

RECORDS IN THE NEWS, FOR BETTER OR FOR WORSE

Security for records and for private information is a hot topic today. Unfortunately, not a day goes by without there being an instance of private information falling into the wrong hands or paper records being thrown away as trash instead of being shredded.

For instance, last February in Portland, Maine, 30 years worth of payroll records—with names and Social Security numbers—were dumped into an outdoor trash bin over the President's Day weekend. The pink and yellow time slips were records from the Portland public school district, discarded by custodians cleaning out the former central office prior to the district's move to a new building.

Dick Paulson, finance and operations director for the school district, said the bin's contents were loaded onto a truck late Monday night or early Tuesday morning and taken straight to an incinerator. He also said that employees usually shred documents, but did not in this case because there were so many documents. Nevertheless, this incident earned the school district unfavorable publicity in local media.

Another move to a new building, another records disaster

In February 2006, the Denver Election Commission moved to a new office. In early June, the commission admitted that about 150,000 voter records had been missing since February, but claimed by mid-June that approximately 87,000 records had been found.

The rest are still missing, presumably in a filing cabinet that cannot be located. Shortly after the move, someone noticed that a file cabinet was still in the former office. When the moving company, Prestige Corporate Relocation, went back for the filing cabinet, it was gone.



Consequently, the commission had to notify voters who registered between 1989 and 1995 that they could be susceptible to identity theft.

Medical records on 365,000 patients were stolen in Oregon

In January, Providence Health System in Oregon disclosed that 365,000 medical records on disks and tapes were stolen from an employee's van. Then on February 27 and March 3 during two car break-ins, laptops were stolen with the records of 122 Providence hospice and home-care patients in Snohomish County, Washington.

These events triggered inquiries at the state and federal level, and a class-action lawsuit was filed. As of late May, it did not appear that criminals had exploited the stolen records. However, Providence will spend \$7 million to \$9 million to extend credit protection to those whose records were stolen. For the 122 patients of Providence Home Services, the company is providing free the Kroll ID TheftSmart package of credit monitoring and restoration services, as announced on February 14.

BUSINESS RECORDS MANAGEMENT Bulletin

These events have also given impetus to state legislation that will regulate businesses which handle sensitive information, as well as providing protection for consumers who have been defrauded by misuse of their personal data. Oregon has no law requiring reporting of data security breaches unlike its neighbors Washington and California and at least 23 other states.

Closing of medical imaging company opens can of worms for patients

In the Pittsburgh, Pennsylvania area, a medical diagnostic imaging company called Main Medical closed unexpectedly in early April, leaving thousands of patients without access to their mammograms, X-rays, ultrasounds, CT scans, echocardiograms, and other tests.

For some weeks after the closing, former employees volunteered their time so that patients had a chance to retrieve their records. But workers found new jobs, there were fewer volunteers to help, and more patients began calling the state Attorney General Tom Corbett.

Under a court order, Main Medical's several locations reopened so that patients could get their records. By mid-June, 3,426 records had been returned and another 922 patients had applied for their records to be retrieved.

That left about 147,000 unclaimed files in the company's possession. A representative for the company said the intent was to transfer the records to a hospital, a new imaging center, or a storage facility.

BRM is proud to be appointed by the Attorney General as Records Management custodian for Main Medical.

Washington, DC is awash in computer data breaches

In recent weeks several federal agencies have been affected by losses of computer data. On May 3, a laptop was stolen from the home of a Veterans Affairs Department employee. Its hard drive contained Social Security numbers and birthdays of 26.5 million veterans and current military troops. Luckily, by late June the laptop had been turned in and the FBI surmised that no one had accessed the information. Further investigation showed that the VA analyst whose home was broken into had received permission to work from home with the laptop and its sensitive data.

In late June, a civilian web site appeared with Social Security numbers and other personal data from 28,000 U. S. Navy sailors and their family members. The web site came down and the Navy said there was no indication the data was used illegally. But the 28,000 persons involved were advised to monitor their bank accounts and credit cards.

In mid-June, there were indications a hacker had accessed names, Social Security numbers, and photos of 26,000 Agricultural Department employees and contractors in the Washington, DC area.

Itinerary for President Bush's trip to Florida found in trash

On May 9, a public sanitation worker in Washington, DC found a stack of papers next to a trash truck, papers with comprehensive details about President George Bush's trip to Florida that month. The papers included exact arrival and departure times for Air Force One, Marine One and backup choppers Nighthawk 2 and 3. The papers also listed every passenger on each aircraft, and had the President's exact schedule for the day, as well as the order for vehicles in the motorcade.

When a copy of the schedule was faxed by WUSA-TV to the Secret Service, the response was that it was a White House staff document, not from the Secret Service, and was "official" but not classified. Many White House offices have "burn bags" for sensitive documents, but this stack of papers became ordinary trash.

"Do as I say, not as I do."

A recent survey of 248 IT professionals showed that 56% had downloaded non-encrypted corporate information onto memory sticks. Of those responding, 65% were aware that removable media can present a security danger, while 66% admitted they had not changed their security policies regarding removable devices. Only 21% used passwords and encryption, and 12% banned removable media from their workplace. The survey, by Pointsec Mobile Technologies, Inc., was conducted with IT persons who, ironically, had attended the Infosecurity Europe 2006 conference in London in May.

Prices for removable media are getting lower while their capacity gets higher, and more people are using them at work. According to Martin Allen of Pointsec U.K., the results show the need to introduce strict guidelines on the use of removable media devices in the workplace, and to invest in software that will force the encryption of all data put on a mobile device. Employers must ensure that all staff know non-company devices are not to be used with the company network.

Is there more you can do to secure your data?

If you think there are vulnerabilities in your records and information management, talk with your storage contractor for ideas on how to improve your system. Security is as important to your contractor as it is to you.

BE PREPARED FOR SEASONAL THREATS TO YOUR ORGANIZATION'S SURVIVAL

With hurricane season upon us and ongoing flooding in the northeast, businesses can take the opportunity to plan for business continuity and take a moment to look through disaster recovery resources available from ARMA International. As a not-for-profit professional association and the authority on managing records and information, ARMA International encourages organizations to update and review their Business Continuity Plan (BCP).

Planning and Prevention

ARMA International suggests having a BCP, which includes policies and procedures that enable an organization to effectively and efficiently respond to an event so that critical business functions continue without interruption.

The 2006 Business Continuity Market Survey of 5,000 U.S. IT professionals conducted by OpenSky Research revealed that nearly half of the surveyed businesses do not currently have a BCP in place. Shockingly, nearly 13% of respondents said they have no plans to implement a BCP. These numbers are astounding when studies show how important BCPs are to businesses. For example, ComputerWeekly.com reported that a recent University of Texas study revealed 94% of companies suffering a catastrophic data loss will not survive, as 43% do not reopen and 51% close within two years.

Business continuity solutions protect companies from any unplanned interruption that prevents access to business-critical data and information technology (IT) applications. With the resources ARMA makes available to records management professionals and their organizations, businesses can be prepared for the worst.

ARMA International's site, located at <http://www.arma.org>, has been a key resource for professional information for ARMA members. Disaster recovery experts from ARMA International have determined which information management-related materials will be most valuable to those aiding in the prevention planning and potential recovery process as businesses prepare for the 2006 hurricane season. These materials are offered as downloadable files from the ARMA site that can be accessed and printed free of charge.

Materials available for free download include:

- Excerpts from the book, *Emergency Management for Records and Information Programs*, including Chapter 8: *Recovery and Resumption of Operations*, and a helpful form from Appendix B: *Initial Damage Assessment Report*. These focus on the steps for responding to an emergency or disaster and for beginning the recovery of information

assets. These response and recovery steps are but a small part of a comprehensive emergency management plan that every organization needs to formulate in order to prepare for disasters and prevent or minimize the loss of records.

- Information on salvage and drying techniques from the ANSI/ARMA 5-2003 Standard: *Vital Records Programs: Identifying, Managing, and Recovering Business-Critical Records*

To download the articles online, visit www.arma.org and see the Industry News headlines on the main page: *Be Prepared for Seasonal Threats to Your Organization's Survival and Half of Businesses Report No Business Continuity Plan*.

ARMA International is the oldest and largest international association dedicated to the management of records and information. ARMA International's 10,000-plus members include records managers, archivists, corporate librarians, imaging specialists, legal professionals, IT managers, consultants, and educators, all of whom work in a wide variety of industries, including government, legal, healthcare, financial services, and petroleum in the United States, Canada, and numerous other countries. ARMA International has more than 125 chapters that provide education and networking on the local and regional levels.

Kallie Foglesong, ARMA International

RECORDS MANAGEMENT ETHICS

In a post-Sarbanes Oxley world, ethics have become more important than ever before in the records and information management profession. Legal compliance, the integrity of records and evidence, and defensible consistency of actions recognized by courts as an integral part of records management program are all impacted by ethical decisions made by records managers. Both ARMA International and the Institute for Certified Records Managers (ICRM) maintain codes of ethics for the records management profession. These documents provide a good basis for decisions impacting records management policies.

The following code of ethics has been adopted by the ICRM:

"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.

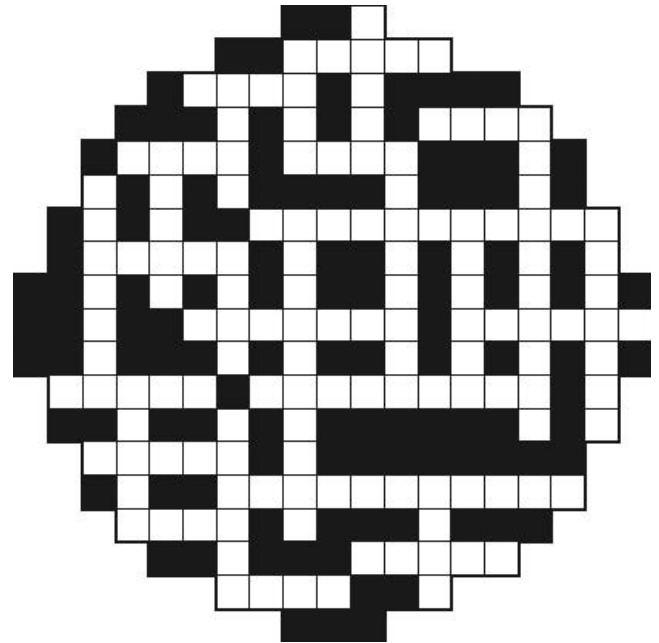
1. Certified Records Managers have a professional responsibility to conduct themselves so that their good faith and integrity shall not be open to question. They will promote the highest possible records management standards.
2. Certified Records Managers shall conform to existing laws and regulations covering the creation, maintenance, and disposition of recorded information, and shall never

knowingly be party 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."

work, he is spending time with his wife Rachel and five-month-old daughter Margaret Anne (Maggie), his greatest accomplishment. Steve, a golden retriever, and Chyna, a jack russell terrier, round out the family. When life gets to hectic, Doug's favorite place to go is a quiet cabin in the woods.

Can you fit the words from the list correctly into the grid?



EMPLOYEE PROFILES

John P. McDonald is a new addition to the **BRM** team, joining us in June 2006, as a customer support specialist. In this position, John serves as the primary contact for all client issues, including client training, on-site access, and any special project requests from clients. He enjoys working with the clients face to face to resolve issues or to complete projects. Customer satisfaction is his number one priority. Graduating from the University of Pittsburgh is John's greatest accomplishment to date, but he looks forward to adding his future career goals with **BRM** to that list. During his free time, John enjoys kicking back and reading at his Moon Township home, attending football games, and taking in a few concerts. When he needs to get away, he and his wonderful girlfriend Erin take off for the Outer Banks in North Carolina.



Douglas Yost also joined the **BRM** family in June 2006, as a customer support specialist. Doug works at our new Johnstown location, and describes his position as "solely pleasing the customer." He enjoys meeting

with clients and making sure they are happy with **BRM's** service. Doug appreciates the fast paced atmosphere at **BRM**, which is never boring. When Doug isn't hard at

4 LETTERS

- APIA
- BONN
- LAOS
- LIMA
- MALE
- MALI
- OMAN
- OSLO
- PERU
- SUVA

- CANADA
- MASERRU

7 LETTERS

- DENMARK
- PHOENIX
- SEATTLE

8 LETTERS

- BARBADOS

9 LETTERS

- LOUISIANA

10 LETTERS

- BIRMINGHAM
- LIBREVILLE

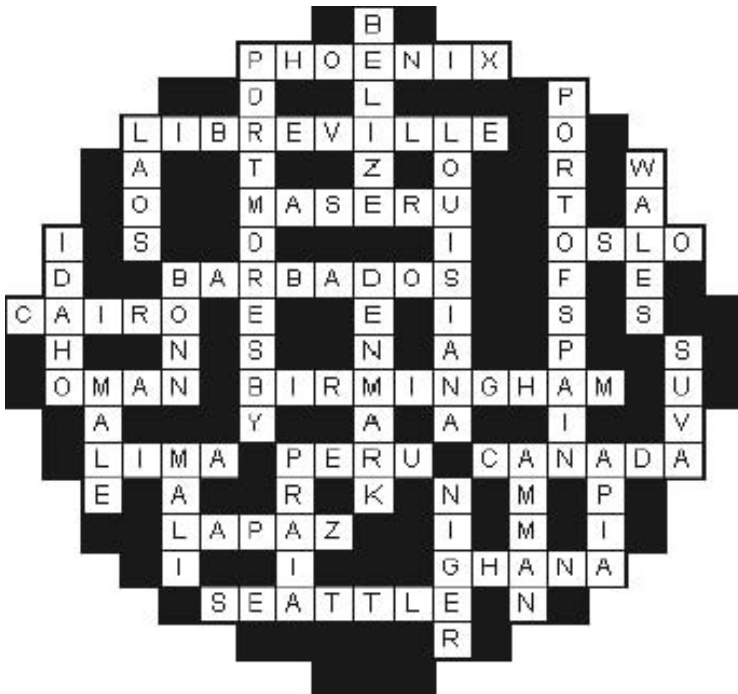
11 LETTERS

- PORT MORESBY
- PORT OF SPAIN

6 LETTERS

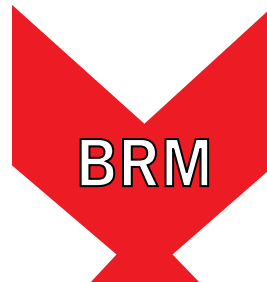
- BELIZE

Answers on last page



CONGRATULATIONS TO BRM'S 3RD QUARTER SUBSCRIBER WINNERS!

Congratulations to **Sandra M. Yoxall** of Williams Coulson; and **Barb Kalanish** of Keystone Digestive Disorder Consultants. They each won two tickets to the PNC Pittsburgh Symphony Pops Series. Thanks so much for your continued support and service to BRM.



**BUSINESS RECORDS MANAGEMENT
BRM Disaster Recovery Services, Inc.**

1018 Western Avenue
Pittsburgh, PA 15233

Voice: 412.321.0600

Fax: 412.321.5152

Web: www.businessrecords.com