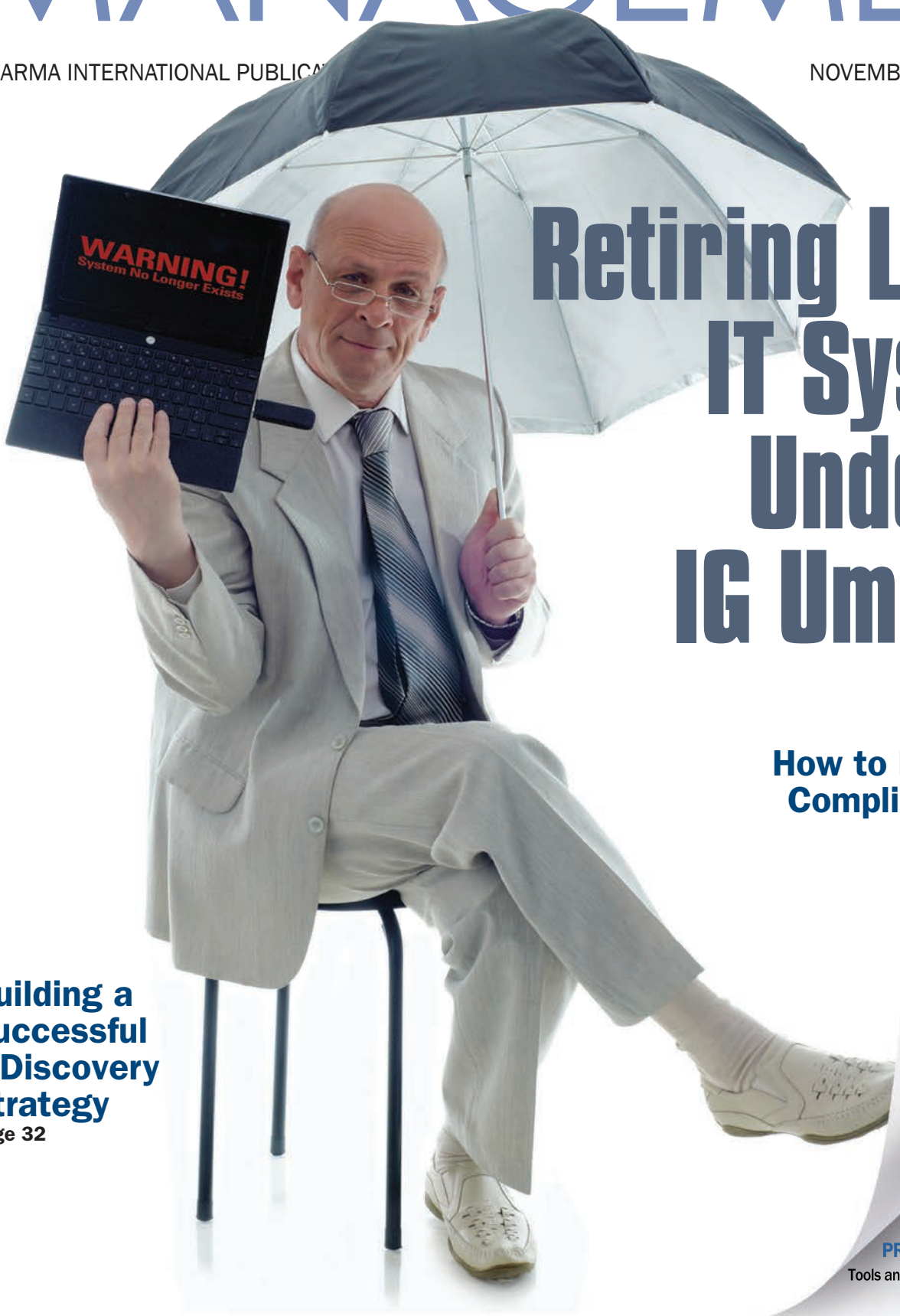
INFORMATION MANAGEMENT

AN ARMA INTERNATIONAL PUBLICA

NOVEMBER/DECEMBER 2013



Retiring Legacy IT Systems Under the IG Umbrella

Page 20

How to Develop a PCI Compliance Program

Page 26

Building a Successful E-Discovery Strategy

Page 32

Special in this issue:

hottopic

PREPARING FOR E-DISCOVERY

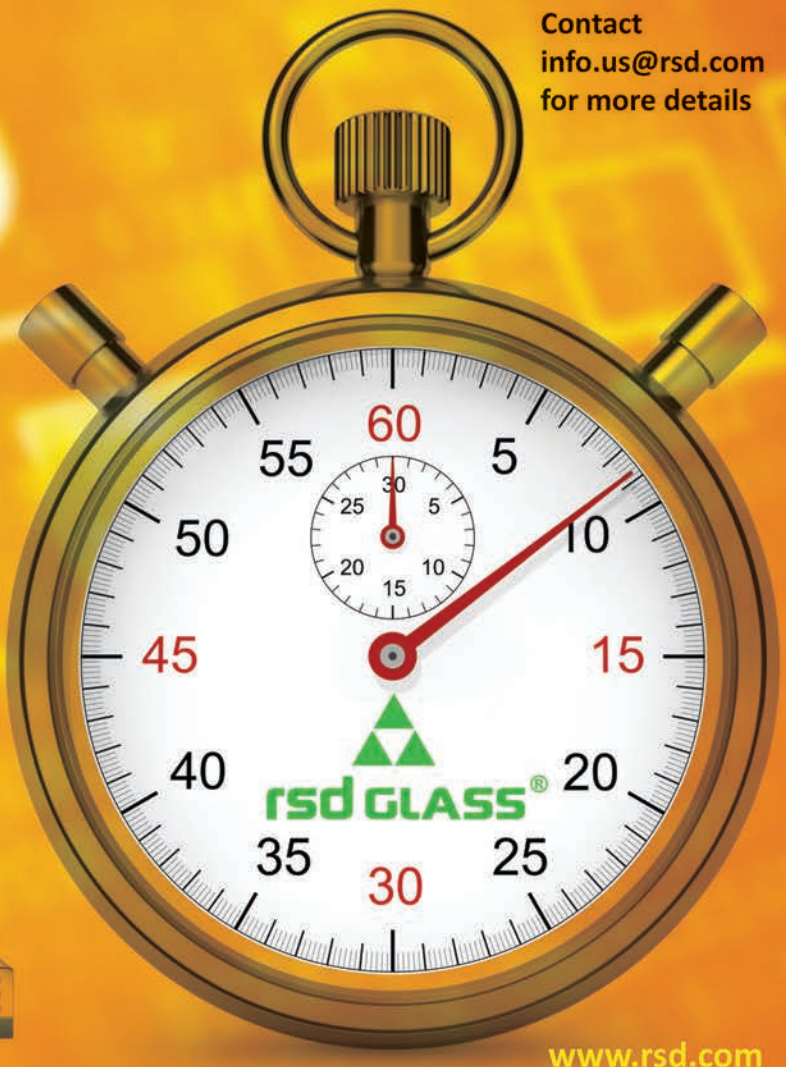
Tools and Techniques to Reduce Risks, Costs

rsd

Deploy Information Governance in Under 10 Minutes

- Define policies to govern corporate information
- Automatically enforce policies “in-place” on premise or in the cloud
- Measure program effectiveness with intuitive dashboards
- Access governed information residing anywhere from any device

Contact
info.us@rsd.com
for more details



Microsoft SharePoint
FileNet
OpenText
THE CONTENT EXPERTS
documentum
a division of EMC
Iron Mountain

www.rsd.com

INFORMATION MANAGEMENT

NOVEMBER/DECEMBER 2013 **VOLUME 47 NUMBER 6**

DEPARTMENTS

4 **IN FOCUS** A Message from the Editor

6 **UP FRONT** News, Trends , and Analysis

FEATURES

20 **Retiring Legacy IT Systems Under the IG Umbrella**
John T. Phillips, CRM, CDIA, FAI

26 **How to Develop a PCI Compliance Program – And Take a Step on the IG Career Path**
Andrew Altepeter

32 **Building a Successful E-Discovery Strategy**
Bill Millican

SPOTLIGHTS

38 **GENERALLY ACCEPTED RECORDKEEPING PRINCIPLES® SERIES**
The Principles at Work at Ameritas: Planning a Unified Approached for Managing E-Records
Julie Gable, CRM, CDIA, FAI

42 **RIM FUNDAMENTALS SERIES**
Keys for Developing a Social Media Policy

45 **IN REVIEW** Noteworthy New Records Management Textbook
Lee R. Nemchek, IGP, CRM

CREDITS

47 **AUTHOR INFO**

48 **ADVERTISING INDEX**

INFORMATION MANAGEMENT

AN ARMA INTERNATIONAL PUBLICATION

Publisher: Marilyn Bier

Editor in Chief: Vicki Wiler

Contributing Editor: Cyndy Launchbaugh, Jeff Whited

Art Director: Brett Dietrich

Advertising Sales Manager: Elizabeth Zlitni

Information Management (ISSN 1535-2897) is published bimonthly by ARMA International. Executive, editorial, and advertising offices are located at 11880 College Blvd., Suite 450, Overland Park, KS 66210.

An annual subscription is included as a benefit of professional membership in ARMA International. Nonmember individual and institutional subscriptions are $140/year (plus $25 shipping to destinations outside the United States and Canada).

ARMA International (*www.arma.org*) is a not-for-profit professional association and the authority on managing records and information. Formed in 1955, ARMA International is the oldest and largest association for the records and information management profession, with a current international membership of more than 10,000. It provides education, publications, and information on the efficient maintenance, retrieval, and preservation of vital information created in public and private organizations in all sectors of the economy.

Information Management welcomes editorial submissions. We reserve the right to edit submissions for grammar, length, and clarity. For submission procedures, please see the "Author Guidelines" at *http://content.arma.org/IMM*.

Editorial Inquiries: Contact Vicki Wiler at 913.217.6014 or by e-mail at *editor@armaintl.org*.

Advertising Inquiries: Contact Karen Lind Russell or Krista Markley at +1 888.277.5838 (US/Canada), +1 913.217.6022 (International), +1 913.341.3742, or e-mail *Karen.Krista@ armaintl.org*.

Periodical postage paid at Shawnee Mission, KS 66202 and additional mailing office.

Canada Post Corp. Agreement No. 40035771

Postmaster: Send address changes to Information Management, 11880 College Blvd., Suite 450, Overland Park, KS 66210.

Log It or Get Fined!

Regulators Have Called BookFactory's Log Book System **The Best They Have Ever Seen**

BookFactory is the Industry Leader. 85% of the Fortune 100 use our Log Books and Lab Notebooks.

Our Books Cost 10-40% Less than Competitors

Quality construction that lasts and stands up to regulatory scrutiny

Sample Log Book Titles We Make:

- Equipment Log Books
- Cleaning and Use Log Books
- Instrument Log Books
- Calibration Log Books
- Maintenance Log Books
- pH Log Books
- Balance Calibration Log Books
- Reagent Log Books
- Access Log Books

We specialize in producing Custom Log Books and Lab Notebooks. Customize page design, cover, size, book numbers, logos, page counts, watermarks.... all to your exact specifications.

Visit www.bookfactory.com/arma

As a Veteran-Owned business BookFactory helps achieve your Supplier Diversity Program goals.

BookFactory, LLC is a Veteran Owned Small Business as verified by the Veteran's Administration (U.S. Department of Veteran Affairs)

BookFactory®

We are a Veteran-Owned Firm, Proudly Making Books in Ohio, USA

Call us today for a free sample:

1-877-431-BOOK

Sales@BookFactory.com
937-226-7100 (for Non-US)

Pursue Knowledge, Collaborative Relationships

As an information management professional, you should come away from this issue with a sense of urgency about two things:

1. Increasing your knowledge of your organization's information technology (IT) infrastructure and of legal, compliance, audit, and privacy issues
2. Developing solid working relationships with the people who lead the programs related to these areas

These are imperative to the successful collaboration needed to ensure that all information – regardless of format or location – is managed throughout its lifecycle, not only to meet business, fiscal, legal/regulatory, and historical needs, but also to contribute to your organization reaching its strategic goals.

For example, when it is time to decommission a legacy information system, you must be involved to ensure the continued availability and usability of the information it contains. John Phillips, CRM, CDIA, FAI, writes in this issue's cover article that doing this depends on extensive planning to ensure backwards compatibility of systems, software, and data formats. And, he writes, "It must involve people who know how to address data security, privacy, and other information risks."

E-discovery is another area where you should play an important role. Bill Millican points out in his article that a strong records and information management (RIM) program is the foundation for a successful e-discovery strategy. E-discovery staff may not be aware of how critical this is, he writes. "They may believe they have the RIM piece covered because they have information technologists who manage their servers, applications, and the data that resides in them; but, it is not that simple."

If your organization processes customer payment cards, your knowledge about IT, compliance, and privacy and your relationships with the leaders of these business areas may position you to lead a Payment Card Industry (PCI) compliance program. Running such a program requires a multidisciplinary team and provides a prudent way to raise awareness of information governance priorities, Andrew Altapeter writes – and it may provide a path for exploring a related information governance career.

A similar multidisciplinary team is helping Ameritas, an insurance and financial services mutual holding company profiled in this issue's Generally Accepted Recordkeeping Principles® article by Julie Gable, CRM, CDIA, FAI. Robin Martin, second vice president of corporate facilities for Ameritas, told Gable that two years into a five-year plan to position the company for effective management of electronic records, she has seen many positive changes, including a heightened awareness of information requirements across the enterprise. "Now if a business area looks at a new system, they are able to ask the right questions," Martin said.

This theme is repeated yet again in the RIM Fundamentals series article, which was excerpted from *Using Social Media in Organizations* (ARMA TR 21-2012). "Successful policy creation and/or modification result from a collaborative, team effort," the article says. It advises RIM leaders to get input from, among other departments, human resources, IT, legal, and marketing.

ARMA International is working hard to provide the resources you need to lead or participate on collaborative information governance teams. Please e-mail *editor@armaintl.org* to let us know what we're missing!

Vicki Wiler
Editor in Chief


TOTAL RECALL™
PHYSICAL RECORDS
MANAGEMENT SOFTWARE
Manage and Protect Your Information
• Manage Onsite and Offsite Records
• Retention and Hold Management
• Organization-Wide Charge-Backs
• SCAN ON DEMAND™
and High-Speed Digital Imaging
• RIM Consulting Services
DHS WORLDWIDE℠
SOFTWARE SOLUTIONS
Call 1-800-377-8406 • www.dhsworldwide.com

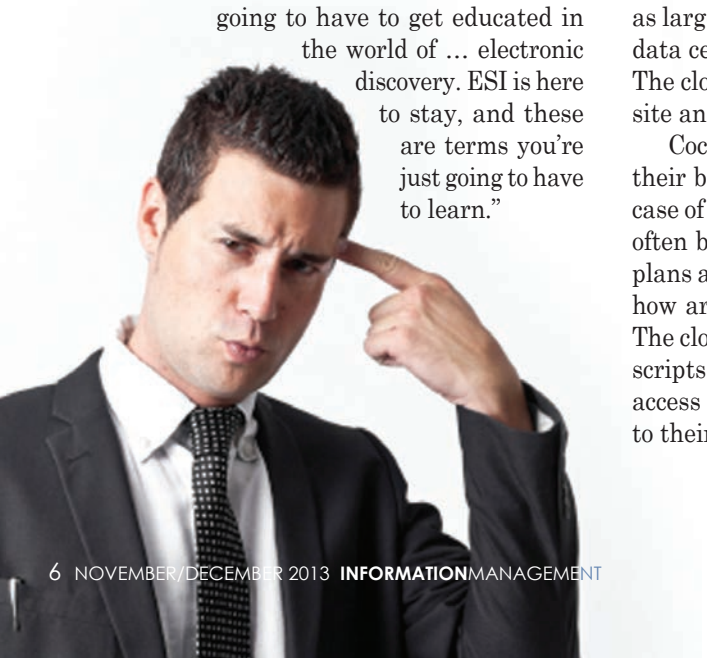
E-DISCOVERY

Court: Ignorance About E-Discovery Is No Excuse

For years attorneys have been advised to become better educated about the ins and outs of electronically stored information (ESI). Failure to do so has recently cost one California attorney $165,000.

According to an article in *Lexology, a California appellate court recent*ly imposed the monetary sanction against an attorney who didn't follow directions well when instructed to allow forensic examinations of her computers during a class action suit. When ordered to produce the records in question in their "native format," the attorney promptly converted the records into PDF and deleted the original Word documents. The trial court then ordered the forensic examination of the attorney's computers, which the attorney refused to allow.

During the discovery dispute, counsel for the attorney reportedly told the court she "[didn't] even know what 'native format' means." The court responded: "You'll have to find out. I know. Apparently [opposing counsel] knows. You're going to have to get educated in the world of … electronic discovery. ESI is here to stay, and these are terms you're just going to have to learn."



CLOUD

Think Cloud, Re-think Disaster Recovery

Add business continuity to the list of considerations if you're deciding whether to move to the cloud. Using it for even the basic purpose of data backup could significantly improve your organization's ability to recover from a disaster.

While most large companies have a backup strategy, many are not sending their data offsite — or far enough offsite — to mitigate geological or meteorological risks, according to Richard Cocchiara, CTO and managing partner of consulting for IBM's Business Continuity and Resiliency Services. "Cloud gives them the ability to store data someplace remote, store it online, and to typically recover faster than from tape," he recently told *Network World*.

Cocchiara said that companies with sophisticated disaster recovery architectures and strategies may benefit from the cloud from financial and control perspectives, for example, because they can test cloud disaster recovery more often. These companies, though, often face the challenge of creating an integrated strategy of processes, architecture, and reporting that is necessary to demonstrate their business continuity capability to auditors, he said.

The cloud levels the playing field for small and medium-sized businesses (SMBs), which are not likely to be able to afford the same protection as larger companies. For example, SMBs typically don't have secondary data centers; they usually rely on tape backups that are stored locally. The cloud enables them to back up data or replicate servers to a remote site and to network to that site when there's a disaster.

Cocchiara reminded all companies, regardless of size, to make sure their business continuity plan is in the cloud so it will be accessible in case of a disaster. "I know it seems like a nit, but you'd be surprised how often business continuity plans are lost in a disaster," he said. "Those plans are critical and if they're stored on a system in the primary center, how are you going to run the recovery if you can't get to that system? The cloud gives them the ability to store those plans and the notification scripts on a server they can access from their laptop anywhere they can access the cloud. And for a business continuity manager, that's critical to their success."

E-MAIL

NY Court Rules E-mail Signatures Valid

A U.S. state of appeals panel recently ruled that signing your name to an e-mail is comparable to physically signing a printed document. This is the third appeals panel to support the validity of e-mail in contractual negotiations.

"Given the widespread use of e-mail as a form of written communication in both personal and business affairs, it would be unreasonable to conclude that e-mail messages are incapable of conforming to the criteria of CPLR [Civil Practice Law and Rules] 2104 simply because they cannot be physically signed in a traditional fashion," New York Appellate Justice Sandra Sgroi wrote in *Forcelli v. Gelco Corporation*, 27584/08. CPLR 2104 states that "an agreement between parties or their attorneys relating to any matter in an action…is not binding upon a party unless it is in a writing subscribed by him or his attorney." It also requires the agreement be "signed" by the party or the attorney.

The *Forcelli* case centered on the enforceability of an e-mail that summarized an apparent agreement to settle a claim from an automobile accident. The official settlement documents, mailed the following day, pointedly referenced the e-mail confirmation. During the time it took to return the signed documents, the court granted the defendant's motion to dismiss the complaint. But the plaintiff argued the agreement had been reached several days prior to the court's decision, as evidenced by the e-mail.

The defendant claimed the agreement was not actionable until the official documents were suitably signed and returned. The court disagreed, concluding it was clear from the contents of the e-mail and the follow-up documents referencing that e-mail that an agreement was reached.

Sgroi pointed out that the close of the letter reinforced this finding because it clearly indicated the author of the e-mail "purposefully added her name to this particular e-mail message, rather than a situation where the sender's e-mail software has been programmed to automatically generate the name of the e-mail sender, along with other identifying information, every time an e-mail message is sent."

Food for thought when composing that next business e-mail message.

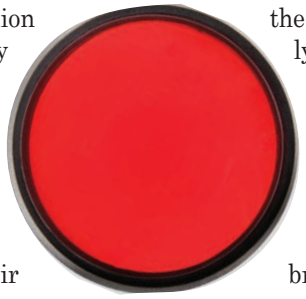
CYBERSECURITY

Cybersecurity: The Gap Between Fear and Action

An amazing 97% of businesses with annual security budgets totaling more than $1 million are concerned they are vulnerable to targeted malware attacks and other sophisticated cyber-crime and cyber-espionage tactics. Their level of concern was revealed in a survey of 200 C-level executives at U.S.-based companies conducted by Opinion Matters, on behalf of ThreatTrack Security. The survey further reported that 33% of the companies — including roughly half of all financial services firms and manufacturing companies that participated — have experienced a targeted cyber attack.

Unfortunately, these executives' fears have not necessarily translated into taking protective action. For example, 42% said they do not have an incident response team in place, and 47% said they are not using advanced malware analysis tools. Most (82 %) financial services firms are concerned about sophisticated attacks to their networks, but only half of them use an advanced malware analysis tool, like a sandbox.

Consumers share some of these basic fears. A companion survey reported that 75% of consumers are concerned about the security of their personally identifiable information. And for good reason, since nearly half (47%) of them said they had been notified at some point that their information had been compromised by a breach.

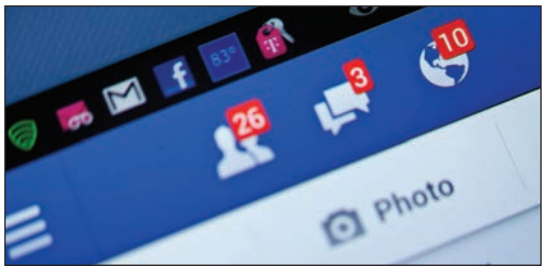


PRIVACY

Student Safety or Privacy Invasion?

A school district in Southern California is monitoring students' posts on social media sites in an effort to stop cyber-bullying and other teenage issues, according to a recent article in the *Los Angeles Times*. Glendale Unified School District reportedly hired Geo Listening in 2012 to track posts by its estimated 14,000 middle school and high school students after two teenagers committed suicide.

The school district has restricted the monitoring to publicly available pages. Further, the district did not supply Geo Listening a list of current accounts. Instead the company uses "deductive reasoning" to link public accounts to students, according to Chris Frydrych, founder and chief executive of Geo Listening. (He declined to elaborate when asked what constituted "deductive reasoning.")



Response to the program on and off campus has been mixed. Many believe that it and other efforts like it walk a fine line between balancing safe and supportive schools with student privacy and free speech. But the Glendale District program "is sweeping and far afield of what is necessary to ensure student safety and intrudes deeply into students' privacy and conduct outside of school," contends Brendan Hamme, an attorney with the American Civil Liberties Union of Southern California.

PRIVACY

Another State Increases Social Media Privacy Protection

Washington is the latest state to pass legislation banning employers from requesting employees' user names and passwords for their personal social media accounts. According to *Corporate Counsel*, the new law also prohibits employers from requiring their employees to:

- Open their accounts so the employers can view their postings
- Add them as friends
- Change their personal settings to make their accounts more public

If the employer is investigating a worker's alleged misconduct or if a worker is accused of making unauthorized transfers of proprietary information, the employer can ask the worker to voluntarily provide his or her log-on information, but the employer cannot require it. The law does not apply to social media sites and platforms used primarily for work purposes.

Some employers contend they need access to their employees' personal social media accounts to protect proprietary information, to meet federal financial regulations, and to minimize legal risk. Lawmakers are siding with the opposition, which calls such attempts an invasion of employees' privacy.

The National Conference of State Legislatures reports that since 2012, the following states have passed such laws: Arkansas, California, Colorado, Delaware, Illinois, Maryland, Michigan, Nevada, New Jersey, New Mexico, Oregon, Utah, Vermont, and now Washington. Legislation has been introduced or is pending in the remaining 36 states. Some states have similar laws protecting students at U.S. colleges and universities.

HR

UnitedHealth Recalls EHR Software

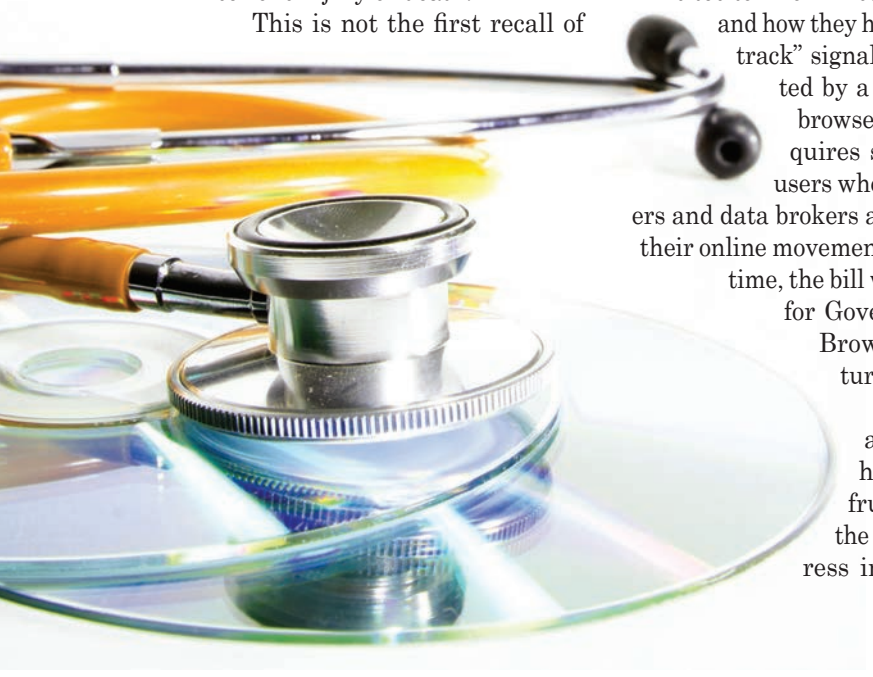
One of the clear advantages of electronic health records (EHRs) is they help to eliminate some common medical mistakes. For example, a study published in the June 2013 *Journal of the American Medical Informatics Association* reported that more than 17 million medication mistakes are avoided in the United States each year because hospitals are using computerized systems for ordering prescription drugs, thereby reducing the risks resulting from sloppy handwriting and dangerous drug combinations.

But what if an error is caused by a software glitch?

The UnitedHealth Group Inc. recently recalled software used in hospital emergency departments in more than 20 states because certain versions failed to print information about medications and failed to add data to patients' charts. Such notes typically contain directions about diet and use; failure to include them could lead to serious injury or death.

This is not the first recall of Picis software (the software manufacturer purchased by UnitedHealth Group in 2010), according to Bloomberg. A database maintained by the Food and Drug Administration (FDA) recorded six recalls since 2009. Unlike medical device manufacturers, makers of EHR software are not required to report safety issues to the FDA.

"It's admirable that the vendor reported this," said Ross Koppel, adjunct professor of sociology and medicine at the University of Pennsylvania, "but realize that this is one of the more obvious errors. Most are not as obvious and go unreported." He explained that some companies require hospitals to sign non-disclosure agreements, and practitioners are often unaware of the technology's role in errors.



PRIVACY

California Sets Pace on 'Do Not Track' Regs

Many privacy advocates are looking to California to blaze the trail for a national Do Not Track law. The state's Online Tracking Act requires websites to inform users whether and how they honor "do not track" signals transmitted by a consumer's browser. It also requires sites to tell users when advertisers and data brokers are tracking their online movements. At press time, the bill was waiting for Governor Jerry Brown's signature.

Privacy advocates have been frustrated by the lack of progress in Congress and the World Wide Web Consortium (W3C) on standards for online tracking and hope the California bill will stir the pot.

"I'm hoping the California bill will set off a digital data stampede for other states to begin regulating privacy," Jeff Chester, executive director for the Center for Digital Democracy and a member of the W3C Tracking Protection Group, recently told *Politico*. "It's not clear there is going to be a standard for Do Not Track from the W3C. It's likely to be a very weak standard."

The technology industry has mixed feelings about the legislation. Michael Beckerman, president of the Internet Association (whose members include Google and Facebook), stated: "The Internet is an area that is evolving every day. The users should have the power of choice here, not government regulations. California should not start the precedent of states or even the federal government regulating this since it's about the relationship between users and Internet companies."

According to the *Politico* article, the trade group TechAmerica initially opposed the bill for "trying to codify a definition of online tracking and lacking nuanced options for firms to describe how they respond to 'do not track' signals." The group dropped its opposition and adopted a neutral stance toward the amended version that passed the state legislature.

It remains to be seen whether the U.S. Congress or W3C will make headway on more far-reaching standards before the end of the year.

EHR

Wyndham Stands Up to the FTC

Hotel operator Wyndham Worldwide Corp. is fighting back in a data breach lawsuit filed in June 2012 by the Federal Trade Commission (FTC) against the company and three of its subsidiaries.

The lawsuit alleges that Wyndham failed to implement reasonable information security measures

and consequently experienced three major data breaches in two years. Hundreds of thousands of credit and debit cards were ultimately compromised, and there were fraud losses of more than $10.6 million.

The FTC accused the hotel operator of unfair trade practices and of deceiving customers into thinking their cardholder data was adequately protected when it wasn't. Other companies facing similar charges have opted to settle with the FTC, accepting fines as high as $10 million (as in the case of ChoicePoint) and comprehensive bi-annual audits.

Wyndham has questioned the FTC's authority to sue companies on behalf of consumers for cybersecurity breaches and lax or misleading data security policies. The U.S. Chamber of Commerce and several other organizations joined the battle by seeking permission to file for a dismissal, accusing the FTC of holding breached entities like Wyndham to unfair and arbitrary standards. *ComputerWorld* reported the groups also alleged that the FTC is forcing businesses into lengthy data breach settlements and imposing costly fines for violating security standards the agency hasn't formally promulgated.

A federal court judge in New Jersey agreed to allow the groups to file for the dismissal.

The Wyndham lawsuit is considered a landmark case because it's the first time the FTC has had to go to a federal court because a breached entity refused to settle.

The Chamber of Commerce *et al.* contend the agency routinely punishes businesses for failing to have reasonable security standards, yet it has never specified what constitutes reasonable standards. And because previous cases have been settled out of court, there has been no clear precedent for courts and legal counsels to reference.

There is also the question of whether Congress intended the FTC to actually regulate data security. Chris Hoofnagle, director of information privacy programs at the University of California Berkeley Center for Law & Technology, filed an amicus brief supporting the FTC, noting the agency's enforcement actions have been the only effective means of holding companies accountable for failing to protect consumers' data.

"Congress, in creating the FTC and in empowering it to police unfair and deceptive trade practices, explicitly gave the agency power to determine what is unfair and deceptive," he told *ComputerWorld*.

Security consultant Paul Rozenweig, founder of Red Branch Law & Consulting, believes a Wyndham victory would disable the FTC to broadly enforce cybersecurity standards.

EHR

NIST Solicits Feedback on Cybersecurity Framework Draft

In accordance with an executive order issued by President Barack Obama in February, the National Institute of Standards and Technology (NIST) has been working diligently to develop a cybersecurity framework that will provide a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" to help organizations manage their cybersecurity risk.

The latest draft of the preliminary framework was discussed with industry representatives in a dedicated workshop in September. NIST was expected to release a full preliminary draft in October for public review, followed in February 2015 by the final 1.0 version.

The finished framework will guide organizations on managing cybersecurity risk in a manner similar to financial, safety, and operational risk. It will focus on supporting cybersecurity improvement using industry-known standards and best practices.

According to NIST, "The framework provides a common language and mechanism for organizations to: 1) describe current cybersecurity posture; 2) describe their target state for cybersecurity; 3) identify and prioritize opportunities for improvement within the context of risk management; 4) assess progress toward the target state; 5) foster communications among internal and external stakeholders." It is not intended to replace an existing business or cybersecurity risk management process and cybersecurity program. Instead it provides guidance for improving or for establishing a program, if necessary.

The framework, which closely resembles a maturity model, comprises three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profile.

The Framework Core contains cybersecurity activities and references that are common across critical infrastructure sectors. The core presents standards and best practices in a manner that allows for communication and risk management across the organization. The core consists of five functions — identify, protect, detect, respond, recover — that can provide a high-level, strategic view of an organization's management of cybersecurity risk.

Part two is the Framework Implementation Tiers, which demonstrate the implementation of the core functions and categories and indicate how cybersecurity risk is managed. These tiers range from "partial" (tier 0) to "adaptive" (tier 3), with each tier building on the previous one.

Finally, part three is the Framework Profile, which conveys how an organization manages cybersecurity risk in each of the core functions and categories by identifying the subcategories that are implemented or planned for implementation. Profiles are also used to identify appropriate goals for organizations.

The NIST proposal has been criticized for not providing "measurable cybersecurity assurance." Ralph Langner, a renowned Germany-based consultant on industry control systems (ICS) security, contended the "fundamental problem of the [framework as it is currently written] is that it is not a method that, if applied properly, would lead to predictable results."

According to *CSO*, Langner is not alone in this belief. Joe Weiss, managing partner of Applied Control Solutions, said the framework draft takes a "useless 'high-level approach' that favors self-regulation over mandates."

In response, NIST has said the early phases were intended to obtain feedback from the industry to help flesh out the framework. However, it likely will not become a prescriptive standard.

Information Governance have your head spinning?

ZASIO

RECORDS & DOCUMENT MANAGEMENT EXPERTS

Wrapping your head around all the issues surrounding information governance can be overwhelming.

The experts at Zasio provide the assurance you need. Zasio can help prioritize your objectives, develop your strategy, and implement the tools unique to your organization.

Call the experts at Zasio to discuss your Information Governance questions and challenges today.

800 513 1000 | www.zasio.com

Connect with us:

www.facebook.com/ZasioEnterprises

www.linkedin.com/company/zasio-enterprises-inc.

DATA SECURITY

Photocopiers Can Pose Data Security Risk

Time to trade in that photocopie? Be sure to wipe its memory first.

Affinity Health Plans recently settled a case filed by the U.S. Department of Health and Human Services (DHHS) and was fined for potential Health Information Portability and Accountability Act (HIPAA) privacy and security violations. Affinity agreed to pay $1.2 million in fines because it failed to clear the hard drive of one of its leased photocopiers, which was later purchased by CBS.

Affinity self-reported the breach after *CBS Evening News* advised it that the copier's hard drive contained confidential patient medical information. Upon researching the breach, Affinity estimated that as many as 344,000 patients may have been affected. And this wasn't the first photocopier Affinity had returned without erasing the hard drive.

The DHHS' investigation found that Affinity had not included photocopier hard drives in its definition of electronic protected health information in its risk assessment as required by the HIPAA Security Rule. It also determined Affinity had violated the HIPAA Privacy Rule by failing to implement policies and procedures to scrub internal hard drives before returning photocopiers to its office equipment vendors.

In addition to the $1.2 million settlement payment, Affinity was directed to make its best effort to track down and scrub all the hard drives on photocopiers it previously leased that are still in the leasing agent's possession.

PRIVACY

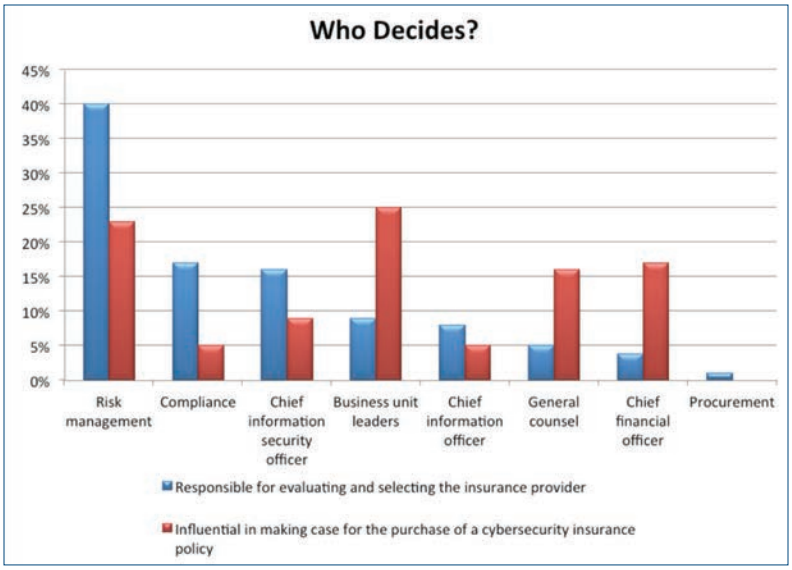
Tips for Complying with HIPAA Omnibus Rule

September 23 marked the compliance deadline for the Health Insurance Portability and Accountability Act (HIPAA) Omnibus Rule that makes business associates accountable for any misuse or failure to safeguard protected health information (PHI).

In a September press release, Karen Carnahan, president and COO of Cintas Document Management, said such HIPAA violations could result in penalties of up to $1.5 million each and that non-compliant companies "risk long-term damage to their reputation and brand."

To help achieve compliance under the Omnibus Rule, Cintas offers these tips:

1. Retrain employees on the updated policies and procedures addressing privacy, security, and PHI breaches.
2. Inventory vendors and look closely at their associates and subcontractors who handle PHI.
3. Update your business agreements. The Department of Health and Human Services has posted a sample version of a revised business associate agreement on its website.
4. Review internal policies and procedures to ensure they reflect the changes made to the HIPAA Privacy Rules. Revisions should reflect changes to the definition of PHI and to the rules governing patient access to records; disclosures to third parties; research; marketing; fundraising and the sale of PHI; notifications to those involved in a patient's care; and other rules governing decedents and immunizations.
5. Update breach policies and procedures.
6. Determine if notice is required for a breach. Under the Omnibus Rule, if there is a breach, it is presumed the covered entity or business associate must give notice unless it can demonstrate a low probability that PHI has been compromised or unless a regulatory exception applies.
7. Review breach notification procedures.
8. Encrypt or destroy PHI.
9. Review your Security Rule gap analysis to ensure it considers the changes made by the Omnibus Rule.
10. Update your HIPAA privacy notices to reflect the changes made by the Omnibus Rule.



Source: Ponemon Institute, 2013

CYBERSECURITY

Rising Data Breech Costs Drive Cybersecurity Insurance Sales

Increasing costs related to data breaches are prompting enterprises to purchase cybersecurity insurance. A new study from Ponemon Institute revealed that 31% of the respondents already have the specialized insurance while 57% of those without it plan to purchase a policy.

Most (70%) of the companies that have purchased a cybersecurity insurance policy have learned first-hand just how costly a breach can be. The respondents reported the average financial impact on companies suffering a breach was $9.4 million. The average potential risk of future incidents was estimated to be $163 million, due largely to the anticipated loss of confidential business information.

From a business perspective, 41% of the respondents consider cybersecurity risks to be greater than other insurable business risks such as natural disasters and business interruption. More than a third (35%) said cybersecurity risks are equal to other insurable business risks.

Many of the policies that have been issued cover expenses incurred during and after a breach. For example, 86% of the policies cover notification costs, 73% cover legal defense costs, 64% cover forensics and investigative costs, and 48% cover replacement of lost or damaged equipment. Fewer than one-third (30%) of the policies cover third-party liability.

Even though insured respondents felt the cost of the insurance was fair given the risk, high premiums were cited as the main reason others had not purchased a policy to date.

Policies typically cover the most common and costly incidents, including human error and negligence, external attacks by cyber criminals, system- or business-process failures, and malicious or criminal attacks from inside. Not surprisingly, the industry sectors with the highest insurance adoption rate were technology and software (41%)

E-MAIL

NARA Implements New Plan for Preserving E-mail

The National Archives and Records Administration (NARA) has offered federal agencies a new, more simplified and automated approach to managing e-mail: Capstone.

The Capstone approach allows an agency to categorize and schedule e-mail based on the work and/or position of the e-mail account owner. For example, the agency could determine that records from the accounts of officials at or near the top of an agency should be preserved as permanent. All other e-mail accounts would be considered temporary and preserved for a set period of time based on the agency's need.

Advantages of using the Capstone approach include:

- Reduced reliance on print-and-file, click-and-file, drag-and-drop, or other user-dependent policies
- Optimized access to records in response to discovery or Freedom of Information requests
- A practical approach to managing legacy e-mail accounts
- Reduced risk of unauthorized destruction of e-mail records
- Technologies are leveraged for other purposes (e.g., e-mail archives used for e-discovery)

Other considerations related to Capstone were contained in an August 29 bulletin from NARA.

PRIVACY

Privacy Groups Oppose Proposed Google Settlement, Facebook Policy Changes

A privacy advocates have asked a U.S. court to decline a proposed $8.5 million settlement with Google in a class action lawsuit over search privacy. Their primary point of contention: it does not require Google to change its business practices.

The lawsuit, filed in October 2010, stated that Google allegedly transmitted user search queries to third parties without users' knowledge or consent in order to increase ad revenue. The plaintiffs contended that when a user clicks a link from Google's search results page, the owner of the website would receive from Google the user's search terms, which could contain the user's real name, contact information, credit card numbers, and Social Security number. Those queries could also include highly personal and sensitive information such as confidential medical information, according to the complaint.

The $8.5 million settlement would not provide a monetary award to the individuals who were part of the class that filed suit, but would be used to pay settlement-related expenses, with the remainder going to organizations that would promote public awareness, research, development, and other initiatives related to protecting privacy on the Internet. At the time of filing, the proposed recipients included World Privacy Forum; Carnegie-Mellon; Chicago-Kent College of Law Center for Information, Society, and Policy; Berkman Center for Internet and Society at Harvard University; Stanford Center for Internet and Society; MacArthur Foundation; and AARP Inc.

In addition, the settlement required Google to notify users of its conduct so "users can make informed choices about whether and how to use Google Search." Google agreed to include the required disclosures on its FAQs webpage.

Privacy organizations, including the Electronic Privacy Information Center, Consumer Watchdog, Patient Privacy Rights, the Center for Digital Democracy, and the Privacy Rights Clearinghouse, contested the settlement, urging the presiding judge not to accept the proposed settlement. They criticized the agreement because it doesn't require Google to change its business practices and the proposed relief does not benefit the class members. Further, the group contended the entities that would receive the settlement funds were not, in fact, "aligned with interests of the purported class members."

Many of the aforementioned privacy organizations also weighed in on a similar matter involving Facebook. The groups petitioned the Federal Trade Commission (FTC) to stop Facebook from changing two of its governing policies, saying the changes compromise users' privacy.

PRIVACY

Student Safety or Privacy Invasion?

A school district in Southern California is monitoring students' posts on social media sites in an effort to stop cyber-bullying and other teenage issues, according to a recent article in the *Los Angeles Times*. Glendale Unified School District reportedly hired Geo Listening in 2012 to track posts by its estimated 14,000 middle school and high school students after two teenagers committed suicide.

The school district has restricted the monitoring to publicly available pages. Further, the district did not supply Geo Listening a list of current accounts. Instead the company uses "deductive reasoning" to link public accounts to students, according to Chris Frydrych, founder and chief executive of Geo Listening. (He declined to elaborate when asked what constituted "deductive reasoning.")

Response to the program on and off campus has been mixed. Many believe that it and other efforts like it walk a fine line between balancing safe and supportive schools with student privacy and free speech. But the Glendale District program "is sweeping and far afield of what is necessary to ensure student safety and intrudes deeply into students' privacy and conduct outside of school," contends Brendan Hamme, an attorney with the American Civil Liberties Union of Southern California.

E-DISCOVERY

Comments Sought on Proposed Amendments to FRCP

A draft of preliminary changes to the rules regarding electronic discovery in federal civil suits is now open for public comment. The proposed amendments to the Federal Rules of Civil Procedure (FRCP) were prepared by the Committee on Rules of Practice and Procedure of the U.S. Judicial Conference. Among other things, the changes address scheduling orders, scope of discovery, document production, and sanctions.

The importance and expectation of cooperation was established in the current rules. The proposed changes would facilitate and encourage that cooperation. For example, they would require that the parties meet face-to-face or by other means of direct, simultaneous communication and would allow them to schedule those conferences earlier. This would likely significantly increase the involvement of the courts early in cases, explained Bennett Borden and Amy Frenzen of Drinker Biddle & Reath LLP in a recent *Modaq* article.

A great deal of the discussions regarding the changes have centered on the duty to preserve, how and when it is triggered, and its scope. The new rules would strengthen the court's ability to limit discovery based on proportionality by moving this under the section about scope.

Bordon and Frenzen pointed out that this would also affect preservation, because "it would allow a party to make and defend preservation decisions based upon the proportional benefit of the information compared to the burden of preserving as well as producing it."

In addition, the new rules regarding discovery sanctions would add a layer of protection to preservation decisions. Sanctions would be imposed, in most situations, only if the party's failure to preserve or produce documents was "willful or in bad faith" and "caused substantial prejudice in the litigation."

This proposed amendment protects reasonable preservation and provides clearer guidance on which sanctions can be imposed, whereas the imposition of sanctions currently varies widely among circuits.

Public hearings have been held in Washington, D.C., Phoenix, and Dallas. Comments on the proposed changes may be submitted to *www.regulations.gov/#!docketDetail;D=USC-RULES-CV-2013-0002* until February 15, 2014. The target effective date for the final rules is December 15, 2015.

INFORMATION SECURITY

Survey: Industrial Firms Underestimate Their Data Risk

Manufacturing and distribution executives have become more aware of the risks associated with business information and data, especially as social media becomes more widespread. Yet more than two-thirds believe their data is at little or no risk, according to a research report from the consulting firm McGladrey. Given that their controls are often insufficient or ineffective, this raises the question of whether the executives fully understand their exposure.

Roughly 70% of small and midsize organizations said their data was at little or no risk, as did 56% of larger companies. Attackers, though, don't seem to care much about size.

"Financially motivated attackers will take any data they can find," wrote Corbin Del Carlo, McGladrey's director and regional leader of security and privacy services. "One company's Internet footprint looks the same as another to anyone interested in finding something of value, whether it's credit information, personnel information, intellectual property such as engineering drawings or processes, technology, or other industrial assets. Size does not matter; information does."

How one defines "at risk" may be telling. Some respondents told the surveyors they defined risk by whether "things are running." In other words, as long as their intranet and website were up, they were fine. Some admitted they were still running on technology from the 1980s and were reluctant to make the sizeable investment to bring them into the 21st century. Others were forced to make the investment because they had been breached.

McGladrey found that one of the best practices that thriving companies share is investing in new or upgraded information technology, allowing them to develop innovative products, decrease cycle time, and increase productivity. Investing in software can also give companies a competitive advantage by enabling executives to access corporate performance information they can translate into actionable plans. **END**

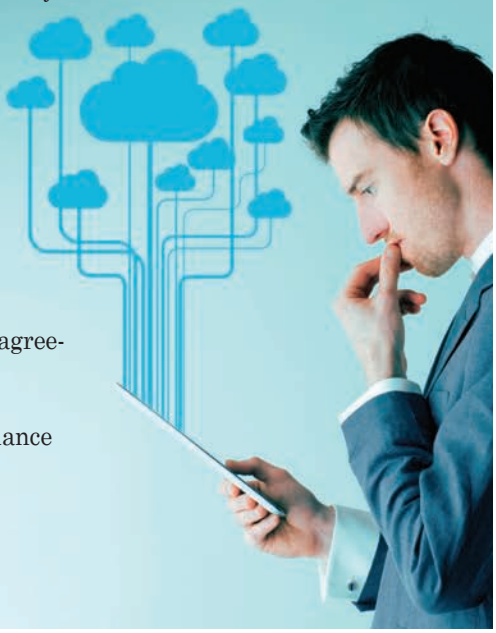
CLOUD

Data Security Top Concern for IT, Business Execs

For the past 50 years, through its National Historical Publications anResults of Saugatuck Technology's "2013 Cloud Survey" of 218 IT and business executives across organizations of all sizes revealed that data protection and security is their top concern related to using cloud-based services. This is consistent with the survey results for most of the past seven years.

Here are the top 11 cloud concerns, according to the survey:

1. Data security/privacy
2. Data/transaction integrity
3. Regulatory compliance
4. Integrating cloud-based data or workflow with existing enterprise applications
5. Cloud provider transparency (e.g., uptime, service level agreements, computer resource location)
6. Ability to customize cloud solutions
7. Dependable delivery of required high availability/performance
8. Viability cloud providers
9. Return on investment for cloud not yet verified
10. Provider lock-in
11. Cross-border data restrictions



CYBERSECURITY

Cybersecurity – An IT Issue or Compliance Issue?

Increasingly, cyber attacks on financial institutions are focusing on interrupting service to users. Consequently, distributed denial of service (DDoS) attacks have become a notable headache for many financial institutions. They are also a reminder of looming responsibility for the organizations' compliance departments, wrote Compliance Complete's Emmanuel Olaoye in a recent Reuters article.

DDoS attacks have become so problematic that the Depository Trust Clearing Corp. (DTCC) considers them one of the three types of attacks that pose a systemic risk to the financial system. (DTCC settles the majority of securities transactions in the United States.) Because regulators are asking more questions about security for such attacks, some contend cybersecurity is becoming a compliance issue. As such, compliance departments may need to become more involved instead of relegating the issue to IT.

Science Applications International Corporation's chief cybersecurity technologist, Gib Sorebo, advises compliance professionals to speak to their IT or information security colleagues when a regulation is introduced so they know whether the organization has the technical capability to comply with the rule.

"The first conversation is understanding what the firm needs when compliance requirements come down," said Sorebo. "It is a lot easier if you have that conversation first about what is doable and not doable."

The role of compliance in cybersecurity likely will continue to change as regulators increase their focus on security. Sorebo predicts compliance departments will need a more extensive cybersecurity program instead of one that is more narrowly focused on protecting customer information. "The compliance officer is going to have to define the overall compliance ecosystem he or she has to have to operate in," he said. "They must certainly be prepared to address, at a minimum, how they are addressing all those compliance obligations." **END**

Retiring Legacy IT Systems Under the IG Umbrella

John T. Phillips, CRM, CDIA, FAI

When an information system is decommissioned, its data must remain usable – either in that system or in a new one to which the data is migrated – to meet retention requirements, as well as potential litigation or regulatory demands. This requires extensive, collaborative planning to ensure backwards compatibility of systems, software, and data formats.

The information technologies that enhance our daily lives – from those that drive the business processes we count on for our livelihoods to those we use for personal enjoyment – depend on hardware and software that have a life cycle.

In business, that life cycle often is extended through upgrades and enhancements, and when there is no funding for new application development, these systems often continue in use beyond what should be the ideal end of their life cycle. Because they represent "the way we've always done the work," they are referred to as *legacy* systems. They can still get the job done, but they are like dinosaurs approaching extinction.

Eventually, though, organizations realize that their legacy systems need to be superseded by more advanced and cost-effective technologies. This signals the end of their life cycle, and they are decommissioned, or retired.

It's likely that a system's legacy data will still be subject to records retention or other requirements. That is why effective information governance (IG) demands continuity of electronic records not only throughout the life cycle of the systems that contain them, but also after those systems are decommissioned.

Collaborating on System Changes

Information technology (IT) personnel have considerable incentive to support business processes with the latest computer technologies. Technical updates enhance user contentment, systems performance, and ease of maintenance over the long run.

This perspective also has special implications for decommissioning systems. When electronic records are archived, they must remain usable, and successful data migration and use of archived records depend on extensive planning to ensure backwards compatibility of systems, software, and data formats.

For that reason, when IT and users both participate in strategic planning for IT infrastructure standards, an important topic should be the long-term viability of electronic records and data. Collaboration is imperative to determining what data formats are the best choices for current and future use.

Leveraging Users' Expertise

A distinction must be made between decommissioning a system because it is no longer viable and decommissioning one because new technology can better handle that system's mission-related activities.

One of the ironies in today's business setting is that even though management typically delegates oversight of IT functions and operations to IT personnel, system users are the real experts in how well a system is working. This is because the heart of an IT system comprises the raw data and electronic records it produces and manages rather than the operational speed of its processors, disk drives, and networks.

If the electronic records and system reports are not working correctly, the users will know first. For this reason, IT system users should participate in system planning sessions and must pay close attention to a system's changes to ensure that it continues to meet workflow and data quality expectations.

Generally, as long as system users can get their daily work done, they are not concerned about infrastructure improvements, and they won't likely ask for more sophisticated solutions or for a system to be decommissioned. The quality of technology system operations is of more interest to IT personnel, as they must perform daily maintenance, upgrade software, patch "bugs," monitor security, and intervene in cases of hardware failure.

IT is far more likely than users to know ahead of time about technology advancements that will call for the organization to consider decommissioning a particular system. Once they know, though, users should also participate in planning for decommissioning a system.

Preserving Data

Decommissioning or just shutting down most computer systems usually involves some form of preservation or data migration, making the data's format and the media upon which it is recorded critical for its viability and utility.

Archiving Data, Technology

Decommissioning a legacy system could entail archiving the system's technology assets and data to ensure its complete protection. Or, it could mean just shutting down the system without taking any precautions under the assumption that the replacement system will assume all previous workflow and data management functions.

Although the complete shutdown – rather than the replacement – of a computer system is rare, it may occur when an organization or one of its functions ceases. For

example, if a research project ends, a government agency closes, or a business declares bankruptcy and ceases to exist, there may no longer be a need for a technology system or the electronic records it contains.

However, if the research information could be used for other projects, or the government records are subject to retention rules, or the business is involved in litigation that requires the resolution of debts, the information in a decommissioned system should be preserved.

... after migrating legacy data, an organization also might choose to preserve the original records in the decommissioned system ...

Migrating Data

In most cases the legacy system's data must be migrated into the new system to ensure new software application viability or to meet regulatory, legal, archival, or other records preservation requirements.

Government agencies may need to maintain public records for many years, or even permanently. Many of those agencies have issued extensive references to how agency systems are to be decommissioned.

For example, the Department of the Interior, Bureau of Land Management published *Information System Decommissioning Guide*, available at *http://tinyurl.com/kdd7x87*. The National Archives and Records Administration's (NARA) "Systems Development Life Cycle Checklists" provides a standardized process for all phases of system development, including decommissioning. See the checklist for that phase in Figure 1 on page 24. The full document is available at *www.archives.gov/records-mgmt/initiatives/sdlc-checklist.pdf*.

It is difficult to predict when records may be needed to support information-gathering activities. Audits can be originated by external organizations. Lawsuits can be filed by unforeseen plaintiffs with surprising claims. Disasters may demand that old data be used to reconstruct computer systems when no instances of an application survived a hurricane or tornado.

For these reasons, after migrating legacy data, an organization also might choose to preserve the original records in the decommissioned system, as it can be useful for demonstrating adherence to archival preservation mandates, achieving disaster recovery goals, or protecting the organization in e-discovery or regulatory investigations.

Choosing Storage Media

Media selected for storing decommissioned system data must be readable by computers from encoded solid state chips, tape, or disk drives. Compact disk – read only memory (CD-ROM), once the standard for long-term personal computer data storage, has given way to digital video disk (DVD), digital tape, optical tape, universal serial bus (USB) drives, and solid state multimedia cards (MMC) or secure digital (SD) devices that use "flash memory" to record data for offline use.

There is valuable debate and guidance from many informed professionals about the best method for long-term storage of data, especially from government sources, that should be considered when planning for a system shut down. For instance, NARA offers brochures providing "Tips for Scheduling Potentially Permanent Electronic Records," including e-mail, scanned images, and PDFs. Visit *www.archives.gov/publications/records-mgmt.html* to find direct links to PDF formats of these brochures.

Choosing the System Environment

In general, when creating a strategy for long-term data storage, consider the:

- Potential use environment for the data and electronic records
- Technology infrastructure of the environment where raw data might need to be loaded
- Operating system and application software environment:
  - A proprietary system (e.g. from Microsoft, Apple, IBM, Oracle, and others)
  - An open system (e.g., Linux operating system, C++, hypertext markup language (HTML), eXtensible markup language (XML), and other less vendor-dominated tools)

The potential use environment is the most important factor, and each decommissioning case will be different. For example, if the potential users of the electronic records are U.S.-based attorneys in e-discovery meetings, using Microsoft Windows operating system and application software and storing files in native formats with some rendered to Adobe Acrobat PDF, would probably work well, as this is the predominant document management environment for that group.

Planning for Software Obsolescence

Because software changes more often than hardware or data formats, it requires the most advanced planning. Organizations generally upgrade software on most machines every year, while their operating systems might receive just a few bug patches during that period.

Some software upgrades don't cause compatibility problems. Different versions of Microsoft Word, for instance, may be upgraded on the same computer with little or no

Compliance monitoring is just a click away

Data protection regulations require organizations to monitor the qualifications and compliance of service providers that process sensitive information.

NAID just made this a lot easier!

Select the "**NAID AAA Notification**" link in NAID's member directory to receive emails announcing status changes to that member's certification and compliance qualifications.

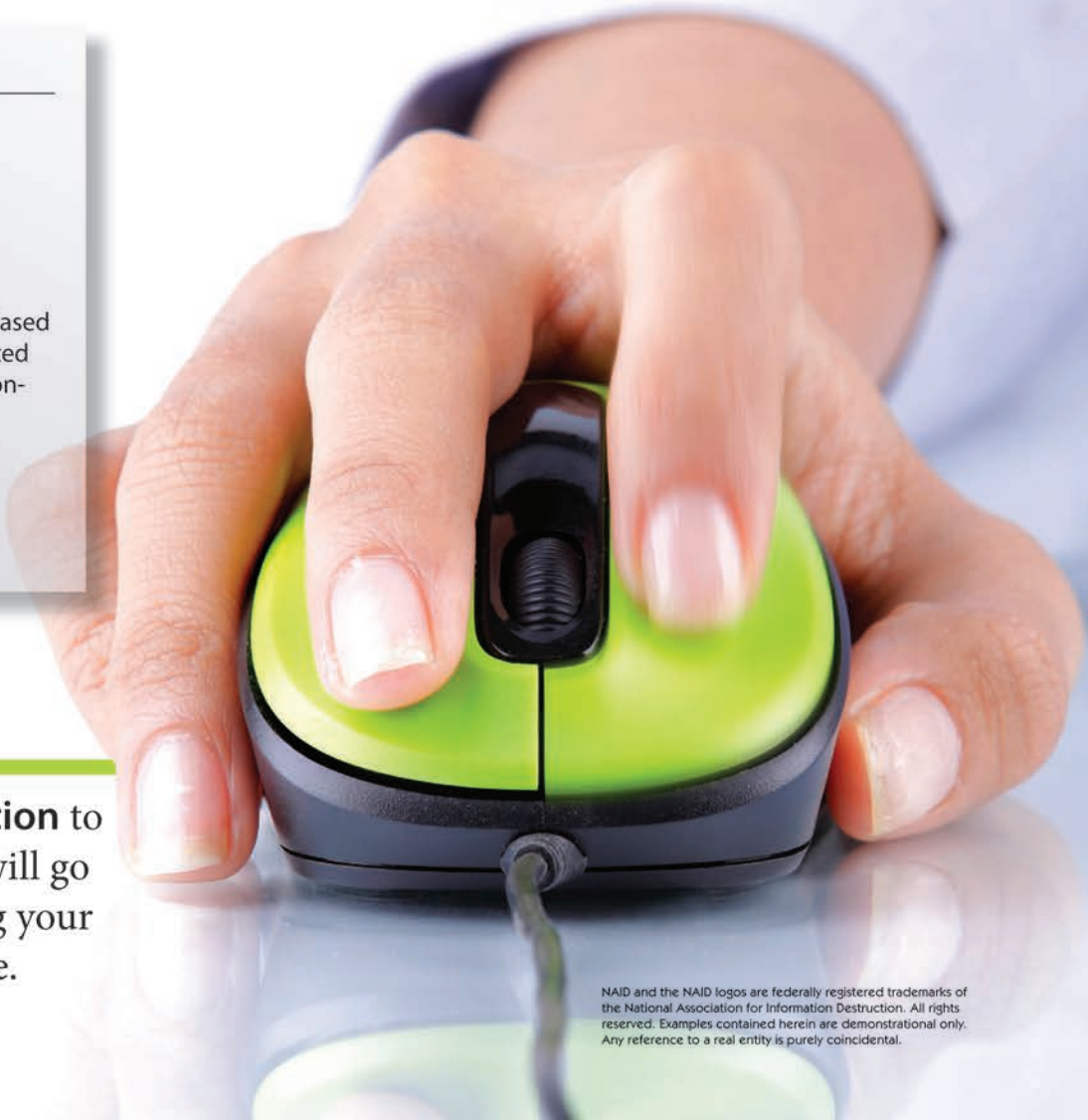
Data Destruction Co.

John Smith
123 S. 1st Ave.
Smalltown, AZ 85011
234-567-8901
www.123destruction.com

NAID CERTIFIED: Mobile and Plant-Based Operations Endorsed for Paper/Printed Media, Computer Hard Drive and Non-Paper Media Destruction

Original Date: January 16, 2008
Expiration Date: August 31, 2014

NAID AAA Notification



Visit **bit.ly/AAAnotification** to sign up. This simple act will go a long way in establishing your organization's compliance.

changes in data formats. This kind of technology transitioning on existing computers increases functionality to manage more complex records, but it does not create backwards compatibility problems that would occur if the new software recognized only its new data format.

Choosing Data Formats

Changing business models create a need for innovative records and associated workflow processes. Fortunately, data formats like HTML, XML, and PDF are all used widely in many software application environments (and are not exclusively software vendor-driven), thus creating an inherent content longevity for any information stored in these formats.

A complicating factor for many organizations is their reliance on vendor software that creates proprietary data formats. There are few data file formats independent in design, though, as many vendors participate in setting standards for software and then try to make their own file formats compatible.

For example, although the PDF file format is often referred to as a *de facto industry standard*, the internal code for creating these files, which was licensed to Adobe until July 2008, was subsequently released as a royalty-free, open standard published by the International Organization for Standardization (ISO) as ISO 32000-1:2008 *Document management – Portable document format – Part 1: PDF 1.7*.

Integrating Records Management into the Systems Development Life Cycle

Phase 9. Retirement and Rollover

1. At the time of retirement or rollover of the system, are records preserved, retained, and fully accessible for the full retentions in accordance with appropriate dispositions?
2. At the time of retirement or rollover of the system, are temporary records destroyed in accordance with appropriate dispositions?
3. At the time of retirement or rollover of the system, are permanent records transferred to NARA in accordance with the appropriate dispositions?

Figure 1: "Integrating RM into the SDLC" **Source:** National Archives and Records Administration "Systems Development Life Cycle Checklists."

Organizations must ensure there will be no long-term issues with file formats used to store decommissioned electronic records. Although most vendors offer several file formats in which their applications can store data, some options may not be in compliance with regulatory guidelines or litigation readiness demands. In fact, deploying most open systems software solutions also promotes a dependence on open systems software maintenance services, which may have limited options. Planning ahead for future access requirements is the key.

Recreating Software Applications

Recreating actual software applications in order to view records is costly and time consuming. So, organizations might elect to preserve the original application software in case it is needed to generate accurate records.

Planning for E-Discovery Challenges

E-discovery presents special challenges related to decommissioning systems, preserving their legacy data over time, and producing it as authentic, credible evidence for litigation- or regulatory-related purposes.

Data maps, which describe the locations and nature of electronic records, are of considerable value when stored information must be located, held, and produced. To ensure their value, successive data maps should be linked in a manner that allows systems migrations or transformations to be understood.

Using these tools will enhance the organization's ability to implement credible legal holds, minimize the cost of its discovery, and improve the utility of the information. They will be especially useful if a large amount of information must be shared during "meet and confer" sessions, during which judges expect attorneys to resolve e-discovery issues before litigation in court begins.

Maintaining Credibility

Once a hold is issued, records subject to the hold must be preserved within their existing computer system or by migration into a records hold repository. Maintaining these records within an existing system can become a problem if that system needs software upgrades that save old records in newer data formats, as this potentially impacts their evidentiary credibility.

Older documents saved in new data formats may not exhibit the same look and feel of the original records. Newer software may not recognize certain fonts or graphics that were generated in older applications. Sometimes the only way to ensure that electronic documents can be properly displayed and printed is to test each document during a system migration, which is a costly and time-consuming process. This can be made less onerous by testing randomly chosen sets of data instead.

Complying with Retention

Outsourcing the retention of electronic records to e-discovery software vendors may present another danger; they may not know that those records are subject to retention rules that exceed immediate needs for records holds. One can only assume that e-discovery vendors are responsible for the retention periods spelled out in their contracts.

Decommissioning Under the IG Umbrella

When organizations design and implement IG programs, they must address the complete life cycle of in-

formation – from creation to disposition. That includes information in operational systems, in system backups, and in specialized data archiving repositories.

Once an IT system has been identified as having reached the end of its lifecycle, appropriate staff and budget resources must be available to plan and perform decommissioning activities, beginning with data migration, if needed, and ending with the post-decommission review.

Organizations may find that planning for de-commissioning coincides well with implementing disaster protection programs or performing records cleanup and destruction activities; these actions typically direct the responsible destruction of electronic records and involve people who know how to address data security, privacy, and other information risks.

Because the goal of IG programs is to encompass all electronic records repositories and data archives, they must address the offline data and software archives that decommissioning of systems creates.

IG programs must inherently incorporate strategic planning for evolving technologies. Standardization of supported data formats, applications software, and operating systems is an important component of IG tactical initiatives. E-discovery issues, including authenticity of data and chain of custody documentation, that enhance the credibility of evidence can be addressed early in the life cycle of information by ensuring that any system proposed for decommissioning is managed thoroughly under the umbrella of a properly managed IG program. **END**

John T. Phillips, CRM, CDIA, FAI, can be contacted at john@infotechdecisions.com. *See his bio on page 47.*

How to Develop a PCI Compliance Program

And Take a Step on the IG Career Path

Andrew Altepeter

Any organization that processes customer payment cards must comply with the Payment Card Industry's Data Security Standard or face possible fines and a great potential for this sensitive information to be compromised. Leading the PCI compliance program's development is a prudent way for a RIM professional to raise awareness of information governance (IG) priorities and, perhaps, take a step toward a broader IG career.

Information governance (IG) and records and information management (RIM) professionals will readily agree that protecting sensitive information is a top job priority and that it has become more difficult and risky because of the explosion of electronic information. Its importance has been underscored by privacy legislation, such as the Fair and Accurate Credit Transactions Act (FACTA), the Health Insurance Portability and Accountability Act (HIPAA), and European Union privacy directives.

As seen by the constant media stories about data breaches and their negative impact on even the most established and respected merchants, handling sensitive information properly is necessary not only to meet business and customer needs, but to prevent severe business disruptions, damaged customer relations, and negative public perceptions that can occur when it is compromised.

ARMA International recognized this important priority in creating the Principle of Protection as one of its eight Generally Accepted Recordkeeping Principles® (Principles). It codified this principle as the need to "ensure a reasonable level of protection for records and information that are private, confidential, privileged, secret, classified, or essential to business continuity."

This emphasizes the imperative for RIM professionals to be involved in the creation and maintenance of policies, processes, and procedures that protect sensitive information. As a bonus, building a compliance program of this type provides an opportunity to expand their skills beyond traditional RIM roles and advance along an IG career path.

PCI DSS: Mitigating the Risk

For organizations that process customer payment cards (either debit or credit), this is one of their most critical types of information to protect, and the risks surrounding it have grown steadily over the last few decades because of the growing use of e-commerce and volume of electronic payment processing.

In 2003, the U.S government responded by passing FACTA, which includes requirements for free annual credit reports, fraud alerts, truncation of payment card numbers, and certain protections for victims of identity theft. However, it lacks specific measures for organizations to strengthen security and prevent breaches.

In 2006, the major payment card companies (Visa, MasterCard, American Express, Discover, and JCB, which is a Japan-based payment card allied with Discover in the United States) formed the Payment Card Industry Security Standards Council (PCI SSC), with requirements for *merchants* – which it defines as "any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC."

The primary objective of this organization has been the production and maintenance of the Payment Card Industry Data Security Standard (PCI DSS), which has given all merchants who process payment cards common controls to help reduce exposure to fraud. There are six goals, which are further broken down into 12 requirements as shown in Table One below.

A cursory look at the requirements demonstrates the interdisciplinary approach organizations must take to reach PCI compliance. Input will be needed from finance, IT, information security, and information governance teams. Executive sponsorship is re-

Payment Card Industry Data Security Standard

Goals	Requirements
Build and maintain a secure network.	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system pass.
Protect cardholder data.	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.
Maintain a vulnerability management program.	5. Use and regularly update anti-virus software or programs. 6. Develop and maintain secure systems and applications.
Implement strong access control measures.	7. Restrict access to cardholder data by business need-to-know. 8. Assign a unique ID to each person with computer access. 9. Restrict physical access to cardholder data.
Regularly monitor and test networks.	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an information security policy.	12. Maintain a policy that addresses information security for employees and contractors.

Table 1: PCI Requirements

quired, especially from finance and the business units processing payment cards.

Complying with PCI DSS should be a top priority for all merchants, as failure to comply could result in fines from the payment card companies and banks. In addition, states such as Minnesota, Nevada, and Washington have passed laws that require all merchants who do business in their state to be PCI compliant.

Developing a PCI Compliance Program

While achieving compliance may seem a tall task, IG professionals should view this challenge as an opportunity: implementing a PCI program gives them an excellent opportunity to expand the scope of their job duties, provide meaningful value to the business, and increase their visibility. Here are some steps to getting started:

1. Build Expertise

The PCI DSS makes all of its resources for its requirements and standards available at *www.pcisecuritystandards.org*. Take some time to read through the requirements, documentation, and available training. Enroll in PCI awareness training or Payment Card Information Professional credential training, both available through the PCI Security Standards website.

2. Form a Team

Running a successful PCI compliance program requires a multidisciplinary team, including people from the following departments.

Finance. The team will need executive sponsorship from finance, as a CFO or equivalent executive officer will need to sign an Attestation of Compliance for the organization's receiving bank. Finance should also assist in creating training and operating procedures for employees processing credit cards.

IT. Someone will need to be able to speak to the organization's network architecture, firewalls, antivirus software, and desktop image. In addition, new software may need to be purchased, and IT policies may need to be updated.

Information Security, Legal, or Privacy. Some assistance from legal or data privacy may be needed, and depending on their place within IT, additional representatives from information security may be needed. Relevant policies should be updated, and these resources may be required to implement some of the PCI requirements.

Internal Audit. While optional, leveraging internal audit resources to effectively monitor and enforce PCI controls reduces the burden on RIM and gives the compliance program added enforcement.

Records and Information Management. See the section "RIM Professional Roles" toward the end of this article.

3. Scope the Cardholder Environment

Work with team members to determine the scope of the card environment. This includes anywhere within the organization's infrastructure that payment card data is stored or transmitted. Payment card data includes the primary account number, cardholder name, service code, expiration data, full magnetic stripe data, three-digit code on the back of the card, and PIN.

The scope may include both electronic and paper information, computers, networks, and finance applications. Completing a network diagram, one of the PCI requirements, will be

helpful in determining scope. Make sure to have an updated roster of anyone who comes in contact with payment card information. Find out from finance the annual number of payment card transactions and how many dollars the organization processes.

4. Determine Requirements

While PCI DSS applies to all organizations that take payment cards, requirements are applied differently, depending on the type of merchant. These levels are determined by the merchant's annual number of payment card transactions. Each payment card company defines its merchant levels slightly differently. For example, Table 2 shows the merchant levels Visa defines.

Merchant Level	Annual Number of Transactions
Level 1 Merchant	6 million or more
Level 2 Merchant	Between 1 million and 6 million
Level 3 Merchant	Between 20,000 and 1 million
Level 4 Merchant	Less than 20,000

Table 2: VISA Merchant Levels

An organization's compliance is tracked by its acquiring bank, which is the financial institution that processes credit and debit card payments for products and services. Major banks have teams that are happy to assist merchants with PCI compliance. They can be contacted through the bank's merchant services division.

An organization's level has a significant impact on what compliance activities it is required to complete. For example, large merchants are required to have either a qualified security assessor or internal security assessor evaluate their environment for PCI compliance, and they must have quarterly vulnerability scans by an approved scanning vendor.

Smaller merchants are able to complete a self-assessment questionnaire (SAQ) and submit it to their acquiring bank. There are also several variations of SAQ; the one that is most appropriate for the methods the organization uses to process payment card information should be chosen. PCI SSC recognizes that the requirements may seem overwhelming to small businesses. See *www.pcisecuritystandards.org/smb/* for a helpful guide for helping small merchants comply with the requirements.

5. Work to Reduce Scope

Certain steps make complying with PCI DSS much easier. Using firewall software, segment the card environment from the rest of the network. Do not store payment card data within the organization's environment. Outsource card processing to a payment application that has been validated by a Payment Application Qualified Security Assessor. (See a list of validated payment applications at *www.pcisecuritystandards.org/approved_companies_providers/*.)

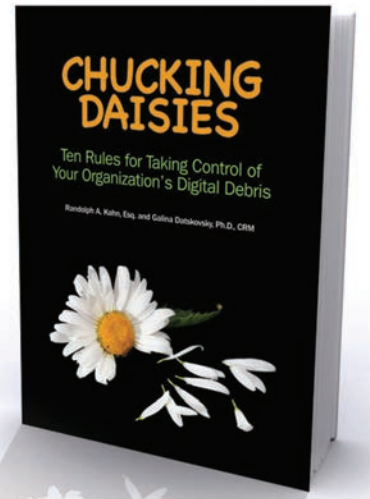
If possible, use *tokenization* – which replaces payment card data with a numeric signifier – to completely eliminate all payment card information from applications. The payment card information is stored with a PCI-compliant provider, with only the token visible to the merchant. Many validated payment vendors offer this service.

6. Establish and Maintain Compliance

It may take time to implement a PCI compliance program. A seasoned project manager may be needed to bring together team members from disparate departments. But do not lose heart: once established, the organization will be more secure, avoiding embarrassing breaches and loss of customer trust.

Reaching compliance is not the end of the road, though; remaining compliant requires an ongoing effort. Employees must continually be

New!



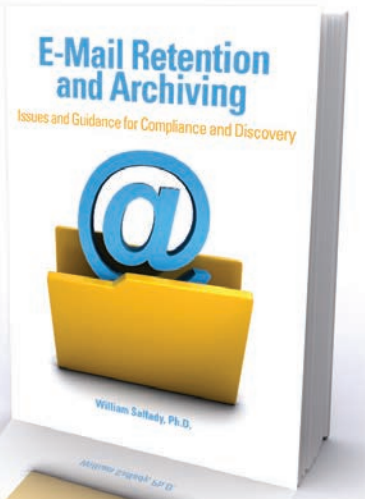
Chucking Daisies

Ten Rules for Taking Control of Your Organization's Digital Debris

Randolph A. Kahn, Esq. and
Galina Datskovsky, Ph.D., CRM

The life cycle of information can be compared to that of a bunch of daisies – valuable in the beginning, but eventually reduced to a smelly mess that needs to be thrown out. If the challenge of dealing with your information ROT – redundant, outdated, and trivial – seems insurmountable, you will find the help you need in *Chucking Daises: Ten Rules for Taking Control of Your Organization's Digital Debris.*

Regular Price: **$25.00**
For Members: **$20.00**



E-Mail Retention and Archiving

Issues and Guidance for Compliance and Discovery

William Saffady, Ph.D.

E-mail likely represents a significant portion of you organization's information. With a focus on the retention of e-mail to satisfy your organization's legal, operational, and historical requirements, *E-Mail Retention and Archiving: Issues and Guidance for Compliance and Discovery* will help you avoid the problems associated with over-retaining e-mail – as well as simplify the discovery process.

Regular Price: **$55.00**
For Members: **$35.00**

Free Shipping Until January 31!

UPS Ground Courtesy of **RSD**. See website for complete details.

ARMA INTERNATIONAL BOOKSTORE
www.arma.org/bookstore

trained and the environment must stay compliant through hardware and software upgrades. The organization must certify compliance annually, and many requirements must be satisfied on quarterly or biannual cycles.

And let's not forget: business happens, and that means ever-changing scope, hardware, and software. Make sure all members of the PCI team continue to meet monthly or quarterly to track the scope and compliance of the entire environment.

The RIM Professional's Role

Even if they do not become PCI compliance program leads, RIM professionals should provide inputs and be part of the team. RIM participation is essential in the following area.

Scoping the Payment Card Environment

The very first step in setting up a PCI compliance program is scoping the environment to determine what system components are subject to the PCI DSS. Because the RIM function has the duty of managing information enterprise-wide, it has a unique ability to locate the repositories where customer payment card data may reside. This includes order processing applications and databases, receipts, backup tapes, and any number of other records on both electronic and paper media.

Analyzing Data Flows, Business Processes

RIM professionals are in a unique position to see the big picture. They can see how data flows through seemingly disparate processes and repositories. After scoping the payment card environment, a RIM professional may be able to assist finance and IT in improving business processes for better efficiency and security.

Assessing Vendors

The PCI DSS requires merchants to track the PCI compliance of their suppliers and vendors. The organization's vendor security questionnaire should include a least one question on that vendor's PCI compliance. This is especially crucial if managing vendors for offsite records or data backup, which could potentially include the storage of customer card data. Make sure to investigate vendors' PCI compliance status before signing a contract, and track their compliance on at least an annual basis.

Updating Policy

While the organization may deem it necessary to create a separate policy regarding PCI compliance, any RIM or information security policies should include references and requirements to compliance with the PCI DSS. Incorporating these requirements into existing policies ensures all relevant team members are aware of the requirements and their responsibilities.

Adding Value, Developing an IG Career

Whether a member of a PCI compliance team or in a leadership role and a PCI subject matter expert, a RIM professional's involvement will add demonstrable value to the organization. The organization will value the efforts made to make the cardholder environment more secure, improve customer trust, and minimize the risk of noncompliance with bank regulations and state law, and the associated fines that may result.

Perhaps most importantly, taking the lead in a PCI compliance program is a prudent way to expand a career path from one narrowly defined in RIM to a more comprehensive IG career. It will also allow a RIM professional to develop relationships with other parts of the organization and expand the presence and awareness of IG priorities. **END**

Andrew Altepeter can be contacted at andrew.altepeter@gmail.com. *See his bio on page 47.*


SUCCESS

Building a Successful E-Discovery Strategy

Bill Millican

Organizations that adhere to sound information governance policies through disciplined records and information management are positioned to find success in even the most complex e-discovery projects.

The best place to start building the strategy for a successful discovery project is at the beginning. Not at the beginning of the investigation or the litigation, but at the records and information management (RIM) stage – which, according to ARMA International, is the foundation for strong information governance (IG) and is built by "establishing and implementing policies, systems, and procedures to capture, create, access, distribute, use, store, secure, retrieve, and ensure disposition of" records and information.

Organizations that adhere to sound IG policies through disciplined RIM are positioned to find success in even the most complex e-discovery projects; this is because the e-discovery process is affected directly by how well information is managed.

In fact, as shown in Figure 1, information management (referred to in this article as RIM) is the beginning stage of the Electronic Discovery Reference Model (EDRM), which is widely recognized as the basis for establishing a meaningful approach to a successful e-discovery strategy.

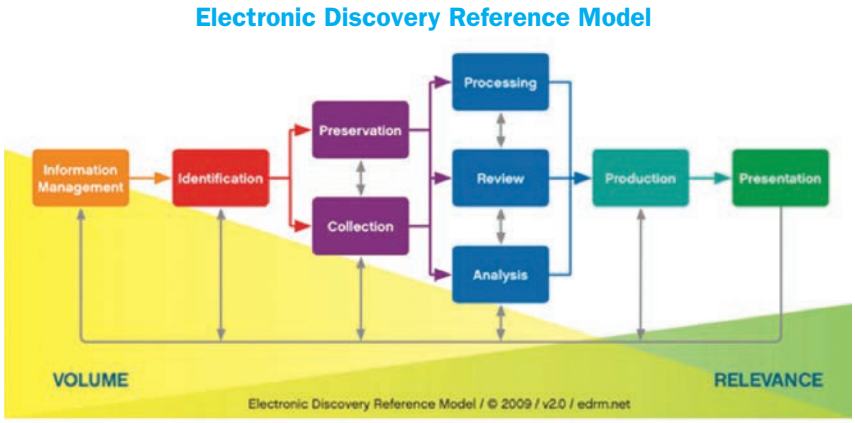


Figure 1: The Electronic Discovery Reference Model **Source:** EDRM

ILM: Critical for E-Discovery

A fundamental tenet of RIM is managing information throughout its life cycle – from creation to disposition; this is referred to as information lifecycle management (ILM). Those who developed the EDRM understood that properly managing information throughout its life cycle – not just when it is needed for litigation or investigation – is essential to e-discovery success.

E-discovery professionals that don't understand what is addressed in the first phase of the EDRM may not be aware of the critical role ILM fundamentals play in the e-discovery process. They may believe they have the RIM piece covered because they have information technologists who manage their servers, applications, and the data that resides in them; but, it is not that simple.

As Table 1 on page 34 illustrates, ILM and the EDRM are very similar.

RIM Reduces Financial Burden

In his "e-Discovery Team" blog about the Rand report "Where the Money Goes," noted attorney and

e-discovery expert Ralph Losey discusses the growing complexities directly associated with the growth of data, and the burdensome cost of governing that data are made clear. Another reference to the increase in over-burdensome cost is from *Inside Counsel*, entitled "E-discovery: Potential cost shifting for document review."

The courts continue to drive home the point that reducing the growing financial burden of the e-discovery process lies within that first phase of the EDRM. They have made it clear that organizations that fail to manage their information proactively and therefore overburden the legal process will be sanctioned accordingly.

Ignorance or lack of budget will not appease the court; both excuses have brought steep sanctions. For example, in the case of *United States v. Philip Morris USA, Inc.,* 327 F.Supp.2d 21, 25-26 (D.D.C. 2004), the court imposed a fine of $2.75 million and barred testimony of witnesses who violated the court's preservation order and company's document retention policy.

In *MasterCard International, Inc. v. Moulton*, 2004 U.S. Dist. LEXIS 11376, *14-16 (S.D.N.Y. June 22, 2004), the court allowed argument for negative inferences due to Moulton's failure to cease normal document retention practices, despite the absence of bad faith.

Rule 26 of the Federal Rules of Civil Procedure (FRCP) requires opposing counsel to "meet and confer" to discuss and, to a great extent, agree upon the types of electronic information each party requires. A successful outcome depends on how well the organizations know what information they have, where it is located, how to cull it, and how to retrieve and produce it in a way that ensures its authenticity – in other words, it depends on how well they *govern* their information.

RIM vs. IG: Not the Same

While the EDRM describes the first e-discovery stage as *information management*, the more encompassing term would be *information governance*. There are important distinctions.

Information Lifecycle Management Stages	Electronic Discovery Reference Model Phases
1. Receive/Create	1. Locate certain and specific records.
2. Use/Activity: modify, edit, transfer or move	2. Gather or collect records.
3. Inactivity: transfer to storage, store, retrieve, return.	3. Review records against criteria to validate that the collection is accurate and complete.
4. Disposition: final review, destruction, documentation	4. Organize the collection properly.
5. Archive: review, use, and return	5. Prepare the collection for proper production.
	6. Present the collection.

Table 1: Similarities Between ILM and EDRM

Information *governance* is *strategic* in nature. It determines how information is to be created/received, if it is to be used and for what purposes, and how it will be stored and then archived or destroyed. Governance also establishes, dictates, monitors, and audits compliance with policies and procedures related to all of these stages of the information lifecycle.

Information *management* is *reactive* in nature. It plays a custodial role, facilitating the organization of information that has been created/received, is being used, and eventually will be stored and then archived or destroyed. Essentially, it is responsible for the implementation and continued execution of information *governance* guidelines, policies, and processes.

The sooner organizations can expand their idea of the EDRM's information management stage to encompass information governance, the better prepared they are going to be for all business processes, not just for litigation.

The EDRM's Six Phases

The EDRM is a six-phase formula for handling the e-discovery process, beginning with information management, as discussed above.

Phase 1 – Information Management

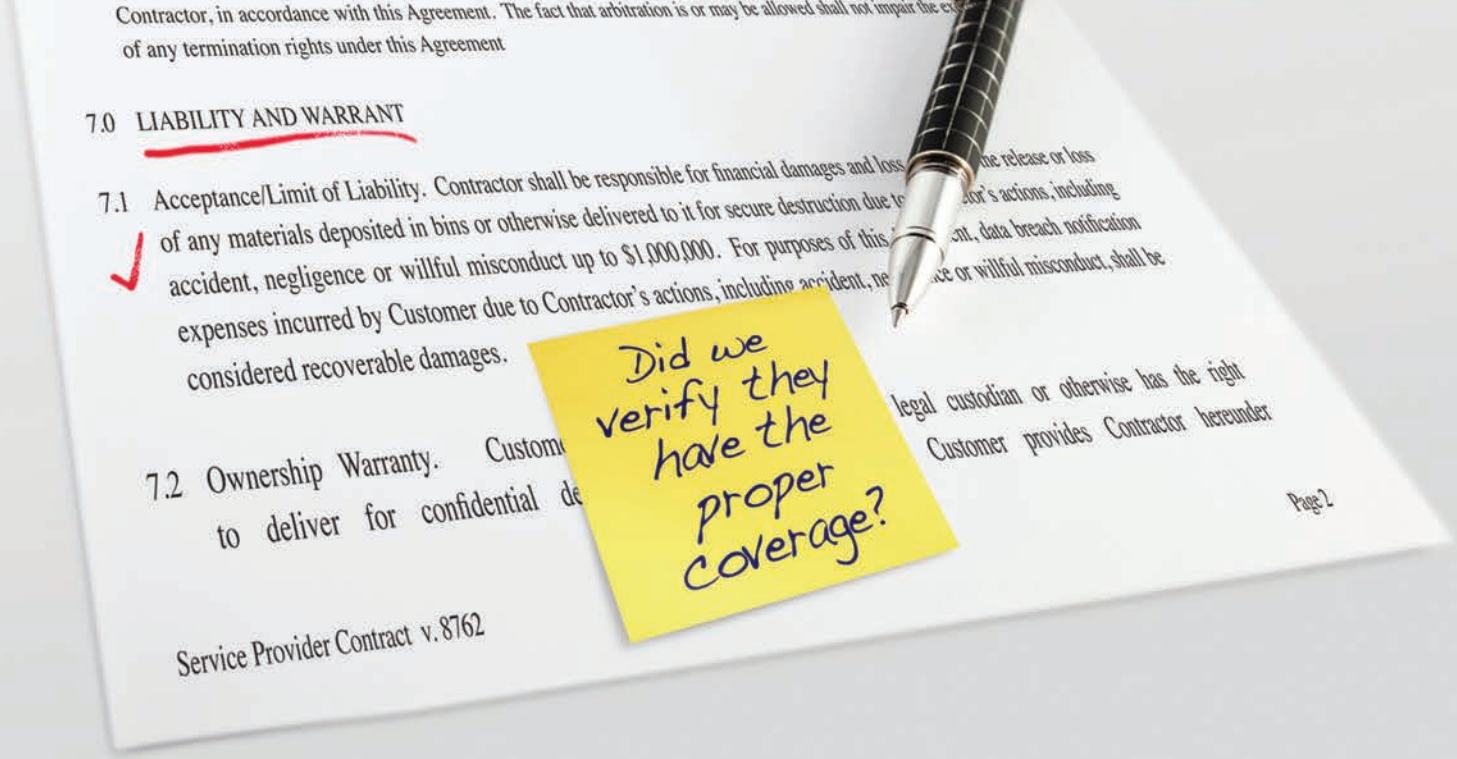
As already noted, this would be better described as IG. Until an organization commits to righting its RIM and IG programs, complete with policies and processes, it cannot believe that it will fare well through e-discovery.

Managing information is simply not enough. Organizations will be better prepared to initiate and negotiate each phase of the EDRM when they have shifted from merely *managing* their information to *governing* their information. It is a paradigm shift that will require significant changes in organizational resources.

Many organizations have vice presidents or chief officers whose sole responsibility is to oversee IG. These individuals and their teams are tasked with overseeing the organization's governance of the information life cycle. From custodian, to supervisor, manager, and vice president, this evolution continues; and to a great extent, it has a direct correlation to the e-discovery process.

Phase 2 – Identification

Judge Shira Scheindlin from the Southern District of the State of New York was instrumental in the development that resulted in FRCP Rule 26 mentioned above that requires opposing counsel to agree to what electroni-



Some customers assume their service providers have the proper liability insurance to cover their mistakes.

Unfortunately, that is not always true.

The National Association for Information Destruction (NAID), the non-profit watchdog for the secure destruction industry, discovered that most professional liability products do not offer adequate protection. So NAID created Downstream Data Coverage, a policy that better protects providers and customers.

- Includes data breach notification coverage to the full limit of the policy
- Requires periodic, unannounced audits of service providers
- Covers liability for electronic media destruction to the full limit of the policy
- Eliminates exclusions that make other policies useless

To protect your organization, encourage your service provider to look into Downstream Data Coverage today.

Downstream® Data Coverage

www.downstreamdata.com

cally stored information (ESI) is to be produced.

This discussion includes identifying not only the types of ESI required, but also the repositories in which it is stored and from which it must be retrieved. It may also include identifying the hardware and software necessary to read the gathered ESI. Whether the ESI is reasonably accessible also may be a part of the discussion.

Phase 3 – Preservation and Collection

Data, records, and information that meet the criteria set forth above by counsel and then approved by the court must be first preserved under a *legal hold,* a process described by ARMA International as "A hold placed on the scheduled destruction of records due to foreseeable or pending litigation, governmental investigation, audit, or special organizational requirements." Organizations that do not have such formal processes in place as a part of their IG program are at great risk.

The legal hold process aligns perfectly with the concept of formal IG, and at the very center of ILM are preservation and collection. The elements of systematic compliance and trust permeate throughout.

***Phase 4* – Review and Analysis**

In the realm of ILM, review and analysis are never ending. For an organization to ensure that its ESI is current and reliable for all business purposes, review and analysis must be constant priorities.

The most time-consuming and costly phase, review and analysis requires that great lengths be taken to ensure beyond a reasonable doubt (often beyond *any* doubt) that the information moved into production and finally to presentation is *exactly* what is required.

It takes hours upon hours to review hundreds of thousands – often millions – of documents to make these determinations. The monetary investment in these human reviewers can reach up to several hundred dollars per hour and the total can soar into the millions of dollars.

This phase of the EDRM is definitive RIM (or ILM).

Phase 5 – Production

Now that the required data has been agreed upon, identified, preserved (locked down), collected, reviewed, and analyzed to ensure accuracy and validity, production is readied for the court. For the RIM ILM purist, this is exciting stuff because it's about the governance of the information life cycle.

Phase 6 – Presentation

This final step places the information into the hands of no return. This final phase is a relief; following and adhering to the tenets that support the process result in a confidence that can be achieved by no other means.

The Evolution: RIM to IG

E-discovery is not easy. It can be enormously expensive and a painful burden on any organization negotiating its way through it. There are those wise prognosticators who say that it is no longer *if* one gets sued, but rather *when* one gets sued. The United States is the most litigious society ever, and the legal industry is big business. The courts are flooded, and the expenses run to unbelievable heights.

The EDRM is a helpful tool that should prompt prudent organizations to start with a strong foundation of RIM and its concept of ILM, then evolve to encompass IG tenets to ensure compliance with policies and processes that will be the key to successful e-discovery. **END**

Bill Millican can be contacted at bmillican@xactdatadiscovery.com. *See his bio on page 47.*

It is your life. It is your career. It is your certification.

CRM

In a business world of doing "more with less," your designation as a Certified Records Manager shows that you understand the many facets of the RIM profession.

In a business world that is rapidly changing, your designation as a Certified Records Manager shows you are up to date on the latest technology, the latest rules and regulations, and the techniques of the RIM profession.

In a business world in which new jobs are increasingly competitive, your designation as a Certified Records Manager shows that you have the experience and expertise that others may lack, and skills to show that you are a leader in the RIM profession.

For more information about becoming a Certified Records Manager, contact (518) 463-8644 or visit www.icrm.org

ICRM®
Institute of Certified Records Managers

The Principles at Work at Ameritas: Planning a Unified Approach for Managing E-Records

Julie Gable, CRM, CDIA, FAI

As the second vice president of corporate facilities at Ameritas, an insurance and financial services mutual holding company headquartered in Lincoln, Nebraska, Robin Martin, CBCP, FLMI, has responsibility for business continuity, purchasing, and project management of new construction underway in Cincinnati. (See Martin's career overview on the next page.)

Martin assumed leadership for records and information management (RIM) in 2011, an organizational move that made sense given her understanding and awareness of records concepts earned through her experience with Ameritas. Up to this point, the Ameritas records program had been mostly focused on paper records, with an in-house records storage facility and a Lotus Notes database to manage storage and retrieval of boxes. Retention schedules had also been developed, but actual disposition of outdated records was primarily of hard copy records.

Around this time, the company realized it needed to apply records principles to focus on disposion of electronic, as well as paper records. Soon the discussion turned to where responsibility for electronic records should reside, and while a case could be made for management by information technology (IT), it was ultimately decided that the data and records belonged to the various business areas. It was determined that a unified, strategic approach was needed when it came to electronic records, and Martin was tasked with overseeing this.

Getting Started

As an initial step, Ameritas engaged Huron Consulting to assess its records and information management program based on the Generally Accepted Recordkeeping Principles® (Principles) and the Information Governance Maturity Model (Maturity Model). Huron determined that pre-existing RIM efforts had many elements of the Principles in place, although they had not necessarily been identified or categorized as such. Using the Maturity Model, Huron was able to determine objectively where various RIM aspects were adequate and address areas that the company might want to consider for

enhancement or improvement.

"One of Ameritas' requests was that assessment results be conveyed as descriptive findings rather than as numeric ratings," says Martin. "There was concern that if we got a numerical score, what would it mean and how would others interpret it? More description was necessary, rather than numbers, and we were able to do this with the definitions that the tool provides. We were also able to explain what the various levels – Sub-standard, In Development, Essential, Proactive, and Transformational – meant when we presented the assessment results to the steering team."

From the assessment, Huron developed a five-year plan, defining activities aimed at improving or enhancing various program elements that would strengthen the program and position Ameritas for effective management of electronic records.

Establishing Accountability

"For [the Principle of] Accountability, for example, Ameritas did not previously have a corporate records officer in place," said Martin. "This was addressed with a formal infrastructure that now includes a steering team comprised of legal, IT and RIM. In addition, all departments have department records administrators, usually people at management level who are ultimately accountable and responsible for RIM.

"There are also records coordinators, the doers who make sure that work gets done, that training takes place, and that retention schedules are reviewed and refreshed on a regular basis," she said. Large departments in bigger lines of business may also have departmental records representatives.

Enhancing Retention

To enhance the Principle of Retention and prepare for applying retention periods to electronic records, retention schedules were consolidated across all lines of business and their regulatory requirements reviewed in 2011.

"Even though we thought we had a process-based schedule, it was really departmental. Different lines of business had different requirements. We were able to streamline when we realized that the process is insurance, for example, and that a policy is a policy. This also helped to eliminate duplicates and get consensus on retention," noted Martin.

Another change was to the retention periods themselves. "The previous schedule had event-based codes," Martin said. Event-based retention codes rely on the occurrence of an event to start the retention clock ticking – things like close of a project or termination of a contract. "When we went through the schedule review, we knew it would be difficult, if not impossible, to apply event-based codes to electronic records, particularly in structured systems like databases. So we worked with tax [personnel] and others to come up with finite, numerical retention times – for example, a specific number of years – which we could more easily apply in both the paper and electronic realms."

Improving Compliance

To improve on the Principle of Compliance, Ameritas reviewed regulatory changes within the insurance and financial services industries. Martin also reviewed existing RIM policies. She noted, "Most of our RIM policies were broad enough to cover all records, not just physical, and with a few tweaks in this area we were able to strengthen them."

Focusing On E-Records Systems

With revised retention schedules in place, Ameritas is focusing on systems that contain structured electronic records, namely databases for such functions as policy administration.

"What we are currently doing," said Martin, "is identifying whether these systems have retention capabilities as part of their

Robin Martin: A Career Overview

Robin Martin is the Second Vice-President of Corporate Facilities at Ameritas, an insurance and financial services mutual holding company headquartered in Lincoln, Nebraska, that serves approximately 3.2 million policy holder/members. Its 2,300 associates nationwide offer life insurance, annuities, individual disability income insurance, group dental, vision and hearing insurance, as well as retirement plans, investments, mutual funds, asset management, and public finance.

Martin has held this post for seven of her 25 years with the company, which includes responsibility for business continuity, purchasing, and project management of new construction underway in Cincinnati. She assumed leadership for records and information management in 2011.

Martin is a Certified Business Continuity Professional and a Fellow of the Life Management Institute *(a life insurance industry accreditation)*.

operating systems, and if so, how they can be utilized, and if not, how such capabilities can be added."

Martin continued, "We started with a pilot project of five systems to get our feet wet. Of those five systems, three required remediation, one didn't contain records, and one needed a retention schedule modification. Since then, we've done an inventory of all systems and have asked records administrators and coordinators to help identify which of these contain records."

Martin said many questions are emerging during this process, beyond those about the availability of retention capabilities, including, "What is a record, what is metadata? What types of records does this system contain, what risks are associated with them? Do we get legal holds on the system? Is it as simple as plugging in retention requirements? How can retention and purge aspects be effected in the system?"

Moving Toward Information Governance

It is a large undertaking, and one that raises questions even beyond records management. Earlier this year, Ameritas formed the Information and Records Governance Advisory Team to discuss questions regarding privacy, protection, and retention of information throughout its life cycle. The advisory team is composed of leaders at the executive level who are in a position to know what is planned for electronic systems within their areas of responsibility. Martin believes the Principles can help this team's efforts by giving everyone a consistent understanding of what good information governance requires.

The past has shown that because Ameritas is a diversified company with various lines of business, some decisions have been made in silos. "What the advisory team is striving for is an organization-wide perspective. There is a need to understand that what one part of the business does can affect other lines as well. If we buy a new system, we must address privacy, security, protection, and recordkeeping up front," said Martin. "We want to make sure we are in compliance with laws and regulations, of course, but also with our own retention schedule and policies."

There is a need to understand that what one part of the business does can affect other lines as well.

Recognizing Benefits

Martin is beginning to see changes. "Now if a business area looks at a new system, they are able to ask the right questions. From our work on structured systems and information governance, we can fine tune the list of requirements that the system must fulfill. More than just checking 'yes' on a list of generic requirements, we can determine if the system under consideration does recordkeeping as Ameritas specifically defines it. These are standards that are starting to develop and will continue in the future."

Another benefit of Martin's work is a heightened awareness of RIM company-wide. Ameritas has developed online RIM presentations that are mandatory for all employees as part of the new hire onboarding process.

"Everyone has records," said Martin, "and we need to make sure they are educated. Associates can go through the module to understand what is meant by 'records' and 'records management.' Ameritas' streamlined and consolidated retention schedules have become easier for everyone to understand and use, and easier to maintain."

Martin added, "Today people ask the question [about retention] where they previously didn't know that a question existed or what the question was."

Looking Toward the Future

One issue familiar to all records managers is the scarcity of resources. Martin notes that RIM is not any one person's full time job in any department. Her own resources are limited to the manager of the imaging function, who is responsible for maintaining the retention schedule; a paralegal in the law department, who provides legal hold and RIM management assistance; and one person who oversees the records storage center.

Despite these limitations, Martin said, "We have learned that we need to be flexible. We may want to accomplish x, y and z, but we may only be able to do x."

Thanks to the Maturity Model, the RIM program can prioritize and concentrate its limited resources on what is most important to the overall goal.

Although Ameritas has not yet determined whether it will do another RIM assessment, Martin believes the program will keep working, possibly with a three-year planning horizon focused on electronic records.

Martin concluded, "We know we don't legally need to be a [Maturity Model] Level 5 in everything, but if we can get to a certain level, that's great, and we can build from there." **END**

Julie Gable, CRM, CDIA, FAI, can be contacted at juliegable@verizon.net. *See her bio on page 47.*

BULLETIN BOARD

Xact Data Discovery

Xact Data Discovery (XDD) is an international discovery and data management company providing forensic collections, processing, hosting, document review, project management, paper discovery, and records management and governance consulting services. XDD offers an exceptional level of customer service, with a keen focus on communication to ensure clients know where their data is throughout the entire discovery life cycle.

www.xactdatadiscovery.com

XACT DATA DISCOVERY
Because you need to know

RSD

RSD recently announced the capability to deploy an information governance platform in under 10 minutes using its Information Governance as a Service (IGaaS™) model. Customers have the opportunity to define their information governance policies and systematically enforce those polices on content residing on premise or in the cloud. This proven approach delivers a predictable, low cost, and minimal risk approach to information governance.

For more information visit ***www.rsd.com/en/products/igaas-information-governance-as-service.***

ZASIO

Versatile RFID Mobile RT™

Zasio is pleased to announce its release of Versatile RFID Mobile RT (Real-Time). RFID tags, unlike barcodes, do not need line-of-sight reading and allow you to read multiple tags in one scan. File tags can be read inside a box without removing the lid, as can box tags located behind other boxes. Versatile RFID Mobile RT can help speed up the processes of inventorying all of your physical records and keeping information about the records updated in the database. Another reason to choose Zasio's Versatile Software for your records management needs!

To learn more about our RFID solutions, visit our website and download the whitepaper! ***www.zasio.com/company-downloads-whitepapers-rfid.asp***

DHS Worldwide, the global leader in records and information management software, is proud to announce the enhanced Optical Character Recognition (OCR) module, which includes up to a 40% increase in recognition speed. Total Recall Digital Imaging products provide improved searchability and accessibility of electronic records.

TOTAL RECALL™ SOFTWARE
BY DHS WORLDWIDE

To find out more about the latest software innovations from DHS, visit ***www.dhsworldwide.com*** or call **904.213.0448**.

NAID

NAID is the non-profit trade association for the secure destruction industry, which currently represents more than 1,900 member locations globally. NAID's mission is to promote the proper destruction of discarded information through education, the NAID 'em initiative, and encouraging the outsourcing of destruction needs to qualified contractors, including those that are NAID-certified. ***www.naidonline.org***.

Iron Mountain

Information is an advantage. Protecting your information is the key to the success of your business!

Whether you're building a foundation or improving upon your current RIM program, the new and improved "Records and Information Management Best Practices" is your key to establishing a comprehensive and compliant RIM program. Discover your copy at ***http://programs.ironmountain.com/forms/RIMBestPractices to uncover the most practical approach.***

Keys for Developing a Social Media Policy

Social media is reshaping the way organizations conduct business – from running sweepstakes to enacting sales transactions of products and services to managing various facets of customer relationships.

Getting ahead of this juggernaut of technological change is no small task. While using social media is rife with risks, a well-constructed and enforced social media policy can substantially mitigate or minimize those risks.

This excerpt from the ARMA International Technical Report *Using Social Media in Organizations* (ARMA TR 21-2012) provides valuable guidance for developing such a policy.

Policy Development

Policy that addresses an organization's participation in social media should be approved and championed at a high level within the organization, be technologically neutral (not restricted to a particular software and/or hardware), and support the organization's goals, objectives, governance structure, and organizational culture.

Successful policy creation and/or modification result from a collaborative, team effort. If records and information management personnel are developing the policy, they should elicit input into policy development from other stakeholder groups, including, but not limited to, Human Resources, Information Technology, Legal, and Marketing.

Initiate social media policy development by:

- Identifying the need for a policy to govern the organizational use of social media technologies
- Examining existing policies to identify which policies (if any) already cover records/information management and social media use
- Determining whether policies governing social media technologies should be embedded into existing policies or will need to stand alone, and, if embedded in existing policies, identifying the policies of which they will be a part
- Ensuring new social media policies align with existing policies
- Identifying key stakeholders responsible for new social media policy approval and implementation

See Figure 1 "Policy Development Workflow" on page 43.

Information Gathering and Analysis

Pertinent information may be gathered through interviews with administrators, decision-makers, records managers, and employees who participate in and/or oversee the use of social media. Analysis of the organization's data map and literature (e.g., annual reports, work and strategic plans, legal documentation, and legislation) should also be undertaken. This analysis will help to understand the administrative structure in which the social media policy, processes, and procedures will function.

Identify the legal and regulatory obligations applicable to the organization's recordkeeping requirements. Identify the relevant points that are key to the use of social media and that will need to be accounted for in the policy. This identification process should include, but is not limited to:

- All applicable laws, regulations, and statutes relating to information governance, protection of privacy, and freedom of information
- Intellectual property, e.g., copyright, legislation, and requirements to ensure protection of organizational assets
- Regulatory and/or professional bodies' guidance on the use of social media

[Editor's note: Further information about laws and regulations is available in section 5 of *Using Social Media in Organizations*.].

A review of social media-related

activities within the organization will also provide an understanding of social media's potential impact on records and information management. Data can be gathered by interviewing social media users and inventorying and analyzing the social media technologies they use. Conducting such a usage review will aid in identifying and understanding:

- Organizational norms and standards for record creation within social media applications
- Personnel and technological concerns and/or constraints about the use of social media
- Business/organization cultural issues that impact the use of social media

Map the existing social media use within the organization to the identified best practices and statutory/regulatory obligations under which the organization operates. This will aid in the identification of gaps that will need to be addressed as well as whether more information gathering is required.

[Editor's note: Further information about risk management and behavioral norms is available in section 7 of *Using Social Media in Organizations*.].

Identifying Required Policy Elements

Whether by inclusion in existing policies that address records and information management or through the creation of a new social media policy, required policy elements should be identified. Establish the elements needed to mitigate the risks associated with the use of social media technologies and enable the identification, creation, capture, transmission, and/or storage of records.

Suggested elements:

1. **Purpose/objectives statement** – Describes the purpose or set of objectives that align the goals of the social media policy with those of the organization.
2. **Scope statement** – Indicates the types of social media to be used, the purposes for the usage, the department personnel to whom the policy applies, and the types of records and information covered.
3. **Mandate statement** – Correlates to the mandate of the organization, agency, or department issuing the social media policy.
4. **Definitions** – Contains a glossary of organizational and social media terms used in the policy (particularly if these terms differ from standard organizational use).
5. **Roles and responsibilities statement** – Identifies stakeholders and their responsibilities pertaining to the social media policy.
6. **References** – Provides a listing of national/regional leg-

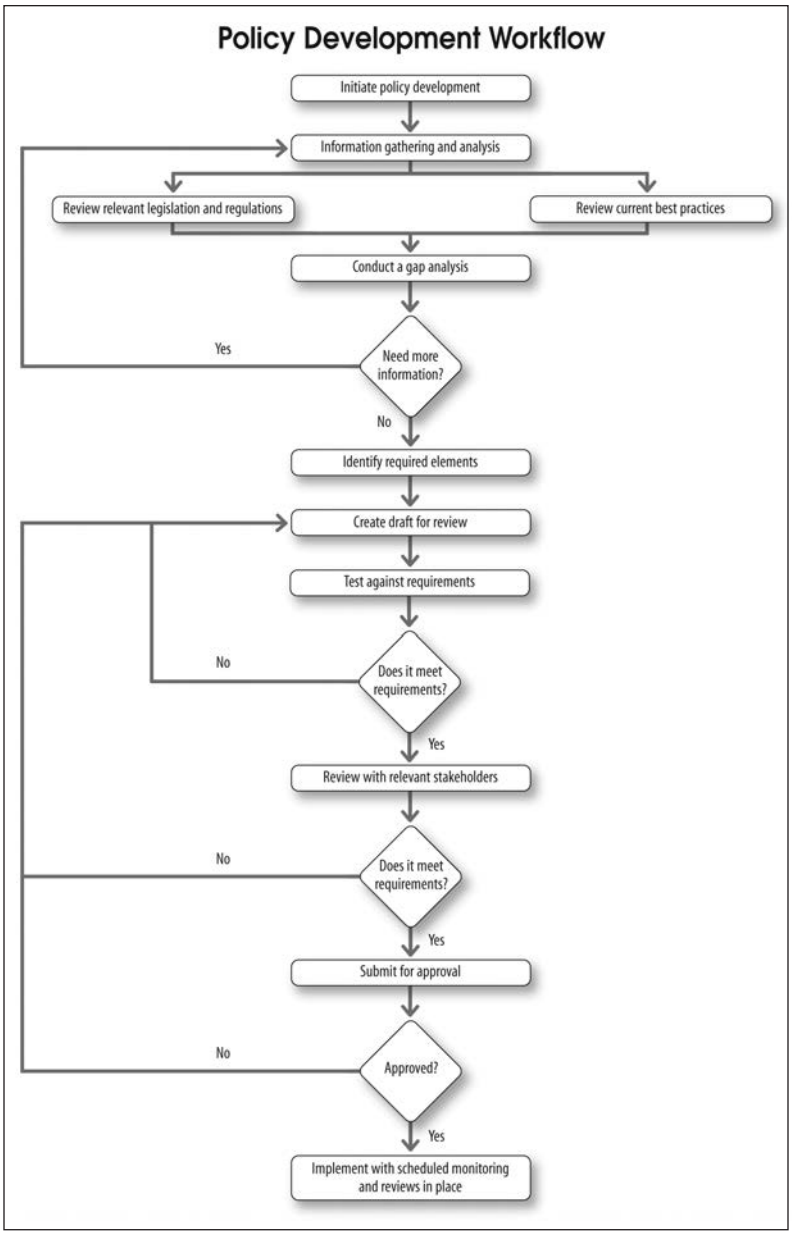


Figure 1: "Policy Development Workflow"

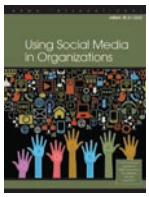
islation and regulations to which the social media policy adheres, including relevant organizational policies.

7. **Version control** – Offers assurance that the most up-to-date social media policy is being followed; includes version number, date policy is effective, and, if superseded, the date superseded and title of the policy it supersedes.
8. **Review statement** – Indicates the individual and/or department responsible for reviewing the social media policy (also the policy contact), the date the social media policy was reviewed, the date the social media policy was approved, the length of time between social media policy reviews, and the date of the next social media policy review.
9. **Behavioral expectations statement** – Describes how an employee is expected to communicate and conduct him/herself on behalf of the organization when using social media – including user authorizations, use and storage of passwords, permissions to post to social media accounts, use of anonymity, rights after termination, and authorization to change account names and settings. (Ensure that organizational social media policies are not in violation of employee rights under applicable labor legislation.)
10. **Expectation of privacy statement** – Delineates the level of privacy employees should expect when using social media sites on behalf of the organization.
11. **Confidentiality guidance** – Instructs employees on the protection of confidential and personal information within the context of social media.
12. **Social media site guidance** – Lists the types of social media tools (e.g., potential sites) approved by the organization to communicate organizational information.
13. **Permissible information statement** – Identifies the categories of information considered permissible for creation, capture, transmission, and/or storage via social media.
14. **Records management guidance** – Provides directives regarding the management of records created with social media technologies including records creation, capture, transmission, storage, retention, and disposition, as well as appropriate records metadata application and preservation.
15. **Account maintenance guidance** – Gives instructions for establishing, maintaining, and closing social media accounts.
16. **Legal statement** – Provides legal disclaimers for inclusion in the organization's social media postings.
17. **Intellectual property statement** – Provides guidance on using and posting copyrighted works, trademarks, and protected materials on social media sites.
18. **Security statement** – Instructs employees on data security within the context of social media.
19. **Ownership statement** – Identifies organizational ownership of social media accounts, content, and participants (e.g., "followers").
20. **Enforcement statement** – Indicates how the policy will be enforced within the organization and the consequences for violating the policy.
21. **Signature** – Provides a line at the end of the policy document so each employee may sign and acknowledge that he/she has read, understood, and agreed to the terms of the policy.

The initial draft policy should be reviewed by the key stakeholders and their feedback elicited.

The initial draft policy should be reviewed by the key stakeholders and their feedback elicited. This will aid in identifying errors in the policy, addressing implementation issues, and ensuring the policy aligns with existing organizational policies and norms.

Following the policy's drafting and approval, the organization should communicate its content to all employees through education and training activities. Due to the ever-evolving nature of social media, the policy should be monitored and updated with concomitant re-education/re-training of employees, as needed. **END**



Editor's Note: *Using Social Media in Organizations* (ARMA TR 21-2012), from which this article was excerpted, is available for purchase from the ARMA online bookstore at *www.arma.org/bookstore*.

Noteworthy New Records Management Textbook

Lee R. Nemchek, IGP, CRM

Though out of print for many years, *Information and Records Management: Document-Based Information Systems* by Mary Robek, Gerald F. Brown & David O. Stephens (Westerville: McGraw-Hill Publishers, 4th Ed., 1996) is arguably the most well-known and respected textbook on records and information management (RIM) practice and procedure. A perusal of ARMA International's bookstore offerings shows a few other, more current general texts, but none of these has the cachet that has kept Robek, Brown & Stephens on most RIM 101/CRM study lists for more than 17 years. That is, until now.

Patricia C. Franks, Ph.D., IGP, CRM, an associate professor in the School of Library and Information Science at San José State University, has authored *Records & Information Management*, the first authoritative RIM text written from an information governance (IG) perspective. The IG model articulates a new set of imperatives for information professionals, one that includes legal, compliance, and information technology elements in equal measure alongside traditional RIM topics, such as inactive records management and records retention and disposition.

As Franks writes, RIM professionals must "master the fundamentals of different but related fields, including compliance, risk management, change management, and project management" in order to be successful in the new era of Records Management 2.0. This book may prove to be a worthy successor to Robek, Brown & Stephens, especially because shortly after its publication, the Institute of Certified Records Managers (ICRM) adopted it as a source of test items for Parts 1 through 5 of the CRM exam.

Scholarship Broad and Deep

As might be expected from a library school professor, *Records & Information Management* reflects comprehensive, far-ranging reading in the discipline. The scholarship is impressive, with cited authorities going back to 1949 and as current as mid-February 2013. What's most impressive, however, is the overall breadth of coverage, which is evident on several levels:

Content

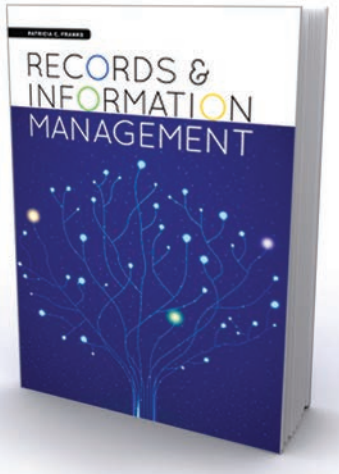
This textbook covers paper-based and electronic records management topics, as well as all of the major IG touchstones, including big data, cloud computing, social networking, bring your own device, information security and privacy, risk management, and information audits.

Jurisdiction

Examples and citations are drawn from U.S. federal and state sources, Canada, the United Kingdom, Italy, Australia, and the Philippines, among other jurisdictions.

Source Format

In addition to common formats such as books, periodicals, professional/academic journals, newspapers, encyclopedias and dictionaries, sources include press releases, news transcripts, videos, slide shows, websites, blogs, wikis, social media sites, product promotional literature, research and consultancy reports, and law firm client advisories. The extensive chapter notes are a great font of information on available RIM resources.



Records & Information Management
Author: **Patricia C. Franks**
Publisher: **Neal-Schuman**
Publication Date: **2013**
Length: **424 pages**
Price: **$80**
ISBN: **978-1-55570-910-5**
Source: ***www.arma.org/bookstore***

Organization Type

Franks describes RIM projects and processes from various national, state and local government and regulatory agencies, educational institutions, for-profit commercial companies, and non-profits.

Standards and Best Practices

Franks draws heavily from the literature of professional and industry associations, including ARMA International, AIIM, ICRM, PRISM, The Sedona Conference®, Project Man-

agement Institute, International Association of Privacy Professionals, International Council on Archives, Society of American Archivists, British Standards Institution, International Organization for Standardization, and American National Standards Institute.

Bibliographic Tools

Each of the 12 chapters includes an introduction, a concluding summary, a brief case study or perspective essay contributed by a RIM industry specialist, and notes. In addition, the book provides more than 100 illustrations (figures, tables and photos), sidebars, an appendix of international regulations, and 70 pages of glossary, bibliography, and index.

On the strength of its currency and coverage alone, Franks' book is poised to take over as the recommended go-to reference for both students and RIM professionals for many years to come.

Agree to Disagree

Experienced RIM practitioners will likely identify certain points of contention among the author's assertions. For example, it is not a given that "the primary purpose of a records retention and disposition schedule is to ensure that records are retained only as long as necessary and then disposed of when they no longer have value." Some might argue that the *primary* purpose is to ensure that an organization meets its legal and regulatory obligations with respect to recordkeeping. Earlier in the same chapter, the author instructs records managers to establish retention periods while inventorying records, whereas actual practice dictates that inventory projects are almost always handled separately from retention/disposition projects, with each requiring a distinct set of resources. Records managers must decide for themselves whether they agree or disagree with the author on these and other issues that are open to differences of professional opinion and practice.

Stronger Editorial Oversight Needed

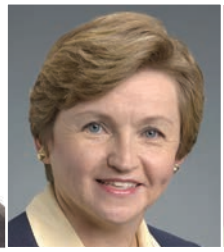
The overall high quality of this book could have been enhanced by stronger editorial oversight. For example, a list of abbreviations/acronyms would have allowed the author to use standard terms instead of writing out the same proper names over and over. Editors should have caught citations to superseded references and other inconsistencies, such as mentioning ARMA's new IGP certification in Chapter 12 (IG programs) but omitting it entirely from Chapter 11 (RIM education, training and professional development).

Some figures are overly vague (e.g., p. 98), and a case can be made that the final chapter, covering development and implementation of RIM and IG programs, properly belongs up front, instead of at the end of the book. Still, the editorial issues do not detract from Franks' achievement in gathering a large volume of both new and familiar material and synthesizing it into an up-to-date, coherent, readable, and highly informative text that all RIM/IG professionals should keep close at hand for ongoing reference. **END**

Lee R. Nemchek, IGP, CRM, can be contacted at lnemchek@oaktreecapital.com. *See her bio on page 47.*

Contact Information

AUTHOR INFO


ALTEPETER GABLE MILLICAN NEMCHEK PHILLIPS

Retiring Legacy IT Systems Under the IG Umbrella Page 20

John T. Phillips, CRM, CDIA, FAI, is a management consultant with Information Technology Decisions. With more than 30 years of experience in many information and technology management professional positions, he currently assists clients in developing comprehensive records management programs, especially with electronic records management issues and technology systems selection. Phillips recently served a six-year term on the National Archives and Record Administration's Advisory Committee for the Electronic Records Archive. He can be contacted at *john@infotech-decisions.com*.

How to Develop a PCI Compliance Program – And Take a Step on the IG Career Path Page 26

Andrew Altepeter is an information governance analyst at Motorola Solutions Inc., where he is responsible for records management and IT audits for Sarbanes-Oxley and Payment Card Industry compliance. He has previous experience in records management and institutional archives. He earned a bachelor's degree in history from Marquette University and a master's degree in public history from Loyola University Chicago. Altepeter can be reached at *andrew.altepeter@gmail.com*.

Building a Successful E-Discovery Strategy Page 32

Bill Millican is a respected expert in the field of records and information management and the director of sales and operations for Xact Data Discovery in Kansas City, Missouri. He has nearly 40 years of experience in various hands-on roles and consulting positions, including having served as director of IT and standards for ARMA International. He can be contacted at *bmillican@xactdatadiscovery.com*.

The Generally Accepted Recordkeeping Principles®
The Principles at Work at Ameritas: Planning a Unified Approached for Managing E-Records Page 38

Julie Gable, CRM, CDIA, FAI, is president and founder of Gable Consulting LLC. She has more than 25 years of experience specializing in strategic planning for electronic records management, including business case development, cost-benefit analysis, requirements definition, and work plan prioritization. Gable has authored numerous articles and frequently speaks at national and international conferences. She holds a master's degree in finance from St. Joseph's University and a bachelor's degree in management from Drexel University. Gable can be contacted at *juliegable@ verizon.net*.

Noteworthy New Records Management Textbook Page 45

Lee R. Nemchek, IGP, CRM, is vice president of enterprise records governance at Oaktree Capital Management L.P. in Los Angeles and previously served 22 years as a law librarian and records manager for an international law firm. She holds a master's degree in library science from the University of Southern California. She has authored numerous publications and is the series editor for ARMA International's new "Information Governance in the Legal Environment" monograph series. The first monograph, *Ethical and Legal Foundations of Law Firm Records Management and Information Governance,* written by Beth Chiaiese, CRM, was published in October and is available at *www.arma.org/bookstore*. She can be contacted at *lnemchek@oaktreecapital.com*.

AD INDEX

Contact Information

11, 15, 19 **AIIM**
www.aiim.org

29,31 **Access Sciences**
800.242.2005 – *www.accesssciences.com/SharePoint*

5 **DHS Worldwide Software**
800.377.8406 – Intl. 904.213.0448 – *www.dhsworldwide.com*

3 **BookFactory**
877.431.BOOK– Intl. 937.226.7100
sales@BookFactory.com/arma

35 **Downstream Data Coverage**
www.downstreamdata.com

37 **Institute of Certified Records Managers**
518.463.8644 – *www.ICRM.org*

BC **Iron Mountain**
www.ironmountain.com/arma

23 **NAID**
www.naid-em.com – bit.ly/AAAnotification

IBC **Recall**
888.RECALL6 – *info@recall.com*

IFC **RSD**
infous@rsd.com

9 **Xact Data Discovery**
877.545.XACT – *www.xactdatadiscovery.com*

13 **Zasio Enterprises Inc.**
800.513.1000 – *www.zasio.com*

Statement of Ownership, Management, and Circulation
(All Periodicals Publications Except Requester Publications)

UNITED STATES POSTAL SERVICE

1. Publication Title	2. Publication Number	3. Filing Date
Information Management	1 5 3 6 - 2 8 9 7	10-02-13

4. Issue Frequency	5. Number of Issues Published Annually	6. Annual Subscription Price
Bi-monthly	6	$140.00

7. Complete Mailing Address of Known Office of Publication (Not printer) (Street, city, county, state, and ZIP+4®)
ARMA International
11880 College Blvd., Suite 450
Overland Park, KS 66210

Contact Person: Vicki Miller
Telephone (Include area code): 913-217-6014

8. Complete Mailing Address of Headquarters or General Business Office of Publisher (Not printer)
ARMA International 11880 College Blvd., Suite 450 Overland Park, KS 66210

9. Full Names and Complete Mailing Addresses of Publisher, Editor, and Managing Editor (Do not leave blank)
Publisher (Name and complete mailing address)
ARMA International, 11880 College Blvd., Suite 450 Overland Park, KS 66210

Editor (Name and complete mailing address)
Vicki Miller, Editor-in-Chief, ARMA International, 11880 College Blvd., Suite 450 Overland Park, KS 66210

Managing Editor (Name and complete mailing address)
N/A

10. Owner (Do not leave blank. If the publication is owned by a corporation, give the name and address of the corporation immediately followed by the names and addresses of all stockholders owning or holding 1 percent or more of the total amount of stock. If not owned by a corporation, give the names and addresses of the individual owners. If owned by a partnership or other unincorporated firm, give its name and address as well as those of each individual owner. If the publication is published by a nonprofit organization, give its name and address.)

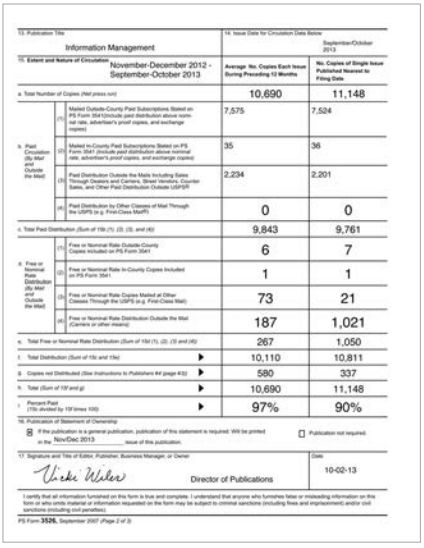
Full Name	Complete Mailing Address
ARMA International	11880 College Blvd., Suite 450 Overland Park, KS 66210

11. Known Bondholders, Mortgagees, and Other Security Holders Owning or Holding 1 Percent or More of Total Amount of Bonds, Mortgages, or Other Securities. If none, check box → ☐ None

Full Name	Complete Mailing Address

12. Tax Status (For completion by nonprofit organizations authorized to mail at nonprofit rates) (Check one)
The purpose, function, and nonprofit status of this organization and the exempt status for federal income tax purposes:
☐ Has Not Changed During Preceding 12 Months
☐ Has Changed During Preceding 12 Months (Publisher must submit explanation of change with this statement)

PS Form **3526**, September 2007 (Page 1 of 3 (Instructions Page 3)) PSN 7530-01-000-9931 **PRIVACY NOTICE:** See our privacy policy on www.usps.com



13. Publication Title: Information Management	14. Issue Date for Circulation Data Below: September/October 2013	
15. Extent and Nature of Circulation	November-December 2012 - September-October 2013	
	Average No. Copies Each Issue During Preceding 12 Months	No. Copies of Single Issue Published Nearest to Filing Date
a. Total Number of Copies (Net press run)	10,690	11,148
b. Paid Circulation (By Mail and Outside the Mail) (1) Mailed Outside-County Paid Subscriptions Stated on PS Form 3541 (Include paid distribution above nominal rate, advertiser's proof copies, and exchange copies)	7,575	7,524
(2) Mailed In-County Paid Subscriptions Stated on PS Form 3541 (Include paid distribution above nominal rate, advertiser's proof copies, and exchange copies)	35	36
(3) Paid Distribution Outside the Mails Including Sales Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Paid Distribution Outside USPS®	2,234	2,201
(4) Paid Distribution by Other Classes of Mail Through the USPS (e.g. First-Class Mail®)	0	0
c. Total Paid Distribution (Sum of 15b (1), (2), (3), and (4))	9,843	9,761
d. Free or Nominal Rate Distribution (By Mail and Outside the Mail) (1) Free or Nominal Rate Outside-County Copies included on PS Form 3541	6	7
(2) Free or Nominal Rate In-County Copies included on PS Form 3541	1	1
(3) Free or Nominal Rate Copies Mailed at Other Classes Through the USPS (e.g. First-Class Mail)	73	21
(4) Free or Nominal Rate Distribution Outside the Mail (Carriers or other means)	187	1,021
e. Total Free or Nominal Rate Distribution (Sum of 15d (1), (2), (3) and (4))	267	1,050
f. Total Distribution (Sum of 15c and 15e) ▶	10,110	10,811
g. Copies not Distributed (See Instructions to Publishers #4 (page #3)) ▶	580	337
h. Total (Sum of 15f and g) ▶	10,690	11,148
i. Percent Paid (15c divided by 15f times 100) ▶	97%	90%

16. Publication of Statement of Ownership
☒ If the publication is a general publication, publication of this statement is required. Will be printed in the Nov/Dec 2013 issue of this publication. ☐ Publication not required.

17. Signature and Title of Editor, Publisher, Business Manager, or Owner
Vicki Miller Director of Publications
Date: 10-02-13

I certify that all information furnished on this form is true and complete. I understand that anyone who furnishes false or misleading information on this form or who omits material or information requested on the form may be subject to criminal sanctions (including fines and imprisonment) and/or civil sanctions (including civil penalties).

PS Form **3526**, September 2007 (Page 2 of 3)


recall
Your Information. Securely Managed.
"Your Passport to Information Management Freedom"
As organizations face increasing complexity with managing the expanding volume of physical and digital information and complying with industry and government regulations, they need a trusted partner that can help them. At Recall, we can help your business gain a competitive edge through the strategic, compliant, and economic use of information. Now that is Information Management Freedom!
Contact us at 1.888.RECALL6 (732.2556) or info@recall.com
PASSPORT
Recall
DOCUMENT MANAGEMENT SOLUTIONS
DATA PROTECTION
SECURE DESTRUCTION
DIGITAL SOLUTIONS
GOVERNANCE SOLUTIONS

Your Records and Information Management program presents opportunity to deliver real value to your business. You need a trusted partner to help you accelerate adoption and achievement of these goals and reach new heights. We can do more, together.

Visit us at ironmountain.com

IRON MOUNTAIN®

INFORMATION IS EVERYTHING