007, the ARMA International Educational Foundation published two articles I wrote dealing with the thorny issue of spoliation. The 2007 article, in particular, addressed the issue of scope of production in the context of what information to put on hold when faced with pending or reasonably anticipated litigation. As of December 2006, the Federal Rules of Civil Procedure (the “FRCP”) had been amended to reflect growing technology and the need to address ESI. Although not specifically mentioned in the revised rules, when it comes to ESI a necessary question arises about how these rules should apply to metadata. How then does an organization avoid spoliation sanctions’, considering how relatively easy it is to alter metadata during the day to day operation of any business application, including any business conducted over the Internet?”

Since the page limitations of this column do not afford me the opportunity to address how these issues can be addressed, I urge you to download the recent paper I wrote entitled “Metadata in Court: What RIM, Legal and IT Need to Know.” The paper was released in November 2010, and you can download it for free (yes, I said F-R-E-E) at www.ARMAEdFoundation.org. If nothing else, I am hoping this brief column has raised your awareness about Metadata and why you should care about it. If I have not, try reading the Foundation paper.

Mr. Isaza is widely recognized as one of the country’s foremost experts on electronic information governance, records management, and e-discovery preparedness. Mr. Isaza chaired the Chicago Program Committee for ARMA’s 2005 international conference; he is a member of ARMA’s Electronic Discovery Advisory Group and the GARP® Metrics Task Force; he is past President of the Greater Los Angeles ARMA Chapter and he has served on the Board of Directors of ARMA International. Mr. Isaza co-authored a book entitled [7 Steps for Legal Holds of ESI & Other Documents](#) released in July 2009. He is the 2008 recipient of ARMA’s prestigious Britt Literary Award. John Isaza is a California-based attorney and founding partner of the Howett Isaza Law Group, a law firm that specializes in electronic information governance, records management and overall corporate compliance. He may be reached at Jisaza@HiLawGroup.com or follow him on Twitter and LinkedIn.

**CONGRATS TO 2011 SCIE ARMA
VENDOR OF THE YEAR**



CRM EXAM STUDY QUESTIONS

1. A(an) _____ chart describes related activities by showing work planned versus work completed in relation to time.
 - a. organization
 - b. Gantt
 - c. workflow
 - d. PERT
 - e. Production
2. A _____ - area network covers a limited geographic distance, such as an office, a building or groups of buildings within close proximity of each other.
 - a. wide
 - b. single
 - c. local
 - d. defined
 - e. digital
3. All of the following are contained on the facilitative area of a form, except:
 - a. Organization name
 - b. Form number
 - c. instructions
 - d. form title
 - e. signature line
4. A primary concern regarding the legal admissibility of electronic records is the inability to detect _____ of the information.
 - a. elements
 - b. value
 - c. location
 - d. cost
 - e. alteration
5. A permanent directive remains in effect until:
 - a. Cancelled or superseded
 - b. A new director is hired
 - c. A termination date is reached
 - d. A merger of companies takes place.
 - e. It causes problems.
6. A group of intangible rights that protect creative works, including _____ copyright, trademarks, and patents is _____ property.
 - a. Cultural
 - b. Mandated
 - c. International
 - d. Lucrative
 - e. Intellectual
7. All the following are contained on the facilitative area of a form, except:
 - a. Organization name
 - b. Form number
 - c. Instructions
 - d. Form Title
 - e. Signature line
8. In a records center operations, _____ special containers are usually necessary to store:
 - a. Correspondence
 - b. Case files
 - c. Bank checks
 - d. Legal-sized files
 - e. Calendars
9. In micrographics, _____ equates to _____ image sharpness.
 - a. Reduction
 - b. Density
 - c. Resolution
 - d. Enhancement
 - e. Duplication
10. In an electronic records management system, single users are allowed to delete a document or volume deletions can be initiated by a system:
 - a. code.
 - b. taxonomy.
 - c. flag.
 - d. administrator.
 - e. E-mail.



Answers
on
Page 17



Is Your Resume' Hurting or Helping You Get that Interview?

By Pamela deForce from Davidson Group

You spend hours finding just the right words for your resume. You struggle over which font to select and what "action" words work best. But, do you know the way you format your resume and the information you include can undo all your time and energy?

NEVER – I mean NEVER use columns or tables. Most companies and many recruiters use databases to keep track of applicants. When you apply online or via email to a potential employer, your resume gets "parsed" into a database. If you use table or columns in order to make things line up and to avoid a struggle with spaces and tabs, it will come out looking very strange on the screen. Borders are inserted – lines show up that won't go away – spacing can look weird. So while it might be quick – all of those easy-to-use resume templates in Microsoft Word decrease your chances of getting called for an interview because most of them use tables and columns.

Do not be a jack of all trades! Make it abundantly clear to anyone who reads your resume what you do and what type of job you want to find – **HAVE AN OBJECTIVE.** And I **DON'T** mean the very vague "I'd like to find a position where I can use my experience and education to help a company grow and prosper and to conquer war and make the world a better place to live for" This is **NOT** a workable objective. Say "I'm looking for Business Development role... OR I want a Senior Project Management position..."

It does not help your case if you have been in sales and marketing and project management and can do just about anything that an employer may ask of you. I've never seen a job description that says "we want to hire a person with all kinds of different experience who we may or may not need in the future..." **FOCUS** on what you want and state it clearly. If you do have difficult skill sets, then make several versions of your resume..."

Use bullet points. The person who screens your resume – on average – does so in 10-15 SECONDS. If you don't grab their attention in that time, they will not read further. Bullet point your:

- education
- relevant experience
- accomplishments
- skills

Bullets make it much easier to quickly review and find the pertinent information needed in order to move you to the next step.

Don't force all your information on one page. If you have been in the work place for more than 10 years, you may very well have a two page resume. That is fine. What is not OK is to decrease the font – increase the margins and force everything into a single page.

And speaking of fonts – DON'T mix them! It is very difficult on the eyes – and it is very distracting – to have your name in one font – the places work in another and the description of what you did in yet another. The same rule goes for bolding and italics. Use them sparsely and occasionally. Special effects are not special if used to frequently.

(Is Your Resume' Hurting or Helping You Get that Interview? continued)

Don't capitalize your name. Again when your resume gets parsed into a database, any correspondence from the recruiter/HR person will pull the information from your resume. So an email to you will say Dear JAMES, if you use caps as yelling.

Please don't name your resume – resume.doc. Everyone who receives your resume will have their own preferences, but remember back to the old days of file cabinets. Use your last name then first name and then any date or other identifying information you want. Example – Johnson, Sandy resume 01-2011.doc OR Johnson, Sandy cover letter 01-2011. You get the idea. Keep your recipient in mind and remember they receive a LOT of resumes and if we filed them by first name we would have to look through many John's to find you.

If you are sending your resume by email – put your BRIEF cover letter in the body of the email. If you can grab enough attention in your email to get the attachment opened, you want them to see your resume – not a cover. OR better yet, forget the traditional cover letter and just make your email short and compelling.

Over the years, our team members have noticed that these pointers work for impressive and winning resumes. If you have any questions about how to formulate a resume, please do not hesitate to contact us at the Davidson Group. We are interested in your success!

Pamela deForce is the Senior Director of Legal Services for the Davidson Group, executive recruiters specializing in the Legal Services Market. Because Pamela worked in the Litigation Support arena over 20 years, she brings an understanding of the positions, duties and requirements that is unmatched by the typical recruiter. Contact Pamela at pdeforce@davidsongroup.com or 415.893.1020 ext. 101.

San José State University

SCHOOL OF LIBRARY & INFORMATION SCIENCE

Graduate Education in Archives and Records Management

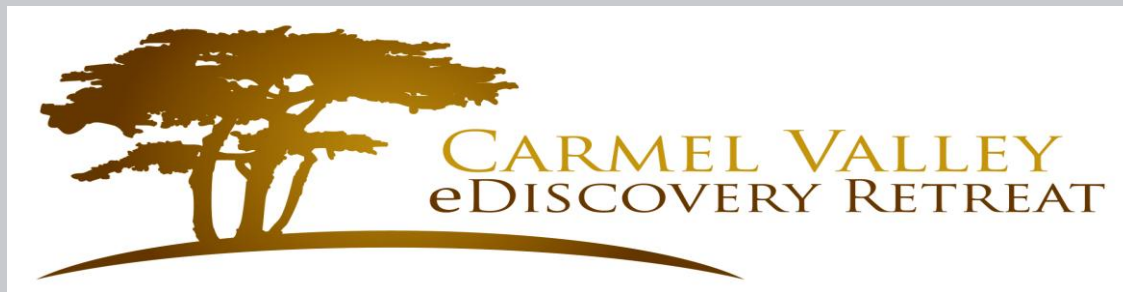
Today's archivists and records managers are faced with a variety of challenges, including managing records created using emerging technologies. While many archivists and records managers recognize the need for further education to prepare them to meet these challenges, busy work schedules and family commitments present barriers.

In response, the San Jose School of Library and Information Science launched a **fully online** Master of Archives and Records Administration (MARA) degree program three years ago. Students can live anywhere as they complete their degree using a variety of sophisticated distance learning tools.

MARA students participate in a cohort model, studying with a small group of peers who share the learning journey together. They receive instruction and mentoring from faculty and professionals who are award-winning scholars and leaders in their academic and professional communities – and who live around the globe, bringing an international perspective on emerging trends in the field.

To learn more about the MARA program or apply, visit <http://slisweb.sjsu.edu/mara/index.htm>

Online open house events are also an excellent way to find out more about the MARA program. To see the schedule for upcoming open house events, or to view a recorded open house, visit <http://slisweb.sjsu.edu/slis/openhouse/>



The Carmel Valley eDiscovery Retreat

The Carmel Valley eDiscovery Retreat will be a premier resource for industry practitioners who wish to focus on the complexities and practicalities of eDiscovery. Whether you're new to eDiscovery, or want to increase your existing expertise, the retreat will allow you to explore this critical topic with established industry leaders and your peers - all in one of the most stunningly beautiful areas of the United States, Carmel, California. Earn CLE credit hours while you get away from the hustle and bustle of the daily grind in one of California's most pristine destinations.

The Carmel Valley eDiscovery Retreat will offer participants opportunities to interact personally with industry experts in a collegial atmosphere. The retreat has been developed with an emphasis on breakout sessions and workshops, tailored to the needs of attendees. Your entire team can participate and explore the latest issues affecting the industry, and develop strategic directions.

To give you a taste of what's in store, here's a short list of confirmed speakers:

- **Laura Zubulake**, Consultant
- **Hon. James Smith** (Ret). - JAMS ADR
- **George Socha**, *Owner* - Socha Consulting LLC
- **Browning Marean**, *Senior Counsel* - DLA Piper
- **Diane Barry**, *Dir. of Discovery Strategy & Management* - ILS-IPP
- **Martha Dawson**, *Partner* - K&L Gates LLP
- **Jeffrey Ritter**, *Founder & CEO* - Waters Edge Consulting LLC
- **Bill Hamilton**, *Partner* - Quarles & Brady LLP
- **Robert Owen**, *Partner* - Fulbright & Jaworski
- **Gareth Evans**, *Partner* - Gibson, Dunn & Crutcher
- **Patrick Mullin**, *Partner* - Jackson Lewis
- **Eric Sinrod**, *Partner* - Duane Morris LLP
- **Greg Buckles**, *Consultant* - Reason-eD, LLC
- **Troy Dunham**, *Senior Electronic Discovery Manager* - Cooley LLP
- **Ruth Hauswirth**, *Dir of Litigation & eDiscovery Services* - Cooley LLP
- **Trent Livingston**, *Partner* - Geekly Group
- **John Isaza**, *Partner* - Howett Isaza Law Group

Please visit www.carmelvalleyediscoveryretreat.com for more information or contact Chris La Cour at: 949.887.3786 clacour@carmelvalleyediscoveryretreat.com

Your registration code is **SCIEARMA**

Retail registration is \$999 for a Full Retreat Pass (3 Days). Using the ARMA discount code above will take off \$500 and the total will come to \$499. Single Day Passes are available at \$499 for a choice of Day 1 or Day 2.



Scholarships Available

The ARMA International Educational Foundation has established a scholarship program to encourage development of the international records and information management community with an appropriately educated records and information management workforce. Eight scholarships are available. Applications must be submitted by **June 30, 2011**.

GRADUATE LEVEL SCHOLARSHIPS

ARMA INTERNATIONAL EDUCATIONAL FOUNDATION SCHOLARSHIPS

Six scholarships of \$3,000 are awarded annually, in the summer to a full-time student entering the second year of a graduate records and information management program or equivalent library science or archival studies program which contains a significant number of records management and information courses at a recognized university or college leading to a Master's or Doctorate degree or equivalent.

MAVIS EPPES, FAI, EXCELLENCE IN RECORDS MANAGEMENT SCHOLARSHIP

One Scholarship of \$3,000 is awarded annually, in the summer to a full-time student entering the second year of a graduate records and information management program or equivalent library science or archival studies program which contains a significant number of records management and information courses at a recognized university or college leading to a Master's or Doctorate degree or equivalent. Funding for this award is provided in recognition of Mavis Eppes, FAI, a distinguished legal records administrator and founding AIEF trustee. Preference is given to a candidate intending on a career in legal records management.

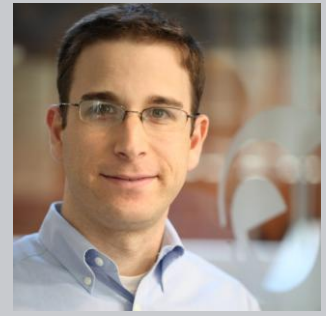
LEADERSHIP SCHOLARSHIP

One Scholarship of \$3,000 in the summer of 2011 to a full-time student entering the second year of a graduate records and information management program or equivalent library science or archival studies program which contains a significant number of records management and information courses at a recognized university or college leading to a Master's or Doctorate degree or equivalent. Funding for this award is provided by leaders of ARMA International

Applications are due **Thursday, June 30, 2011**. Click http://www.armaedfoundation.org/grants_scholarships.html for requirements and forms. Click http://www.armaedfoundation.org/scholarships_awarded.html for information about past winners.

The Evolution of E-Discovery Sanctions

By Michael Swarz, "VP Marketing and Operations at eClaris, Inc."



It is now well-established that electronically stored information (ESI) is discoverable if it may lead to information relevant to any party's claim or defense. The 2006 revisions to the Federal Rules of Civil Procedure address ESI expressly and further validate the notion that ESI shapes modern litigation, from disclosure through trial.

Given the volume of ESI many businesses generate that should be preserved appropriately, and possibly produced, it is no wonder that many companies and law firms have made e-discovery a top priority. Companies are particularly sensitive to their ESI due to the possible liability involved, and they are constantly seeking ways to negate the possibility that a court may impose harsh sanctions.

Foreshadowing of E-Discovery Sanctions

E-discovery sanctions primarily arise out of sanctions traditionally imposed for spoliation of evidence. Simply put, traditionally, spoliation refers to the manipulation or destruction of evidence and can also refer to not properly maintaining or preserving evidence. As applied to e-discovery, if, for example, data were altered during the reviewing, collecting, or processing of ESI, spoliation may have occurred and a court may impose sanctions against a culpable party.

Generally, the issue of spoliation will arise from a demand for disclosure or discovery, followed by a motion for sanctions as a result of the other side's failure to produce the information sought. Courts may impose spoliation sanctions in response to a party's discovery missteps, such as failing to preserve, destroying, or losing relevant evidence, regardless of whether the spoliation was intentional. Common types of spoliation sanctions include monetary sanctions, additional discovery, preclusion of evidence, an adverse inference jury instruction, and even dismissal.

E-discovery sanctions have their genesis in Federal Rule of Civil Procedure 37, which gives the court the power to discipline a party that circumvents disclosure and discovery rules and orders. Courts have used this authority to guard against misconduct and impose sanctions on those who improperly exploit and distort disclosure and discovery procedures. The primary purposes of such sanctions are to elicit mandatory disclosures, to deter and punish improper conduct, and to address any prejudice suffered by an innocent party.

The Top Four

There are four primary types of e-discovery sanctions: economic sanctions, adverse inferences, preclusion sanctions, and entry of default. Each type has its own unique application.¹

1. How Much Cash Is in Your Wallet? Monetary sanctions are often considered by courts as a milder form of discipline fore-discovery. Monetary penalties do not necessarily determine a particular outcome in a

"Reprinted with permission from ABA – Pretrial Practice & Discovery (2008) Fall Vol. 17, No.1 pgs 17-18"

case. Nonetheless, monetary sanctions can hurt as well. Indeed, in certain instances, courts have imposed substantial monetary sanctions.

A groundbreaking case dealing with e-discovery monetary sanctions is *Zubulake v. USB Warburg*.² *Zubulake* involved an employment discrimination claim made by a former Wall Street executive who sought ESI in discovery requests. Ultimately, the court found that the executive's former employer had failed to properly maintain and produce relevant ESI (including backup tapes and email), and returned a verdict for \$29.3 million including \$20.2 million in punitive damages.³

Monetary sanctions for e-discovery missteps frequently include attorney fee awards. For example, in *Wachtel v. Health Net*,⁴ the court imposed substantial sanctions on an ERISA defendant for continually exploiting discovery. In particular, the court found that the defendant neglected to search or properly retain email.⁵ This omission triggered the court to impose a slew of sanctions, including awarding the plaintiff applicable attorney fees related to the defendant's misconduct.⁶

These and other cases imposing monetary sanctions teach many important lessons. Parties must be aware of their duty to preserve ESI and must be frank when dealing with counsel and the court during disclosure and discovery. Attorneys must become well versed in their clients' information technology systems; they must know that there is an obligation to preserve and produce ESI, and learn about the mechanics of doing so.

Attorneys also need to work with a knowledgeable representative from their client's information technology team to discuss effective e-discovery procedures. Having a true grasp of the scope of a client's ESI will empower an attorney to avoid having to hastily locate additional ESI, and then needing to try to justify or explain its tardy disclosure (or, worse yet, having relevant ESI be destroyed).

2. Instructing a Fact-Finder to Assume the Worst. Courts have long instructed juries to make an adverse inference as a form of sanctioning a party when it comes to discovery abuses. This is equally true for e-discovery abuses. An adverse inference occurs when a court instructs the jury to assume that the party who destroyed or tampered with evidence did so because the party was aware that it was damaging to their position. Adverse inferences are difficult to overcome and can force a case to conclude prematurely, or badly, or both.

As evidenced by *In re Napster*,⁷ adverse inferences can have a damaging effect on a party's case. In that case, the district court ruled against a defendant who invested in Napster. The court concluded that the defendant continually purged employee emails without considering if they were relevant to litigation.⁸ As a sanction, the court instructed the jury to assume that the deleted emails not produced were adverse to the defendant.⁹

In re Napster a good example of a court utilizing the adverse inference jury instruction as a proportionate remedy sanction a party even though the actual number of email messages not produced was minuscule. When vital data are missing, an adverse inference has the potential to be outcome determinative and may be as damaging as entry of default.

In addition, courts have used adverse inference sanctions while mixing in some form of monetary sanctions. A prime example was *Coleman Holdings, Inc. v. Morgan Stanley & Co., Inc.*, a Florida state court case decided in 2005.¹⁰ In that case, after Morgan Stanley verified that all pertinent electronic evidence had been produced, other relevant backup tapes were found to exist (contrary to the verification). As a result, the court concluded that Morgan Stanley violated the discovery rules and orders. As a sanction, the court instructed the jury regarding the failure to preserve documents.¹¹

"Reprinted with permission from ABA – Pretrial Practice & Discovery 2008 Fall Vol. 17, No.1 pgs 17-18"

3. Trying a Case with One Hand Behind Your Back. Another useful mechanism is the preclusion sanction, which means that as a sanction to a party who failed to comply with a court's discovery rules or orders, a court will not admit particular evidence. Preclusion sanctions can occur as a separate sanction or in addition to other types of sanctions. Usually, courts will use a preclusion sanction for evidence that was not adequately or timely disclosed or produced.

Preclusion sanctions can severely weaken the substance of an opponent's case. A recent court case, *R & R Sails, Inc. v. Insurance Co. of the State of Pennsylvania*.¹² illustrates this point. This case turned on the issue of whether a preclusion sanction was an appropriate response to a discovery violation. The court held that indeed it was, because the insurer plaintiff had failed to search for and produce relevant ESI. As a result, the court imposed a preclusion sanction on the insurer that barred the insurer from offering evidence related to ESI that had not already been produced to the other side.

Courts appear cautious in using preclusion sanctions, which are generally limited to the most outrageous discovery transgressions. Nevertheless, by its mere existence, the preclusion sanction serves its purpose as a robust deterrent to a party contemplating misusing the discovery process, and encourages counsel to be truthful when dealing with opposing parties as well as the court.

4. Sudden Death. In the most extreme cases, a court may enter default or a default judgment against the party abusing the discovery process. Entry of default is the most severe e-discovery sanction the court can impose.

A default judgment was entered as an e-discovery sanction in *Quantum Communications Corp. v. Star Broadcasting*.¹³ whose central issue was the purchase of a radio station. The *Quantum* court noted that the defendant had neglected to produce vital email in response to requests for production. Once those key emails were located—via a third party no less—they squarely contradicted the defendant's testimony. Although vigorously opposing the "sudden death" sanction, the court concluded that default judgment was appropriate and also imposed the equitable relief of specific performance in favor of the plaintiff.¹⁴

Conclusion

Businesses rightfully continue to struggle to comply with new e-discovery realities and bemoan the cost of doing so. Not fulfilling one's e-discovery obligations, however, can result in far worse consequences. As cases noted here demonstrate, courts have multiple types of sanctions at their disposal to be imposed on those who abuse the e-discovery process.

Courts are increasingly willing to impose such discovery sanctions on parties who fail to fulfill their e-discovery obligations, even when the party has not willfully tampered with or destroyed relevant evidence. Parties are on notice of severe e-discovery sanctions available for even passive action and inaction, such as neglecting to stop routine email deletion protocols. As a result, businesses must be vigilant in pinpointing, preserving, and producing all relevant ESI.

Parties and counsel must anticipate that a court will pore over disclosures and discovery to determine if sanctions are appropriate. Failing to be vigilant can be disastrous, with each side taking the risk that any destruction of relevant ESI may lead to harsh sanctions that can make or break a case. A thoughtful and thorough approach to ESI prior to and during discovery is now a prerequisite to the success of any case.¹⁵

Endnotes

1. These four types of sanctions do not represent the universe of possible e-discovery sanctions. For example, courts may invoke countless other versions of e-discovery sanctions, such as revoking counsel's pro hac vice status and forcing a party to locate another attorney. These other types of e-discovery sanctions, although less popular, can be no less damaging as courts have become creative in determining how to enforce e-discovery infractions.
2. Zubulake v. UBS Warburg, 217 F.R.D. 309 (S.D.N.Y. 2003).
3. Zubulake v. UBS Warburg LLC, 382 F. Supp. 2d 536 (S.D.N.Y.2005).
4. Wachtel v. Health Net, Inc., 239 F.R.D. 81 (D.N.J. 2006).
5. *Id.* at 84.
6. *Id.* at 85.
7. *In re* Napster, Inc. Copyright Litig., 377 F. Supp. 2d 796, 802–04 (N.D. Cal. 2005).
8. *Id.* at 805.
9. *Id.* at 806.
10. Coleman Holdings, Inc. v. Morgan Stanley & Co., Inc., 2005 WL 679071 (Fla. Cir. Mar. 1, 2005).
11. *Id.*
12. R & R Sails, Inc. v. Ins. Co. of the State of Pa., 2008 U.S. Dist. LEXIS 44552 (S.D. Cal. Apr. 18,2008).
13. Quantum Comm'ns Corp. v. Star Broad Inc., 382 F. Supp. 2d 1362 (S.D. Fla. 2005).
14. *Id.* at 1366.
15. For additional ESI resources, see www.law.cornell.edu/rules/frcp/Rule37.htm (discussing extent of sanctions available under Rule 37);www.lexisnexis.com/applieddiscovery/lawlibrary/focus_07.asp (discussing Zubulake); www.law.com/jsp/legaltechnology/edd.jsp (discussing e-discovery process generally); <http://technology.findlaw.com/electronic-discovery/electronic-discovery-guide/> (similar); <http://technology.findlaw.com/electronic-discovery/electronic-discovery-wizard.html/> (similar).

Michael Swarz, J.D., VP Marketing and Operations

Michael Swarz currently serves as VP of Marketing and Operations for eClaris, Inc. eClaris offers consultative solutions helping clients respond to investigative or legal requests for digital data. Services include: tactical digital forensics, litigation hold, evidence storage, data hosting and backup tapes. Michael is well versed in the state and federal laws that relate to electronic discovery and has written extensively on the subject. His recent article, *The Evolution of eDiscovery Sanctions*, provides a guide to the penalties a court can impose on those abusing the discovery process and has been published by the American Bar Association. Michael is a graduate of both Brandeis University and New England Law in Boston. He can be reached at mwarz@eclaris.com, 213.784.0231 and through www.eclaris.com

"Reprinted with permission from ABA – Pretrial Practice & Discovery (2008) Fall Vol. 17, No.1 pgs 17-18"

WHY ATTEND ARMA PACIFIC REGIONAL LEADERSHIP CONFERENCE ON JULY 17-19, 2011 IN SAN JOSE?

The following are results from the Chapter Leadership Survey conducted by ARMA International in January 2011.

- 47% believe In person training at Region Leadership Conference is a Top Resource they utilized from ARMA International as a Chapter Leader
- 24% believe In person training at Region Leadership Conference is a Most beneficial resources provided by ARMA International as a Chapter Leader

Published in ARMA International (May 2011) Chapter Connections

ANSWERS TO CRM EXAM QUESTIONS

- | | |
|------|-------|
| 1. B | 2. C |
| 3. E | 4. E |
| 5. A | 6. E |
| 7. E | 8. C |
| 9. C | 10. D |

Introduction

The nature of business information technology is at a crossroads. On the one hand, pressure to enforce good corporate governance, secure sensitive information and meet compliance mandates would seem to demand ever-tighter controls. On the other hand, the need to respond to new business opportunities, to collaborate with a greater number of partners more closely, and the emergence of new technologies are placing unprecedented strain on existing security processes and practices.

One of the most commonly cited areas where these two opposing waves meet is in the area of control over user-owned devices that may hold sensitive or proprietary data. This problem has become acute as the storage power of removable media such as flash drives and portable hard drives has rapidly outstripped the security controls designed to manage them.

This two-part whitepaper will address some of the best practice approaches that you may wish to evaluate and potentially adopt in order to reduce the risk of USB devices becoming the source of a significant leak or virus infection.

Part one will discuss the nature of the challenges facing organizations such as yours that wish to reduce the risk of a data breach caused by the unmanaged use of removable media such as USB flash drives. It will also discuss how to begin to address these challenges, from building policy to educating users.

Part two will address the various controls that can be put in place, discuss which are appropriate depending on the type of information you wish to secure, and also provide guidance on an idealized solution.

:

THE REMOVABLE MEDIA PROBLEM

The storage capacity of removable media such as USB drives has grown at an almost exponential rate for the last several years. With storage capacities now measured in hundreds of gigabytes and even terabytes, and devices that are so cheap and small they have become almost disposable, the capacity for sensitive information to be copied onto a device, and then lost, has become a source of significant concern for IT and security professionals. A single USB drive could hold millions of patient records, and should it be lost, leave a hospital system open to fines and lawsuits. A single device could carry billions of dollars worth of intellectual property, and yet controls to monitor and manage the use of such devices have been slow in coming and are often poorly enforced.

Significant losses of protected information continue to reach the news, especially involving unencrypted information stored on flash drives and accidentally lost or misplaced. Furthermore, recent reports show that USB drives are increasingly being used to transport malware from system to system, often without the owner's knowledge.

As the regulatory pressure to secure information grows both in the US and the rest of the world, the need to quickly enforce security on removable media has never been greater. Why then, has this problem not been fully addressed?

THE REMOVABLE MEDIA CHALLENGE

There are many reasons why some organizations now find themselves playing a game of catch-up with USB security. Often, senior management have not prioritized removable media security or allocated resources to address the problem. In other cases, although technical controls have been put in place, they are either inadequate or have met with resistance from users who expect significant freedom to use their USB devices within the corporate network as easily as they can at home. Whatever the level of security you currently have in place, it is likely that your organization faces some of these challenges still:

The Range of devices

The range of devices that need to be protected and managed presents a significant technical and process hurdle. USB devices range from simple flash drives to high-capacity external storage, and include Mobile computing and Smart Phones. Even within these broad categories there are numerous sub-types. For example, flash drives may be the traditional type, they may be U3 devices capable of auto-executing applications, or even secure devices with their own encryption built-in. Likewise, the range of mobile computing devices and smart phones has grown dramatically, especially with the widespread use in the corporate world of RIM blackberry's, Android-based devices, and the growing number of Apple offerings such as iPhones and iPads.

These devices will all need to be taken into consideration while planning for endpoint protection of data, and as the diversity of the platforms grow; traditional approaches to securing them have become difficult to manage at best, and in many cases, simply obsolete.

User resistance

One of the most significant, and yet least discussed, challenges for USB device protection is user resistance. Users expect to use USB flash drives for a variety of purposes, from moving files between systems to backing

up data and sharing information. Once restrictions are placed on the way USB devices are used, significant resistance from the user community often results. This can derail even the best-planned encryption project, or as often happens, leave pockets of unprotected systems and users that ultimately represent potential risk for a breach to occur.

Management cost

Deploying any new technology incurs some degree of cost. However, deploying software to enforce policies around a technology as ubiquitous as removable media can result in some significant management headaches. One of the biggest management challenges is simply deciding what level of control should be put in place, and how to deal with data already on a USB drive that may not need encryption.

As more and more users bring their own devices into the enterprise network, and as the consumerization of business computing takes effect, this problem often grows rapidly in complexity. Key management planning is a vital issue to address – especially as it pertains to restoring access to devices if the user is unable to remember the key, as is addressed below.

Recovery issues for lost keys

The benefit of encrypting data on removable media devices is that it provides protection to your organization in the event that device containing sensitive information is lost. However, you must also plan to support users who lose (or forget) their encryption keys. Key management, specialty recovery of lost keys, can be challenging when the systems in question are within the corporate network. When the keys are for USB devices that are distributed around the world, the problem may seem insurmountable. The difficulty in helping a remote user recover data from a thumb drive at short notice can often spell the end of device encryption pilot projects. As will be discussed later, the ideal solution should enable users to recover their own keys with only minimal involvement from central support and helpdesk staff. However, if this is not possible, the cost of

supporting thousands of users, each of whom may possess several drives, can be excessive.

Reporting and auditing

As an essential part of any security and compliance program, reporting and auditing requirements must be met. As sensitive data gets copied to more and more devices, the need to centrally manage and report on the security of those devices grows too. For many organizations, the challenge has been so great that they have simply ignored the problem and instead concentrated on fixed devices within the network. This, of course, leaves them vulnerable not only to a breach, but to an audit finding or failure to meet a compliance mandate.

Lack of visibility of the problem with Senior management

While senior management may well understand the need for controls on devices within the corporate network, and even protection for mobile computing resources such as laptops, there may be little awareness of the risks posed by removable media. The low-cost, high-capacity storage devices that many employees routinely carry with them, and use, represent a significant threat to data security. But without careful education of senior management stakeholders, budgets to address this area of risk may not be forthcoming, or may take second place to more directly visible projects.

PROTECTING YOUR ENTERPRISE—BEST PRACTICES

The most effective approach to reducing the risk from removable media such as USB storage devices is, as in any other area, to adopt a structured methodology based on deciding where the greatest risks lie for your organization and implementing a policy to manage them.

The recommended steps, then, will be:

- Assess Risk
- Build Policy
- Communicating Policy

- Education of Users and Management
- Implementation
- Monitoring and Reporting

Each step will most likely mirror work that is already underway and therefore should be integrated with existing practices and processes to gain the greatest possible efficiencies.

ASSESSING AND QUANTIFYING RISKS

The nature and location of sensitive information should be determined and documented. Access controls already in place should be considered and assessed in the light of USB storage devices, physical and network availability, and existing monitoring capabilities. If sensitive information is stored on endpoint systems rather than in a central server, the following questions should be determined:

- Who has access?
- What is the volume of information available?
- Are USB devices commonly used?
- What capability is there to monitor mounted USB storage devices, as well as copying information to/ from them?

There are numerous risk assessment frameworks commonly in use, and incorporating removable media into them should be a priority. One of the key factors to consider is the extent of regulatory impact from a breach, especially in light of the current multi-state patchwork of breach notification laws, and extension of such mandates as HIPAA with the HITECH act. In the US, for example, a significant portion of the breaches reported by the Department of Health and Human Services are the result of lost portable devices.

BUILD POLICY

All good security policies are built to help enable business while reducing risk. The objective of a removable media and USB device policy (or incorporating policies for USB devices within your existing framework) should be no different. Like any security policy, it should:

- **Be clear** – Is there ambiguity or is the policy clear on what is required?
- **Be understandable** – Can users understand the policy without deep technical knowledge?
- **Set attainable goals** – Is the policy sensible in a real-world situation?
- **Provide sufficient detail to enable action** – Will administrators know how to enforce the policy?
- **Enhance business goals** – Does this policy provide for the support of underlying, core business objectives?
- **Take into account existing policies and practices** – Does the policy on removable media align well with the policy on other types of information technology usage?
- **Reflect the regulatory landscape of the organization** – Does it provide the level of good governance required to meet the organizational mandate needs?

As we discuss later, some of the types of controls that you may wish to put in place to reduce risk from unmanaged USB devices may influence your policy decisions, although policies should never be driven by technical capabilities alone (or even in the majority). Your policy for removable media usage must, above all, reflect the real-world usage of devices by your business user community if it is to be successfully implemented.

Communicate the policy

Any changes to security policy must always be clearly communicated, but it is especially important when that policy affects day-to-day activities such as using USB storage devices. Few users will give any thought to the implications of moving data to and from such

devices, therefore suddenly restricting their use or imposing onerous operational requirements on how they are used without clearly explaining why will inevitably result in resistance and push-back from the business units affected.

As has been seen in many real-world examples, users will expend inordinate amounts of energy to circumvent policies that they feel are unnecessarily restrictive and impact their capability to perform their job function – resulting in weakened security and lost productivity. Clear communication up front is the easiest way to avoid this and address concerns that business users may have.

Educate

Hand-in-hand with communicating any new policies or changes to existing policies is the need to educate users. In fact, it is usually better to begin with more senior management, as their buy-in will be essential to the success of any new policy. Understanding the level of risk that unsecured USB devices represent, and the need to impose some degree of control is vital, however, resist the temptation to bombard managers and users with worst-case scenarios or horror stories. These usually serve only to undermine credibility and therefore call in question the need for controls. Explain how and why controls are to be put in place, show how they will be implemented, and give clear guidance on how business processes will be impacted—especially focusing on how that impact will be minimized.

Part two of this white paper will address which controls to implement and how to build an integrated, centrally managed approach to protecting information and reducing the risk of a breach.

CREDANT Technologies
15303 Dallas Parkway, Suite 1420, Addison, Texas
75001 USA (972) 458-5400
For more information:
www.credant.com
info@credant.com

2011 ANNUAL SPRING RIM SEMINAR Retention



“Records Inventory & Retention Scheduling” – Christine Figueroa, CRM

The 8th Annual SCIE ARMA Seminar was held at the Riverside Canyon Crest Country Club on Wednesday, March 30, 2011. There were a total of 30 attendees at this event that focused on RIM development from Retention, Auditing Records to Professional RIM Development.

Christine Figueroa, MLIS, CRM, Head of RIM at Irvine Company gave an excellent presentation on “How to Create a Records Retention Schedule”. There were two key points in her presentation: drafting your retention schedule & maintenance. She stated after you complete your records inventory that it’s best to create your schedule utilizing the Big Bucket theory. This way you can make it easier for members throughout the organization to understand it.

However, the most important point of her presentation was maintaining and implementing a Records Retention Schedule. You should regularly audit department records retention schedules. There are often times when changes in personal, new software and company policies can impact your current Records Retention schedule.

Auditing



“Auditing your Records Management Program” – Taunya Bauthard

Taunya Bauthard is a Solution Development Executive with Iron Mountain’s consulting practice. For the past 3 years, she has been working with companies to develop Compliant Records Management programs in all facets of information management, including auditing RIM programs.

Taunya has worked in the industry for over 17 years and is a past San Diego Chapter ARMA President and Public Relations Chairperson. Taunya was also the recipient of Iron Mountain’s Award for “Outstanding ARMA Chapter Leadership” in 1998 for her service to the San Diego ARMA Chapter. Taunya resides in San Diego, CA and works with Iron Mountain’s customers in the Western United States.

Taunya addressed the guiding principles for accountability and auditing of your records management program. She explained all the necessary steps from establishing a Steering Committee to involvement of IT department.

There were two important takeaways from her presentation: (1) Regularly communicate changes throughout the organization and (2) Conduct regular audits to ensure your Records Management Program is compliant to the organization’s internal audit process.

Professional Development



“Executive Coaching for the Information Management Professional & CRM Exam Coaching” – Ilona Koti, CRM

Ilona Koti is the founder of Crystalview Consulting Group an independent Record & Information Management (RIM) consulting firm with over 17 years of experience. She is a Certified Records Manager (CRM), Certified Project Manager (PMP), Certified Document and Image Architec (CDIA+) and has a Masters of Library Science (MLS) and Masters of Information Management (MS IM) from Syracuse University.

She has also written and published for ARMA International and sits on the GARP (Metrics Task Force) and the HETF (Higher Education Task Force). Ilona is serving as a Board of Directors member for ARMA International (July 2011) and for CHRAB (California Historical Records Advisory Board).

She spoke about Executive Coaching for the Information Manager and Strategies for passing the CRM. A book will be coming out soon about these topics.

The attendees stated Ilona was “Inspirational & encouraging”, “Very well spent time” and “She presented a very clear, in-depth presentation.”

ICRM Code of Ethics

Certified Records Managers® should maintain high professional standards of conduct in the performance of their duties. The Code of Ethics is provided as a guide to professional conduct.

1. Certified Records Managers have a professional responsibility to conduct themselves so that their good faith and integrity shall not be open to question. They will promote the highest possible records management standards.

2. Certified Records Managers shall conform to existing laws and regulations covering the creation, maintenance, and disposition of recorded information, and shall never knowingly be parties to any illegal or improper activities relative thereto.

3. Certified Records Managers shall be prudent in the use of information acquired in the course of their duties. They should protect confidential, proprietary and trade secret information obtained from others and use it only for the purposes approved by the party from whom it was obtained or for the benefit of that party, and not for the personal gain of anyone else.

4. Certified Records Managers shall not accept gifts or gratuities from clients, business associates, or suppliers as inducements to influence any procurements or decisions they may make.

5. Certified Records Managers shall use all reasonable care to obtain factual evidence to support their opinion.

6. Certified Records Managers shall strive for continuing proficiency and effectiveness in their profession and shall contribute to further research, development, and education. It is their professional responsibility to encourage those interested in records management and offer assistance whenever possible to those who enter the profession and to those already in the profession.

(Reprinted with permission from the Winter 2011 issue of the ICRM's *ProfessioNotes* newsletter).

ICRM 2011 Examination Schedule

Summer:

Parts 1-5, August 1-5, 2011; Part 6, Aug 11, 2011
Registration Open: May 20, 2011 - July 28, 2011

Fall:

Parts 1-5, Nov 7-11, 2011; Part 6, Nov 17, 2011
Registration Open: Aug 19, 2011 - Nov 3, 2011

NEW CRMs

Congratulations to the following individuals in the U.S. and Canada who earned their Certified Records Manager (CRM) designation by passing the Part 6 examination in November, 2010:

Patricia S. Brackin, CRM, Apopka, FL

Jack W. Lydick, CRM, Kyle, TX

John A. Carroll, CRM, Austin, TX

Laura L. McGee, CRM, Boulder, CO

Christopher L. Flynn, CRM, Grand Forks, ND

Ebbie A. Moody, CRM, Castle Rock, CO

James P. Flynn, CRM, Chicago, IL

Linda M. Naj, CRM, Aurora, CO

Stephen F. Goodfellow, CRM, Manlius, NY

Angel R. Ramos, CRM, Blairstown, NJ

Daniel Henrie, CRM, Vaudrevil-Dorion, QB
CANADA

Felishia M. Squires, CRM, Virginia Beach, VA

Wayne S. Hoff, CRM, Calgary, AB CANADA

James R. Strickland, CRM, Decatur, GA

Jay A. Kasperski, CRM, Regina, SK CANADA

Deborah A. Tamborski, CRM, Greenlawn, NY

Kim M. Kindrew, CRM, Hampton, VA

Molly A. Weinbender, CRM, Pasco, WA

Gilles F. Legare, CRM, Millet, AB CANADA

Clinton W. Wentworth, CRM, San Antonio, TX

Margaret M. Lell, CRM, Cary, NC

Alice Branham Young, CRM, Titusville, FL

Phoebe Lopez-Walter, CRM, Torrance, CA

(Reprinted with permission from the Spring 2010 issue of the ICRM's *ProfessioNotes* newsletter).

Ex-Employee, Social Media and a Security

Breach: Oh My! By Lisa J. Berry-Tayman, Esq.

Lisa is an active member of ARMA International and serves as the President of the Greater Indianapolis Chapter of ARMA



It's a company's worst nightmare – a rogue ex-employee with confidential company information about the sensitive information, in particular alleging an unreported security breach by the company. (An alleged security breach caused by the loss of backup tapes, involving the loss of personal information, including names, addresses, social security numbers, payroll data, checking account and credit card information on approximately 400,000 customers.) But, if the former employee signed an employee covenants and non-disclosure agreement, an agreement in which the former employee agreed to maintain the confidentiality of company's business information, the company's business information, the company can go to court and seek enforcement of the agreement. Problem solved, right? No. When the company in Cambridge Who's Who Publishing, Inc. v. Sethi case went to court and sought enforcement of their agreement in the form of an injunction to restrain the former employee's continued disparaging remarks by blog and email, the company's request was denied. Oh my!

Case

In January 2011, the New York Supreme Court denied a company's injunction requesting that a former employee be prohibited from making disparaging comments about the company. Cambridge Who's Who Publishing, Inc. v. Sethi, 009175/10, NYLJ 1201482619238 (Sup. Ct. Nassau Cty. Jan. 25, 2011). A key factor in this denial was that the former employee was using social media and email to discuss a matter of public opinion – an alleged security breach. The court stated that discussions on matters of public concern are protected by the U.S. Constitution. The judge acknowledged that the former

employee's intent may have been to disparage the business or to retaliate against the company for his discharge; but nonetheless, the content of the communication — the loss of personal information “implicates the economic interests of a large number of people” and that is protected free speech under our Constitution. The court held that the company had failed to establish ‘extraordinary circumstances’ to justify restraint on prior speech and denied the company's injunction.

What Now?

The true issue in this case is not the enforcement of the employment agreement, but the alleged security breach. So, remove the issue of the security breach. Arguably, if the former employee had not blogged or emailed about a security breach — a matter of public concern, then the company could have successfully enforced their employee covenants and non-disclosure agreement.

Protect your company with employee covenants and non-disclosure agreements, but add an Information Management and Information Protection Program. These defensible programs are designed to help your business find, use, manage, and protect company information by marrying policy/procedure and the right technology. In the case above, if the company had implemented Information Management and Information Protection Programs (and followed them), the company would have known if and where personal information resided on their backup tapes.

They could have used appropriate technology, such as encryption to protect the personal information. (Under many states' Breach

(Ex-Employee, Social Media and a Security Breach: Oh My! Continued)

Notification Laws, loss of encrypted information does not require disclosure.) And, if the company did experience a breach, under their Information Protection Program, they would have made the appropriate timely disclosures to government and their customers, as required by law.

Don't wait for the nightmare of an Ex-Employee, Social Media, and Security Breach. Remove the security breach component by proactively establishing Information Management and Protection Programs, in addition to your employee covenants and non-disclosure agreement. If and when a security breach occurs, your company will be ready to respond appropriately and confidently. And, if a former employee makes disparaging comments about your company, the court can focus on the non-disclosure agreement, not on the security breach.

Author: Lisa J. Berry-Tayman, Esq., CIPP is the owner of Information Consulting, a consulting group focused on information management, information protection and e-discovery. She may be reached at LBTayman@InformationConsulting.biz or 317-908-0377.

2010 – 2011 Year in Pictures



25th SCIE ARMA Anniversary Celebration at Mission Inn Hotel

The Southern California Inland Empire ARMA Chapter No. 127 celebrated their 25th Anniversary Celebration at the Mission Inn Hotel on Thursday, May 12, 2011 in the Spanish Art Gallery. There were 7 of the past 14 chapter past-president present at the event.

- Ron Harrington (1985-1987)
- Mary Cox (1990-1992)
- Steve Gray (1993 & 1996)
- Brenda Hutchinson (2002-2005)
- David Wilkerson (2005)
- Debora K. Thomsen (2006-2008)
- President, Brandon L. Reeder (2008-2011)

David Fleming, Pacific Regional Coordinator/Utah-Salt Lake Past-President and Central Coast President Manual Bulwa attended the event, too.

The following annual awards were presented as follows:

ARMA Service Years

20 years
Mary Cox
Steve Gray

15 years
Naty Kopenhaver

10 years
Debora K. Thomsen
Cindy Simmons

Chapter Vendor of the Year – Iron Mountain

Chapter Member of the Year – Debora K. Thomsen

Chapter Leader of the Year – Brandon L. Reeder

Non-Member Certificate of Appreciation – Laura P. Reeder

SCIE ARMA Hall of Fame Award Inductee No. 1 – Ronald Harrington, CRM

- Original Charter Member (1985)
- UIEC 1st Chapter President (1985 – 1987)
- Chapter Past-President (2 terms)
- Chapter Vice-President (1 term)
- Programs Director (5 terms)
- Education Director (2 terms)
- CRM Advisor (1 term)
- Special Projects (1 term)

We Thank our Event Sponsors:



**SCIE/ARMA CHAPTER # 127
BOARD OF DIRECTORS
FY 2010 - 2011**

President

Brandon L. Reeder
K&N Engineering, Inc.
(951) 826-4000
BrandonR@knfilters.com

Vice President

Rhonda Basore
City of Murrieta
(951) 461-6030
rbasore@murrieta.org

Secretary

Debi Thomsen, CMC
(951) 688-6081
deborathomsen@sbcglobal.net

Treasurer

Traci R. McGinley, MMC
(909) 208-5828
tracimcginley@sbcglobal.net

Hospitality Director

Justin Lee
Iron Mountain
(714) 323-6954
justin.lee@ironmountain.com

Membership Director

Brenda Hutchinson, D.P.A.
United Health Group
(951) 328-6318
brenda.hutchinson@uhc.com

Programs Director

(Open)

Webmaster

Kylene Sotelo
City of Chino Hills
(909) 364-2631
ksotelo@chinohills.org

Chapter Mailing Address:

SCIE/ARMA
P.O. BOX 1434
RIVERSIDE, CA. 92501-1434

Newsletter Publisher & Editor:

Brandon L. Reeder
1455 Citrus Street
Riverside, CA. 92507
(951) 826-4000 ext. 4302
BrandonR@knfilters.com

2010 – 2011 Sponsors

PLATINUM SPONSOR



GOLD SPONSOR



SILVER SPONSOR

