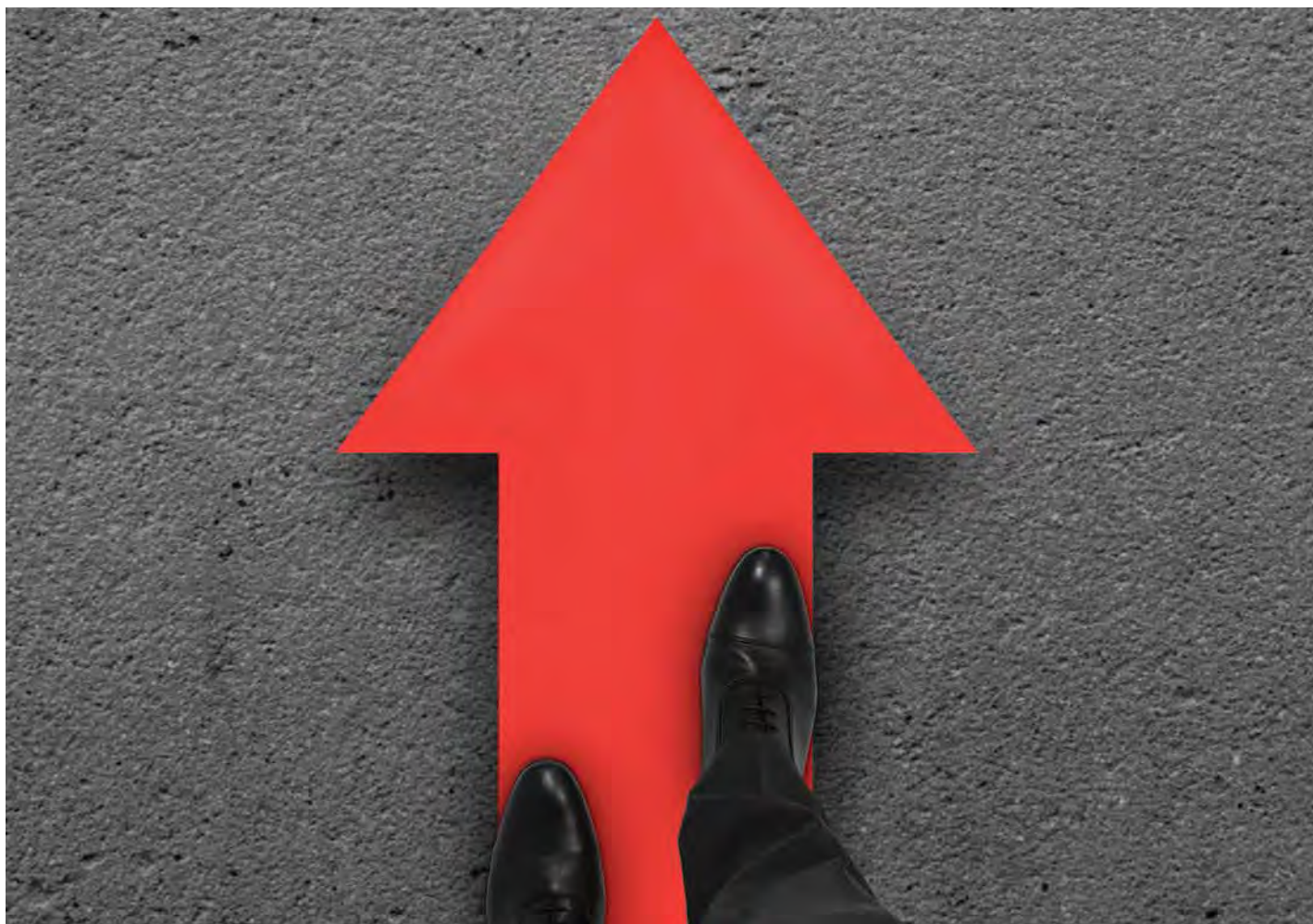


INFORMATION MANAGEMENT

AN ARMA INTERNATIONAL PUBLICATION

JULY/AUGUST 2015

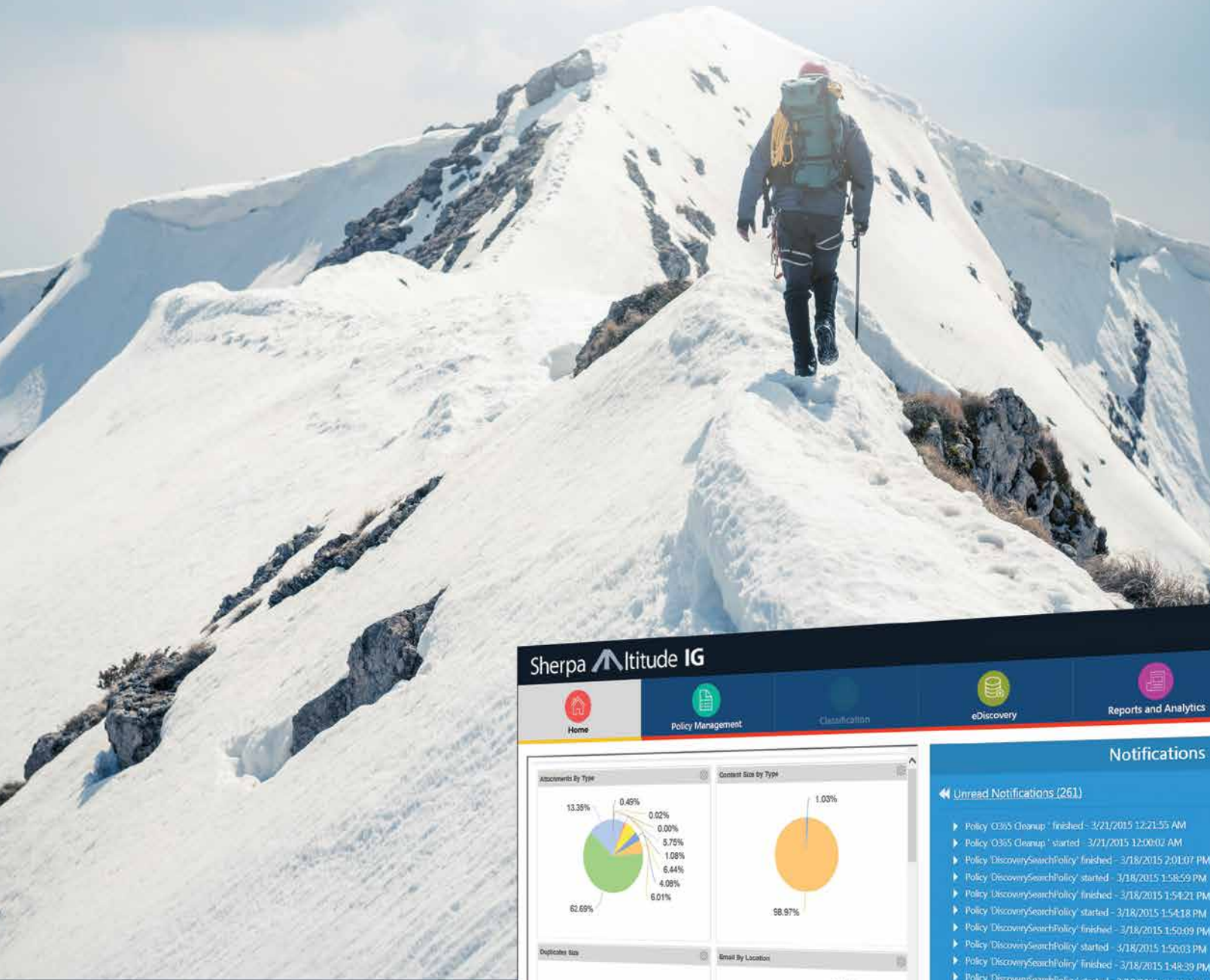


Critical Steps to Creating a Consistent **Preservation Hold Process**
Page 16

The Principles and External Audits Page 24

RIM's Role in Harnessing the Power of Big Data Page 29

Sherpa Ititude IG[®]



Take the first step
toward information governance.

Records and information management professionals are faced with the monumental challenge of locating, organizing, and managing electronic data. How do you manage something that large and complex? Where do you start? With a mountain of data to scale, you need a guide with the right tools. You need a Sherpa. Contact Sherpa Software to reach new heights in managing ESI.



www.SherpaSoftware.com | 1.800.255.5155

INFORMATION MANAGEMENT

JULY/AUGUST 2015 VOLUME 49 NUMBER 4



DEPARTMENTS 4
6

FEATURES 16

INFOCUS A Message from the Editor

UPFRONT News, Trends, and Analysis

Critical Steps to Creating a Consistent Preservation Hold Process

Richard Vestuto, J.D., and Bill Piwonka

THEPRINCIPLES

The Principles and External Audits

Julie Gable, CRM, CDIA, FAI

RIM's Role in Harnessing the Power of Big Data

Kevin L. Dale, CRM

SPOTLIGHTS 34

BUSINESSMATTERS

Planning for and Managing During a Paper Document Disaster

William R. Gulley, Jr

RIMFUNDAMENTALS
Records Management or Information Governance?

William Saffady, Ph.D., FAI

INREVIEW

A New Cataloging Standard for Today's Varied Resources

Robert Bailey, Ph.D., CRM

INREVIEW

Weighty Tome Is Light on Comprehensive RM Best Practices

Sheila Taylor, IGP, CRM

INREVIEW

Distracted? You May Have ADT (No, Not the Home Security System...)

Beth Mellinger

CREDITS 47

AUTHORINFO

48

ADVERTISINGINDEX

Online **Info** for Offline **Success**



Industry-leading **Information Management** magazine puts cutting-edge topics at your fingertips so you can turn best practices into reality for your organization. It's just one of the many perks of ARMA membership.

ARE YOU AN ARMA PRO?

**INFORMATION
MANAGEMENT**
www.arma.org

ONLINE

INFORMATION MANAGEMENT

AN ARMA INTERNATIONAL PUBLICATION

Publisher: Robert Baird, PMP

Editor in Chief: Vicki Wiler

Contributing Editors: Cyndy Launchbaugh, Jeff Whited

Art Director: Brett Dietrich

Advertising Account Manager: Karen Lind Russell, Krista Markley

Editorial Board: Sonali Bhavsar, IBM • Alexandra Bradley, CRM, FAI, Harwood Information Associates Ltd. • Marti Fischer, CRM, FAI, Wells Fargo Bank • Uta Fox, CRM, Calgary Police Service • Deborah Juhnke, IGP, CRM, Husch Blackwell LLP • Preston Shimer, FAI, Records Management Alternatives • Sheila Taylor, IGP, CRM, Ergo Information Management Consulting • Stuart Rennie, Stuart Rennie Consulting • Mehran Vahedi, Enbridge Gas Distribution Inc. • Jeremy Wunsch, LuciData Inc. • Penny Zuber, Ameriprise Financial

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 governing information as a strategic asset. Established in 1955, the association's approximately 27,000+ members include records and information managers, information governance professionals, archivists, corporate librarians, imaging specialists, legal professionals, IT managers, consultants, and educators, all of whom work in a wide variety of industries, including government, legal, healthcare, financial services, and petroleum, in the United States, Canada, and more than 30 other countries around the globe.

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.

Opinions and suggestions of the writers and authors of articles in **Information Management** do not necessarily reflect the opinion or policy of ARMA International. Acceptance of advertising is for the benefit and information of the membership and readers, but it does not constitute official endorsement by ARMA International of the product or service advertised.

© 2015 by ARMA International.

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.



KEEP CALM AND DUE DILIGENCE

Data protection laws require due diligence when
selecting service providers.

NAID's Services Selection Dashboard helps you achieve compliance.

<http://directory.naidonline.org>

Collaboration Ensures RIM Career Success and Growth



Wherever you are along the records and information management (RIM) career ladder, good collaboration skills are among the most critical to your being effective in your current role and to climbing to a higher rung. This issue's articles describe the valuable collaborative roles you can play in several business functions, including legal and technology initiatives.

Richard Vestuto, J.D., and Bill Piwonka write in the cover article that because legal holds “intersect with business units across the organization, including legal, IT, records management, HR, and compliance, among others,” a steering committee comprising these stakeholders is essential to ensuring that the organization's preservation protocols are applied consistently.

In “RIMS's Role in Harnessing the Power of Big Data,” author Kevin L.

Dale, CRM, says RIM professionals can help solve the big data problems that come with disorganized, duplicative, poor quality data. “Big data can partner with RIM to reduce the costs of identifying, preparing, and analyzing data,” Dale writes. Further, he says, “By creating synergies between RIM and the big data program staff and integrating RIM principles into all processes that ‘touch’ data, organizations can forge and maintain a sustainable path to the information governance (IG) needed to ensure high-value data.”

As the foundation of IG, RIM must be effective to ensure positive outcomes from audits, Julie Gable, CRM, CDIA, FAI, writes in the Principles Series article. “An IG program based on the Generally Accepted Record-keeping Principles® (Principles) and the Information Governance Maturity Model (IGMM) goes a long way to show that the organization takes its information management responsibilities seriously,” she says. “Used well, these comprehensive tools guide in developing and sustaining an IG program that delivers reliably during even the pickiest inspections.”

It also delivers in disaster scenarios. In “Planning for and Managing During a Paper Document Disaster,” William R. Gulley, Jr. writes that RIM best practices are not only fundamental to an organization being prepared for a disaster, but also to it responding efficiently and getting a favorable insurance settlement.

To close the issue, an excerpt from the upcoming third edition of *Records and Information Management: Fundamentals of Professional Practice* by William Saffady, Ph.D., FAI, emphasizes that “Information is a collaborative initiative that requires the involvement and expertise of multiple stakeholders.” In addition to records management, Saffady identifies IG stakeholders as IT, information security, risk management, legal, compliance, and business units that have or supervise control of information.

To be sure, RIM professionals who collaborate regularly with other IG stakeholders will broaden their skill sets, be sought out for their expertise, and find themselves in a good position for advancement.

How else can we help you excel in your career? Let us know at editor@armaintl.org.

Correction: In the print edition of the May/June 2015 *Information Management*, we should have included this disclaimer for “Avoiding the Hammer: Defensible Strategies for FRCP Proposed Rule 37(e)” by Katherine Aversano, J.D., and Joe Starnes, J.D.: “The views and opinions expressed in this article do not necessarily represent the position of the Department of Justice, the United States, or any agency thereof.” We apologize for this error.

Vicki Wiler
Editor in Chief



PREX15

September 16-18, 2015 | The Nines Hotel, Portland, Oregon

Sharpen your skills and advance your knowledge of the legal preservation process with comprehensive sessions, nationally recognized experts and ample opportunity for peer-to-peer learning.



FEATURED SESSIONS

Preservation and The Evolving IT Landscape

Given a brief glimpse into the future of IT, how must our organizations respond when it comes to e-discovery planning and strategies? Big data and the ever-expanding list of new types of data and storage devices can boggle the mind of even the most seasoned e-discovery professional. How must our policies and processes evolve as data becomes more mobile and global? How do we train our legal teams, our custodians and our IT professionals to respond to the anticipated pace of change? What processes and technologies do we need for ensuring defensible and cost-effective approaches to preserve, collect and review data in the future?

Snapshot of Collection Practices Today

Many corporate law departments are re-examining their collection strategies to drive more efficiency into their preservation process. Panelists will examine issues such as 1) when you need a collection done by a forensic examiner, when you don't, 2) best practices for performing more targeted collections, to shrink collection sizes, 3) issues and solutions for remote user and departing employee laptop collections, 4) pros and cons of the "collect everything" approach, 5) insights on how and if to collect from mobile devices, cloud sources, social media and other new data types.

Register today at www.PREX15.com

PROMO CODE: PREX200 FOR \$200 OFF

E-MAIL

NARA Develops E-mail Retention Schedule

With the 2016 year-end deadline for managing all records electronically on the horizon, the National Archives and Records Administration (NARA) is preparing new rules and guidelines to help U.S. federal agencies meet the requirements of the 2011 presidential directive on management of government records.

NARA is putting the finishing touches on a retention schedule for retaining e-mail as part of implementing its Capstone program. The schedule is to designate as “permanent” the records of certain senior officials – such as all heads of department, deputies to senior officials, staff assistants, and chief executive officers – for transfer to the National Archives after declassification or 15 years, whichever is longer.

Federal agencies are not required to adopt Capstone, but they do have to meet the deadline set by the presidential directive, and their plans must be approved by NARA.

“Capstone dispenses with content analysis,” said NARA General Counsel Gary Stern during a forum with agencies and other stakeholders in May. “It’s a crude, simplistic approach. It may not be great, but it’s better than the existing approach.”

In a recent *FCW* article, Paul Wester, chief records officer for the U.S. government, said, “Our archivists who deal with the permanent records, some of them are a little frustrated with this approach because they know that they’re going to be getting these large volumes, which still will contain lots of not very substantive records within them.”

As the article pointed out, e-mail management has become a charged issue given the publicity around former Secretary of State Hillary Clinton using a personal e-mail server for State Department business. Just as her staff had to cull through tens of thousands of e-mails to separate the official from the non-official, so will others subject to Capstone – with the exception of those mentioned above whose records are deemed permanent by default. This can be a manual, automated, or hybrid process.

Although there is software that analyzes e-mail content, selects relevant e-mail, and deletes the chaff, it is not used much in government yet, pointed out Adam Mazmanian, a senior staff writer who covers Congress, health IT, and government-wide IT policy.



E-DISCOVERY

Proposed Federal Rules Advance

The Supreme Court of the United States has given the proposed changes to the U.S. Federal Rules of Civil Procedure (FRCP) its blessings. Now the rules await Congressional approval, which, if everything goes according to plan, will have the rules going into effect December 1, 2015.

Amendments to Rule 37(e) specifically address electronic discovery. In brief, the revisions provide a unified standard for the courts to use in situations where electronically stored information (ESI) is not properly preserved.

If ESI that should have been preserved for a legal hold is lost because the party didn’t take the appropriate steps, and it can’t be easily reproduced, it’s up to the court to determine a remedy that is “no greater than necessary to cure the prejudice.” Only if the court decides the offending party destroyed the ESI intentionally can it choose to issue an adverse inference, jury instruction, or dismissal.

The other FRCP amendments focus on the importance of cooperation, proportionality, and reasonableness in discovery. Part of the goal is to minimize delays and control the mushrooming costs of producing documents during discovery.





MOBILE

Is Your Mobile Policy Ready for Wearables?

The next big trend in mobile computing is wearables, such as a Fitbit, the Apple watch, and Google Glass. We're clearly still in the early-adopter phase, but consider how quickly smartphones changed the way people do business.

Like most new technologies, wearables bring both exciting opportunities and serious challenges. While they can put the data within a short glance of the wearer, they can also present privacy and data security concerns.

"Employers would have to address those [concerns] head on, and be prepared to answer an array of questions—for starters, what data will be tracked? How will the data get stored? Who in the organization will have access to it? How will the information be used," warned Alberto Torres, chief executive officer of Atheer Labs, in a recent guest article in *ReadWrite*.

This is likely to be true for all wearables. Torres pointed out that the medical sector, which has been an early adopter of many technologies (including tablets), has shown great interest in such gadgets as Glass. For example, Glass puts critical medical information in the literal view of doctors as they treat their patients, but it raises privacy

concerns. During a patient visit, what information can/should doctors capture? Have patients given their permission to be recorded? How are files stored or shared and

with whom?

Torres noted that these types of concerns are not insurmountable and may well be outweighed by the benefits of using the technology.

E-DISCOVERY

Survey Identifies Top E-Discovery Challenges

In-house legal and IT professionals involved in electronic discovery who were recently asked what their biggest e-discovery challenge is named the following:

- Locating potentially responsive data (36%)
- Controlling the amount of data sent for outside review and managing multiple e-discovery projects at once (14% each)
- Defensibly deleting data that was on legal hold (13%)

The survey, which was conducted by Exterro, offered the following four tips for addressing these challenges.

1. Implement an information governance program that enables you to know where the data is.
2. Integrate with commonly collected data sources for streamlined data collection.
3. Leverage new e-discovery technology that enables legal teams to rapidly identify and locate the most important documents before collection.
4. Develop repeatable, predictable processes between the identification, collection, processing, and analysis stages.



INFO SECURITY

Compliance ≠ Security

The majority – 61%, to be precise – of IT professionals surveyed in April at the 2015 RSA Conference said their organizations had implemented an IT security product simply to satisfy a compliance requirement, which actually put the organization's data at greater risk.

This is one of several factors that prompted 71% of the respondents to fear for their organization's data security. The other major contributors were:

- IT security products not being used to their full potential (cited by 70% of respondents)
- The difficulty of finding skilled IT security personnel (reported by 85%)
- Cyber attacks evolving too quickly for IT pros to keep pace (76%)

Lieberman Software's annual *Information Security Survey* was conducted during the 2015 RSA Conference because its attendees include IT security professionals from all regions of the world and all major vertical markets. It is available at <http://go.liebsoft.com/2015-information-security-survey>.



PRIVACY

U.S., French Patriot Acts Meet Different Ends

In early May, as U.S. lawmakers were preparing to narrow the scope of the USA Patriot Act in light of opposition to the National Security Agency (NSA) surveillance made public in recent years, French lawmakers were passing their own legislation to expand state surveillance.



France's National Assembly passed legislation that grants the state sweeping surveillance rights, despite loud opposition from civil rights groups, which have reportedly dubbed it the French Patriot Act. It is one of several government reforms introduced following the terrorist attacks in Paris in January.

According to news channel France 24, the country is still on high alert and has received repeated threats from jihadist groups, including the Islamic State (IS) group in the Syria-Iraq region. It is also struggling "to keep up with the hundreds of French citizens who travel to and from battlefields in Iraq and Syria to wage jihad, often lured over the Internet," reported the *New York Times*.

The new law would give French intelligence services the right to gather potentially unlimited electronic data on such suspected terrorists. It would allow them to tap cellphones, read e-mails, and force Internet providers to allow government access to their subscribers' communications. In other words, it would allow them to collect bulk information and analyze metadata in much the same way the NSA did – the very thing U.S. lawmakers were seeking to limit.

The intelligence services could also request permission to hide microphones in a room or on objects, such as on cars or in computers, or to place antennas to capture telephone conversations or mechanisms that capture text messages, the *New York Times* said. Both French citizens and foreigners could be tapped. Civil rights groups fear such access could easily and quickly extend to others the state deems a threat. The senate is expected to pass the law prior to its summer recess.

Meanwhile, in Washington, D.C., lawmakers allowed a portion of the USA Patriot Act to expire in early June and then passed the U.S. Freedom Act, which leaves it to phone companies, rather than the federal government, to gather and store metadata – the numbers called and the time and length of calls – but not content.

U.S. officials will be able to access the data only after securing a warrant from a special court. According to an article in the *Christian Science Monitor*, a panel of civil liberty advocates will argue for privacy at the special court. The government has until the end of the year to make the transition.

RISK MANAGEMENT

NIST Releases Draft on Privacy Risk Management

The U.S. National Institute of Standards and Technology (NIST) recently released for public comment the draft “Privacy Risk Management for Federal Information Systems,” which, among other things, establishes a common vocabulary and a risk model for assessing privacy risk in information systems.

“Risk management methods provide systematic ways to identify and address risk and have proven effective in areas such as cybersecurity, safety and finance,” says Naomi Lefkowitz, senior privacy policy advisor at NIST. “We see a great deal of potential for these methods to help agencies design and manage federal information systems that minimize risks to privacy.”

Lefkowitz told *LegalTech News* that the impetus for the framework stemmed from a need to deal



with the challenges of protecting personal data.

“The first trigger was internal, we’re working on research concerning Big Data, smart grid, cybersecurity, and Internet of Things, and one thing they all have in common is there are implications for privacy. We had a need to think about how to consider privacy implications of these technologies in a consistent and repeatable, and measurable way,” Lefkowitz said. “We are the mea-

surement agency after all.”

The framework focuses on best practices for the internal production and processing of private information. It leaves guidelines for dealing with cyber attacks and information recovery to cybersecurity research.

The comment period for the draft, which was available at http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf, was to close on July 13, 2015.

E-DISCOVERY

Courts Continue to Endorse Predictive Coding

Technology-assisted review (TAR), also known as predictive coding, continues to gain the support of federal courts. Magistrate Judge Andrew J. Peck of the U.S. District Court for the Southern District of New York, one of the first judges to endorse TAR, recently proclaimed that the right to use TAR for high-volume electronically stored information (ESI) cases is “now black letter law,” reported Bond Schoeneck & King PLLC. Peck’s statement was part of his discussion in *Rio Tinto PLC v Vale S.A., et al.*

The court’s growing acceptance of TAR is expected to affect all

producing parties in future cases, regardless of whether they would prefer to use traditional keyword searching instead of predictive cod-



ing. “As more courts tout the precision of TAR, requesting parties are ever more likely to demand that producing parties use this sophisticated technology to ensure that the maximum number of responsive documents are being unearthed,” predicted Bond Schoeneck & King.

In large-volume ESI cases in which TAR would be appropriate, it may be wise to use the technology from the start and develop a protocol to ensure the selected technology is both defensible and transparent, the attorneys advised. It would maximize cost-savings and minimize the likelihood of expensive discovery disputes.



90/70

The percentage of large and small-to-midsize UK businesses, respectively, that has suffered an information security breach.

Source: *Information Security Breaches Survey 2015, PwC*

CYBERSECURITY

Cost of UK Cybersecurity Breaches Doubles

The average cost of the worst single security breach experienced by UK businesses of all sizes has risen sharply over the last year, according to the Information Security Breaches Survey 2015 commissioned by the UK's Department for Business, Innovation and Skills (BIS). Breach costs include elements such as business disruption, lost sales, recovery of assets, and fines and compensation.

Costs have more than doubled for larger businesses (more than 500 employees), ranging from £1.46 million to £314 million (about

\$2.2 million to \$4.7 million, U.S.) as compared to £600,000 to £1.15 million (\$900,000 to \$1.7 million) the prior year. Smaller businesses didn't fare much better as the average cost climbed to £75,000 to £311,000 (\$112,500 to \$466,500) from £65,000 to £115,000 (\$97,500 to \$172,500) in 2014.

The type of attacks didn't show such dramatic change. The majority of them (60%) came from external threats for larger businesses, 38% for smaller businesses. That compares to 55% and 33% in the 2014 report.

When asked specifically about

the cause of the worst breach experienced, 50% were the result of inadvertent human error, up from 31% in 2014. That's even though 72% of large businesses and 63% of smaller businesses provide ongoing security awareness training for their employees.

To assist businesses in their efforts to secure their data, the UK government has issued "10 Steps to Cyber Security" advice sheets. They offer guidance in a variety of areas, including information management, security management, network security, and user education and awareness.



ELECTRONIC RECORDS

NARA Creating Registry for Controlled, Unclassified Information

The National Archives and Records Administration (NARA) is nearing completion of rules for managing the extensive volumes of controlled, unclassified information (CUI) the U.S. government generates. Reflecting input from agencies, the new rules establish 23 categories and 82 subcategories of CUI in a registry, with links to the statutory or regulatory basis for keeping the information under wraps, reported *FCW*.

Comments on the rules were due to NARA by July 7. The final rules are expected before the end of this year, at which time a three-to four-year phased implementation will begin. The greatest change for agencies is that they will need to mark CUI documents prior to dissemination rather than after. NARA is developing a marking handbook with input from agencies.



CYBERSECURITY

India Wants to Become Cybersecurity Hub

In March, India Prime Minister Narendra Modi called on his country's IT industry and youth to help address the global cyber-

security challenge. Three months later, the industry's lobby group Nasscom announced it was heeding the call and had formed the Nasscom Cyber Security Task Force with its goal to make India the hub of cybersecurity research, training, and products, reported the *Economic Times*. It will present a comprehensive cybersecurity plan within the next year.

"This task force will study the Indian cyber security ecosystem to identify issues and challenges and develop an action plan to address the priority issues," said BVR Mohan Reddy, chairman of Nasscom. "It will also identify possible intervention opportunities for the Indian IT industry in global cyber security space and bring together stakeholders from across the board to develop cutting-edge technolo-

gies and address the global market requirements."

The task force will include four working groups focused on industry development, policy enablement, technology development, and skill development, the *Economic Times* article stated. Their recommendations will be the foundation for the country's cybersecurity plan.

In the meantime, the National Cyber Security Policy of India strives to create a half-million skilled cybersecurity workers in India by 2018. The number of cybersecurity professionals is increasing, but quality is the major concern.

"The challenge is finding that ultra-specialized group of people [in cyber security]," said the task force chair, Rajendra Pawar. This challenge exists not only nationally, but globally.



Your Connection to RIM & IG Products and Services

BUYER'S GUIDE ONLINE!

Looking for a software solution, records center, or archiving supplies? The **2015-2016 Buyer's Guide for Records Management and Information Governance Professionals** is the place to start!

ARMA International's online listing of solution providers puts the power of purchasing at the click of your mouse.

www.arma.org/buyersguide

Want to advertise in the online Buyer's Guide?

Contact Karen Lind Russell or Krista Markley at Karen.Krista@armaintl.org today!



CYBERSECURITY

Survey Cites Human Error as Biggest Cause of Data Breaches

External cybersecurity breaches get the headlines, but evidence points to human error as a greater cybersecurity threat for organizations of all sizes.

A data security incident response report released in May by BakerHostetler revealed that in the 200-plus cases its firm advised on in 2014, human error was the top cause of data security incidents. Employee negligence was responsible 36% of the time, while theft by outsiders was 22%, theft by

insiders 16%, malware 16%, and phishing attacks 14%.

While the healthcare industry was affected most – largely due to strict data breach notification laws healthcare providers must follow – no industry is immune from threats to its sensitive information.

“It is important for companies to understand that data security is not just an issue for retailers, financial firms and hospitals. Incidents do not only occur at businesses that have payment card data or protected health information. Privacy and data security issues are firmly entrenched as a significant public and regulatory



concern and a risk that executive leadership and boards of directors must confront,” stated the report’s authors.

Other findings noted in the report include:

- Not all security lapses involved the theft or hacking of electronic records; 21% involved paper records.
- 58% of the incidents required notification of affected individuals, based on state breach notification laws.
- Credit monitoring was offered in 67% of the incidents.
- In 75 incidents where notification letters were mailed, only five of the companies faced litigation by potentially affected individuals.
- For incidents involving stolen payment card data, PCI Data Security Standards fines for non-compliance ranged from \$5,000 to \$50,000 per matter. Initial demands for operating expense and fraud assessments ranged from \$3 to \$25 per card involved.

“Our analysis shows that best-in-class cyber risk management starts with awareness that breaches cannot be prevented entirely, so emphasis is increasingly on defense-in-depth, segmentation, rapid detection and containment, coupled with ongoing effort to monitor threat intelligence and adapt to changing risks,” the authors advised.



RECORDS AND INFORMATION MANAGEMENT

AU National Archives Issues RIM ‘Capability Matrix’

Because managing an organization’s records and information is each employee’s responsibility, the National Archives of Australia developed a “capability matrix” that outlines the skills and knowledge each one needs to enable an organization to transition to fully electronic information management and ensure its information assets remain accessible and usable over time.

“Rapid advances in technology, the growing volume of information, and the increasing complexity of the online environment all mean that Australian government Agencies face significant challenges in managing their business information,” stated Director-General of National Archives David Fricker when announcing the matrix, as reported by *PS News*.

The matrix addresses the capabilities for all staff, for information communication technologies specialists, and for records and information management specialists and is designed to be used in conjunction with the Australian Public Service Commission Integrated Leadership System, which has a stronger focus on behaviors.

The Challenges of Cross-Border Discovery

Global organizations are increasingly finding themselves in a difficult position in their attempts to address cross-border discovery.

If they comply with U.S. data preservation obligations, they could violate the rights of employees, customers, or other individuals under EU and other countries' international data protection laws. But, if they abide by individual countries' data protection laws, they risk potentially devastating spoliation sanctions in U.S. courts, explained e-discovery experts Jeane Thomas and Brad Davis in a recent *Corporate Counsel* article.

Bridging that gap is challenging, if not impossible. Thomas and Davis offered some practical steps counsel could take before and after litigation to minimize the conflict.

- **Retain records only as long as required by law or business necessity.** This will limit the volume of personal data that may be subject to preservation requirements.
- **Institute a litigation-readiness program.**
- **Educate foreign business units with the concept and requirements of U.S. discovery.**
- **Foster transparency.** "Advise employees through policies and specific notices that the company may be required to preserve and collect work-related email and other data containing personal information in the event of U.S. litigation or an investigation."
- **Ask for consent.** It may not be considered sufficient under foreign law, but explaining to affected employees why you need access to their data and what you intend to do with it and asking for their written



consent "demonstrates respect for foreign data protection laws and the employee's individual rights."

- **Preserve data in place.** Avoid "imaging, harvesting, relocating or otherwise altering the data," particularly before you know what's needed.
- **Tailor legal holds, particularly for non-U.S. custodians.** Instead of issuing a company-wide legal hold, ask the necessary custodians to preserve data related to a particular transaction, activity, or issue.
- **Address foreign data-preservation issues with opposing counsel.** Discuss ways to limit the scope of non-U.S. data preservation obligations by narrowing discovery requests and focusing on available U.S. sources first.
- **Ask the court for a stipulation or court order.** This should address "limitations and requirements for the preservation and production of non-U.S. personal data, including restrictions on use and dissemination of the data and providing confidentiality and security protections."
- **Release preservation measures as early as possible.** Once you know non-U.S. data is no longer subject to U.S. preservation obligations, return it to normal data management practices.

CYBERSECURITY

Employee Cybersecurity Training Tips

Hackers prey on the most vulnerable links in your company's security – your employees. That's why they use *phishing* e-mails, malware-laden messages that appear harmless to the untrained employee's eye. It's imperative for organizations to train their employees in the best cybersecurity practices. Entrust, an identity-based security solution provider, suggested the following basic practices for all employees:

Avoid any e-mail that asks for username/password information – even if it's on their personal device. Connecting an infected personal device to the company network can infect other devices on the network. No legitimate service or website will ask users to transmit sensitive account-related data over e-mail. Make it clear that employees should enter sensitive data only on sites that have been administratively vetted or after consulting with IT.

Have open discussions about cybersecurity around the office. The most important step in getting people to be proactive about an issue is to promote awareness about it. Just setting aside five to 10 minutes at a company-wide meeting to discuss emerging threats and to share safe computing tips from the IT team can make a huge difference.

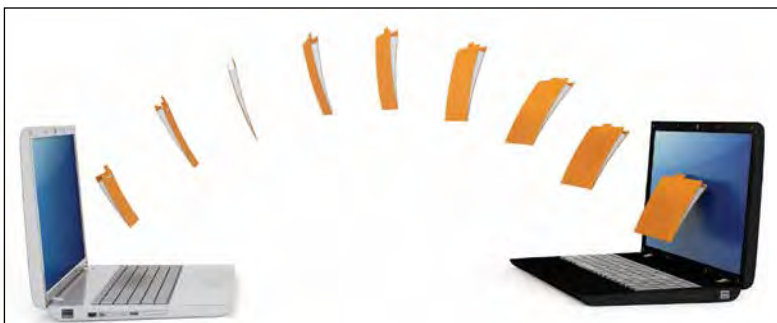


CLOUD

The Top Trends Driving Cloud Use

There are many ways to leverage the cloud. Some can make you a hero, others can be disastrous. To understand both scenarios, it helps to look at how others are using the cloud. According to a recent *Cloud Computing Magazine* article by Mike Chase, J.D., executive vice president and chief technology officer for the cloud service provider dinCloud, some of the top trends are:

- Virtual offices for disaster recovery – Companies intent on staying in business no matter what are leveraging the cloud to relieve concerns about the effects of such emergencies as environmental disasters, global terrorism, criminal activity (internal and external), and shifting legal/political landscapes. Setting up virtual offices with servers, desktops, file shares, and everything synced to the cloud can make business continuity easier.
- Desktop as a service – The cloud can offer so much more than the typical enterprise desktop. There are fewer licensing headaches and the cloud may have functionality that is not even available at the enterprise level.
- Regulatory relief – “Cloud has become the best way to meet new regulatory challenges because regulatory requirements around physical facilities hosting sensitive customer data can be a real drain on time/money/resources,” stated Chase. “Security guards, cameras, logs, man-traps, cages, availability, become a real headache.”
- Security – Cloud-based security can be licensed monthly and is scalable. There also is a huge marketplace of cloud-based tools from which to choose. Leveraging the cloud can provide a depth of security not possible at the enterprise level.
- Mobile – The cloud makes it easy to tie servers, desktops, and cloud storage to an existing Microsoft Active Directory, keeping full policies and permissions intact across most, if not all, mobile devices.



EHRs

Overcoming Health Information Blocking

The ability to share medical records electronically is a critical element in creating an effective healthcare system. So, why isn't it happening? According to a recent *New York Times* article, too often it's because that transfer is being blocked by the developers of the technology or "greedy medical centers that refuse to send records to rival providers."

The Office of the National Coordinator for Health Information Technology (ONC) recently presented a report to the U.S. Congress about the issue and provided criteria for identifying it and distinguishing it from other barriers to interoperability. ONC stated that it's difficult to assess the full extent of the problem, especially because of contractual restrictions imposed by software developers on their clients.

According to the report, ONC is already taking steps to target, deter, and remedy information blocking, including strengthening in-the-field surveillance of health IT certified by ONC. Many of the requirements for certification are aimed at enabling information-sharing between systems. Tightening standards is another step being taken.

"One of the most effective ways to reduce information blocking is to promote transparency in the health IT marketplace," the ONC told Congress. "Providing customers with more reliable and complete information about health IT products and services would make developers more responsive to customer demands and help ameliorate market distortions that enable developers to engage in certain opportunistic and other behavior that raises serious information blocking concerns."

The office also noted that congressional action may be needed to address some issues that are beyond the reach of current federal law and programs.

E-MAIL

E-Mail Overload Has Predictable Results

Knowledge workers today are dealing with e-mail overload, a perception that they send, receive, and process more e-mails than they can handle, find, or process on a daily basis. Interestingly, on average, those

who receive 100 or more e-mails each day can respond to only about 5% of them, according to a report on a recent study of 2 million users exchanging 16 billion e-mails over several months, "Evolution of Conversations in the Age of Email Overload."

In short, the researchers found that "as users receive more email messages in a day, they reply to a smaller fraction of them, using

shorter replies," and they often reply faster.

Some of the key findings of the research, as summarized in a blog post by the Information Governance Initiative (IGI), were:

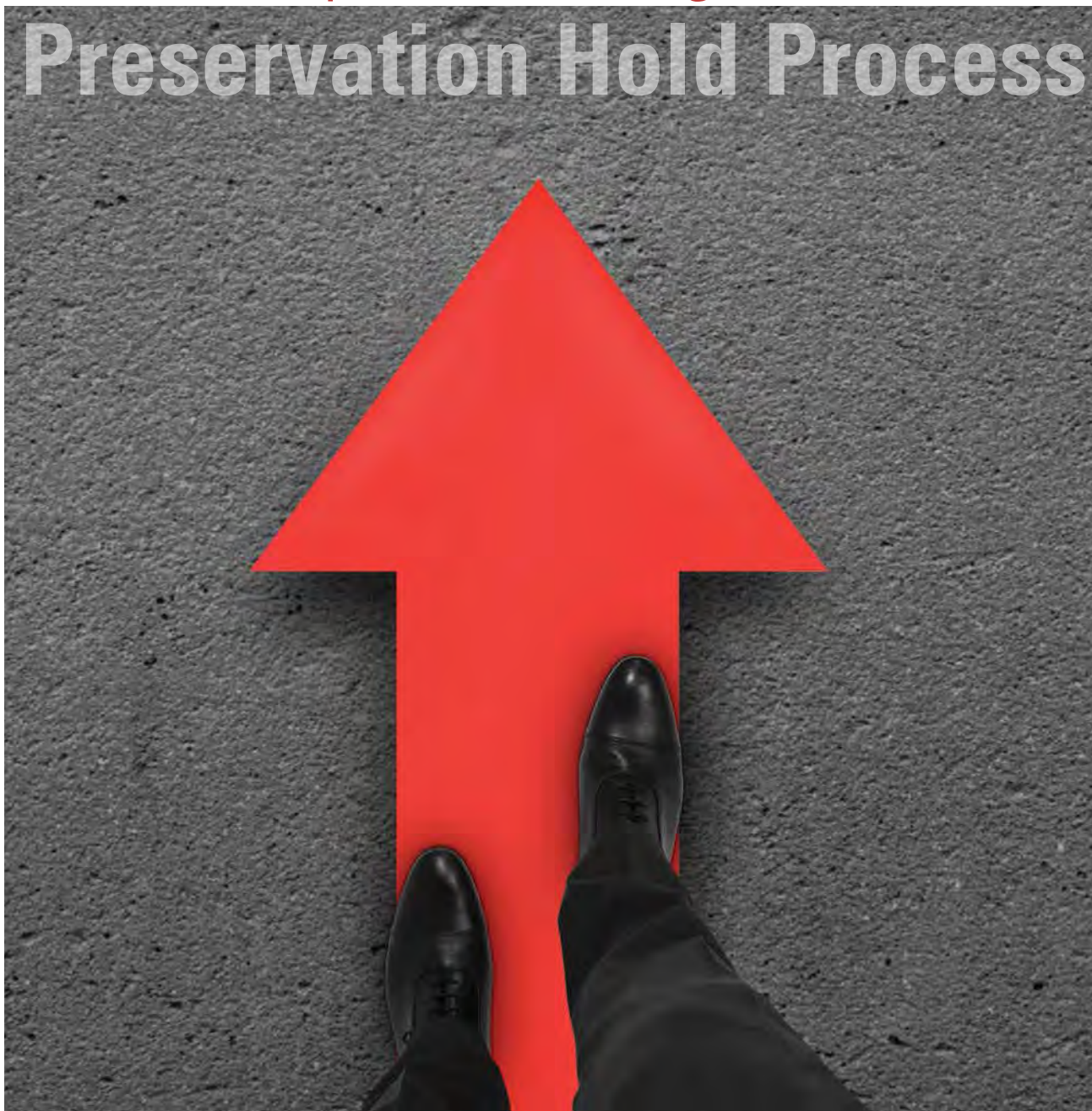
- People generally reply quickly to e-mails, most often within an hour of receiving a message.
- Younger users reply faster to messages than their older peers, and they send shorter responses.
- Women are slightly more affected by e-mail overload than men, but the difference is negligible.
- E-mailing behavior is predictable; the research team was able to forecast the time and length of a reply, as well as when a conversation between two people will end with high accuracy.

"These findings could be used in designing better email clients that help people deal with email overload," Farshad Kooti, a Ph.D. student at the University of Southern California who conducted the research with four colleagues, told IGI.

The full report can be accessed at <http://arxiv.org/pdf/w1504.00704v1.pdf>. **END**



Critical Steps to Creating a Consistent Preservation Hold Process



Richard Vestuto, J.D., and Bill Piwonka

Many organizations struggle to develop a cost-effective and defensible hold process. This article provides six steps to help organizations plan, automate, and communicate a legal hold process that will improve efficiency, reduce risks, and meet their preservation obligations.

Any organization subject to large, complex, high-stakes lawsuits or investigations requires a repeatable process for preserving potentially relevant electronically stored information (ESI). Yet for many organizations, the preservation process is often chaotic, time-consuming, and error-prone. This is often because they rely on disparate technologies or manual processes to support preservation efforts, with potential mistakes occurring due to poor coordination and sloppy hand-offs. These errors are frequently amplified by the many complexities and challenges that can complicate preservation efforts.

One such challenge is dealing with employee status changes. Employees go on leave, move to new positions or different business units, or depart the organization altogether. While employee movement is a routine element of modern business life, it takes on critical significance in the context of e-discovery, where failing to properly track employees can result in data spoliation and severe sanctions.

Having a legal hold process that preserves data throughout the e-discovery life cycle – from initiation to release and data deletion – is critical. This article walks through several critical steps for creating a consistent preservation hold process.

Step 1: Understand the Legal Hold Life Cycle

At its most basic level, a legal hold is a form of notification, often an e-mail, informing the recipient that a lawsuit has been commenced or is reasonably anticipated and that the party receiving the e-mail must preserve all data potentially related to the subject matter of the case.

While the basic process of issuing, monitoring, and documenting legal holds is fairly similar across many organizations, priorities for preserving ESI vary depending on the organization's size, type, and industry. Large organizations typically have hundreds

or thousands of employees that are dispersed geographically and spread among a number of business units. The legal team needs to be able to create, acknowledge, and track legal holds efficiently. Simply sending out a legal hold notification e-mail does not equate to a defensible process.

Basic Steps

Following are basic steps organizations should consider to help ensure a defensible preservation process:

1. Confer with key stakeholders, including information technology (IT) and human resources (HR), to confirm that every person related or potentially related to the legal matter understands the scope of the preservation obligations.
2. Suspend any automatic deletion or purging of e-mail and other key information systems by taking these actions:
 - a. Pull current backup tapes from rotation or recycling to ensure data is preserved without risk of spoliation.
 - b. Identify any laptop/desktop backup routines running on a scheduled basis and archive the most recent backups.
 - c. Stop recycling or reissuing hardware.
 - d. Stop purging user accounts and individual network shares for departed employees.
3. Issue legal hold notices when litigation is reasonably foreseeable, which is usually before notice of suit is given.
 - a. Write the notice in "plain English," describing the nature of the matter and the issues at hand.
 - b. Give clear instructions to employees not to modify, destroy, delete, or hide any electronic or hard copy data related to the commenced or anticipated litigation or investigation, including all paper or ESI, other data stored on the company's

computer systems and storage media, or any other electronic data.

- c. Take steps as early as possible to preserve data from user-assigned laptop/desktop computers and mobile devices.
4. Interview the key players subject to the legal hold to confirm they understand their legal obligations as well as to get their help identifying other employees or data that may be subject to the preservation obligation.
5. Remind employees of their preservation obligations on a regular schedule to facilitate compliance.

Issue legal hold notices when litigation is reasonably foreseeable, which is usually before notice of suit is given.

The legal hold must remain in place until final disposition of the underlying matter.

6. Release the hold as soon as the underlying matter is resolved. This allows the electronic evidence to be deleted according to the company's regular retention policies, assuming it's not subject to preservation obligations on another matter.

Key Stakeholders

Legal holds occur at the very crossroads of an organization's people, processes, and technologies. They also intersect with business units across the organization, including legal, IT,

records management, HR, and compliance, among others. As with any business-critical practice, it is important that basic legal hold requirements are communicated to each business unit and that each knows its specific role in the process.

It's also important to establish a steering committee comprising these stakeholders to help ensure the organization's preservation protocols are applied consistently on every matter, while not disrupting other business processes. This will help arm counsel with the critical details needed for

... it is important that basic legal hold requirements are communicated to each business unit and that each knows its specific role in the process.

effective case negotiations, including the backup system status, relevant search terms, date ranges, and other qualifiers that can narrow the scope of discovery. It will also empower IT and records management to facilitate the defensible deletion of ESI when it no longer has business or legal utility. The committee should be chaired by a C-level executive to help ensure recommendations are incorporated into policy.

Step 2: Avoid Common Preservation Mistakes

Many legal hold mistakes can be traced back to the common causes described below.

Poor Custodian Identification and Tracking

This includes failing to diligently identify all likely custodians when litigation becomes reasonably expected and not conducting effective custodian interviews to learn more about the case or other potential custodians.

Poor Data Source Identification

If an organization doesn't know where the data resides or who has access to that data, it will most likely fail to properly preserve it. Data residing on file shares, detachable drives, and third-party systems can often be overlooked. Don't forget to examine these common enterprise data sources that are often subject to discovery:

- **Employer-Controlled Sources**
 - E-mail servers (mailboxes of individual e-mail users)
 - File servers and print servers (including individually assigned network stores or "home shares")
 - Network drives ("group shares" accessed by multiple individual users)
 - Archival data on backup tape or other storage media
 - E-mail journaling systems
 - Document management systems
 - Proprietary structured databases (e.g., databases containing HR, customer, or sales data)
 - File shares and other web-based collaboration sites
 - Social networking sites and services/accounts used and maintained by the company
 - Video and audio systems (e.g., voicemail)
 - Legacy data (e.g., ESI generated by computer programs no longer used by the company)
 - Hard copy document archives maintained by the company (including offsite storage)
 - ESI maintained in hosted databases in connection with

prior litigations / investigations

- **Employee-Controlled Sources**
 - ESI found on user-assigned laptop/desktop hard drives, including word processing, spreadsheets, images, and other text-based files
 - Locally stored e-mail archives (user-archived PSTs, OSTs)
 - Individual backup and temp files
 - Internet usage data (e.g., cookies)
 - Portable storage media (e.g., user-controlled external hard drives, flash drives, CD/DVDs)
 - Company-issued mobile devices (e.g., cell phones, tablets)
 - Hard copy documents maintained by the employee
 - Cloud-based storage
 - Social media and personal e-mail accounts

Poor Hold Discipline

Examples of this are issuing legal holds verbally, sending a written hold notice without any follow-up notices, and not escalating to a custodian's superior when the custodian is non-compliant.

Poor Communication

Issuing a legal hold without enough details to the custodian or stakeholders, for example, can result in custodian non-compliance or omission of potentially relevant ESI.

Lack of Protocols

Established protocols are critical to ensuring data sources are protected and for preventing ad hoc approaches for identifying ESI, search criteria, online and offline repositories, and employee status changes.

Step 3. Understand Legal Ramifications of Failure

A lack of planning, an over-reliance on manual, error-prone methods, and poor communication between

IS INFORMATION YOUR ALLY OR YOUR ENEMY?

**NEXT
LEVEL™**

**> information
governance
assessment**

Your business data is doubling by the year. And all this new data can either help you or hurt you. Find out what it's doing for your company with the Next Level Information Governance Assessment. You'll discover areas of strength and opportunities for improvement. In the end, you will be empowered to increase organizational transparency and data integrity while decreasing risk.

Start turning information into an asset by visiting arma.org/nextlevel.

various stakeholders involved in the preservation process can lead to severe sanctions; courts have made it very clear that ignoring the problem no longer works. The two recent case law examples below reinforce the importance of having solid preservation practices.

Failure to Preserve Employee Data

A leading IT services company was embroiled in a discrimination claim with the U.S. Equal Employment Opportunity Commission (EEOC). The company terminated an employee who had filed a claim in November

Automation can help prevent the legal and IT teams from making preservation mistakes, as well as save time, promote consistency, and improve communication.

of 2009, and he filed a second EEOC charge in December of 2009, claiming he was terminated in retaliation for his discrimination claim.

The terminated employee had worked remotely, and all or nearly all of his data was located on his work laptop, which he returned to the company upon termination in December. The company subsequently wiped the laptop and reissued it to another employee the following month.

A couple of years later, the terminated employee filed a discrimination suit against the company under 42 U.S.C. § 1981 and state civil rights laws. The company did not issue a

legal hold until three months later. Additionally, a year later, the employee's former supervisor also left the company, and he later testified that he did not back up any of his own data before returning his laptop. Apparently, the data was lost.

The company claimed that the data sought by the employee was not stored centrally at the company; later that assertion was contradicted by testimony by company witnesses. The employee alleged that the company deleted responsive data on both his laptop and his supervisor's laptop and moved for sanctions.

The court found that the company was grossly negligent in its duty to preserve and granted an adverse inference instruction with respect to the data stored on the laptops. The terminated employee's request for sanctions was granted in part and denied in part. The company was not sanctioned for the destruction of data on the employee's computer, but the court issued an adverse inference instruction for the spoliation of the data on the supervisor's hard drive.

Failure to Interview Custodians

In a litigation involving two drug manufacturing companies, in two separate opinions, the court addressed the obligations with regard to the preservation and collection of data and the obligation of counsel to obtain input from relevant custodians.

In the first opinion, the court ordered an extensive forensic examination of the plaintiff's data by a neutral third party and crafted a protocol for production of the data identified by the applied search terms.

In the second opinion, the court confirmed a basic rule that counsel must carefully craft the appropriate keywords, with input from the custodians, as to the words and abbreviations they use. The court ordered counsel to obtain search word input from all custodians and to pay a portion of the attorney's fees awarded.

Step 4: Eliminate Manual Processes

Automation is one area where technology becomes indispensable to a defensible, efficient preservation process. Preservation requirements tend to change over time. For example, as more custodians are added to a legal hold, the complexity and the effort required to manually track the process increases exponentially. A single custodian may interact with five or six data sources.

Automation can help prevent the legal and IT teams from making preservation mistakes, as well as save time, promote consistency, and improve communication. Areas of the preservation process that can be automated include:

Creating Legal Hold Notices

Users should be able to automate the legal hold process by leveraging customized templates that are created based on case type or legal objective and can be reused on similar matters.

Automating Custodian Interviews

Surveys can help custodians better understand their preservation obligations, as well as help the legal team learn more about the matter and its potential scope. Having the system automatically send out the interviews may eliminate the need to recreate interviews for every new matter and allow responses to be added to the system of record automatically.

Tagging Notices

Tags, or identifiers that attach to a preservation notice, such as a brief description of a matter or the matter name, can be automatically attached to all relevant preservation notices to eliminate tedious, repetitive, and error-prone information entry and inform both IT and legal across matters to avoid repeat of work.

Establishing Workflows

Establishing automated workflows

can ensure approvals are received at specified steps in the preservation process before moving forward. They can also ensure copies of holds and interviews are automatically issued to designated recipients. For example, organizations should be able to set up an automatic process to ensure that an attorney approves a hold notice before it's issued and approves the interview before it goes out.

Sending Reminders, Escalation Notices

It's important to keep in mind that recipients of legal holds have day-to-day business responsibilities and will likely need to be reminded of their hold obligations from time to time. The preservation system should allow the legal team to automate such notices on a predetermined schedule, as well as escalate them to supervisors to help ensure that non-responsive custodians take a requested action.

Step 5: Track Employee Changes

When an employee departs an organization, it is common practice for IT to delete, reimage, or destroy the individual's data from local devices, as well as shared servers, and reissue the equipment to someone else. What often gets overlooked in the process is that the departed employee may have been subject to a preservation obligation, which persists regardless of whether the person is actively employed at the organization.

While departing employees may present the greatest risk for inadvertent data spoliation, it's important to recognize that other employee status changes, such as extended leaves of absence, departmental transfers, relocations, promotions, or even last name changes can also warrant corrective action.

It's important to track all employee movement to prevent data spoliation. Technology is advancing to automate this process. By integrating

the organization's HR and e-discovery systems, the legal team can eliminate the manual, time-consuming review of daily spreadsheets issued by HR and automatically be alerted of employee changes requiring corrective action, as can IT and other impacted business units.

For example, if an active custodian is changing departments, legal may respond by simply updating its records to reflect the change and send a reminder e-mail to the employee so he or she knows that the terms of the legal hold still apply.

Or, if an employee is leaving for maternity/paternity leave, IT needs to be notified to ensure that the systems and data won't be compromised as a result of the prolonged absence. This type of information can also help legal and IT understand why data volumes vary greatly during discovery – potentially explaining away suspicions of missing data or spoliation.

Step 6: Be Proactive and Educate

One of the easiest countermeasures to data spoliation is awareness and education. It's critical that legal teams educate their counterparts in HR and IT, as well as other employees, that preservation obligations persist.

In some work environments, it works well to have a single member of each team participate in regular, in-person meetings, which help promote a more active, engaged dialogue around the key issues. Ultimately, the goal is to come up with a plan that strikes a balance between the organization's legal obligations and its desire to minimize operational expenses. To get started in developing this plan, it's important to take the following steps.

Understand the Data Landscape

Gain a level of familiarity and comfort with the organization's data landscape, including an understand-

ing of the nature and location of key data sources, a strong working relationship with important IT contacts who can assist in getting to relevant ESI, and a general sense of the significant data risks and issues that may arise as a result of the format or location of certain ESI.

Talk to Custodians

The duty to preserve potentially relevant ESI applies to all custodians, including those who may have had only a passing encounter with the central issues in the litigation. Custodians not only have the relevant data,

**...keep in mind
that recipients of
legal holds have
day-to-day business
responsibilities
and will likely
need to be
reminded of their
hold obligations
from time to time.**

they also have information that can be extremely valuable in tracking down other responsive ESI and developing a case strategy. To be effective, the custodian interview process should be conducted in a consistent, repeatable manner to help ensure that the resulting information can be easily processed and acted upon.

Document the Process

Make it a priority to document the preservation process. Having a documented process fosters a culture of communication and efficiency because team members know exactly what's expected of them and under-

AIEF Scholarships Now Available

- **Graduate education scholarship** *Deadline: August 15* – **\$3,000**
- **Access Leadership scholarship for undergraduate education**
Deadline: August 15 – **\$2,000 & \$6,000**
- **Undergraduate tuition reimbursement** *Deadline: August 15* – **\$1,000** per semester
- **RIM continuing education reimbursement** – **\$750**
- **RIM certificate/certification reimbursement** – **\$500**
- **Arizona Chapter scholarships for CRM certification/IGP certification reimbursement** (*Pacific Region only*) – **\$500**

**ARMA INTERNATIONAL
EDUCATIONAL FOUNDATION**

Apply today!

www.armaedfoundation.org



Donate to the AIEF at www.armaedfoundation.org

stand their tasks in the context of larger objectives. In the event that e-discovery mistakes do occur, a well-documented process can also mitigate repercussions by demonstrating that the mistakes were likely not systemic in nature, but rather were simple, isolated oversights.

Result: A Cost-Effective, Defensible Process

Preservation obligations are generally well understood by corporate legal teams. Where many organizations struggle is in developing preservation processes that help ensure these obligations can be sufficiently met in a defensible, cost-effective fashion. Many legal hold mistakes can be traced back to a lack of planning, an over reliance on manual, error-prone methods, and poor communication between various stakeholders involved in the process. By following the steps listed above, organizations can effectively modernize their preservation processes, thereby reducing risk and improving efficiency.

Note: This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication. Deloitte does not provide legal services and will not provide any legal advice or address any questions of law. **END**

Richard Vestuto, J.D., can be contacted at rvestuto@deloitte.com. Bill Piwonka can be contacted at bill.piwonka@exterro.com. See their bios 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 (CRM) demonstrates that you have the experience and expertise to lead change and deploy best practices as they evolve in the RIM profession.

For more information about becoming a Certified Records Manager, **contact (518) 694-5362** or visit www.icrm.org



The Principles and External Audits

Julie Gable, CRM, CDIA, FAI

External audits depend on documentation, and that can make them stressful, time-consuming, and psychologically draining for records and information management (RIM) professionals who have to produce the documentation quickly. Learn how to prepare and respond to an audit and how basing your RIM program on the Generally Accepted Recordkeeping Principles® can reduce the strain and deliver good results even when under intense scrutiny.

Third-party audits are a fact of life for organizations large and small. Some audits are limited in scope. A U.S. Department of Labor audit, for example, reviews employee job classifications and wage rates. Tax audits, on the other hand, encompass all income and all expenses and are generally broad in scope. Even non-profits are subject to audits by grant-makers who want to ensure that their funds are well spent.

Regardless of type, third-party audits have several aspects in common. The auditors must form an opinion of how, and how well, an organization conforms to the laws or standards that govern it. Auditors rely on direct observa-

tions, overall impressions, and first-hand inspections during onsite visits that can last from days to weeks. While on the premises, auditors test an organization's compliance or non-compliance by gathering evidence in the form of records and documentation. In the process, every principle of good recordkeeping will come under scrutiny.

Even though the outcome of an external audit is a judgment on company-wide compliance, the audit processes themselves are often the ultimate test of an information governance (IG) program. As the examples will show, this is particularly true for audits conducted in regulated industries. (See sidebar "SEC, FDA Regulatory Audits.")



Timing Is Everything

Though regulatory audits may be purely routine, they may be triggered by newspaper headlines, litigation, consumer complaints, or wrongdoing by other organizations in the same sector.

Audits may also be a surprise. At best, the U.S. Securities and Exchange Commission (SEC) gives a two-week notice for an impending visit. The U.S. Food and Drug Administration (FDA) may give no notice at all and simply appear at the reception desk. Like pop quizzes, external audits, even expected ones, are measures of what has been done to date.

An IG program based on the Generally Accepted Record-keeping Principles® (Principles) and the Information Governance Maturity Model (IGMM) goes a long way to show that the organization takes its information management responsibilities seriously. Used well, these comprehensive tools guide in developing and sustaining an IG program that delivers reliably during even the pickiest inspections.

Work guided by the Principles also provides a number of spillover benefits that become very handy during the audit process. Finally, understanding the Principles can also uncover potential problems, which are best handled before an audit occurs.

IG Bedrock Principles

The Principles of Compliance, Accountability, and Transparency are the bedrock of the IG program and the backdrop against which audit scenarios unfold. In industries where information is a crucial part of the company's end product – financials and pharmaceuticals, for example – what affects IG affects the overall entity, as shown below.

Compliance

IG compliance requires the organization to review all applicable laws, regulations, codes of conduct, and ethics that apply to it. An organization makes and maintains records to prove that it does business in accord with these, and its policies reflect how it interprets them in their operations.

These internal policies impose a duty of compliance on the organization and its personnel, and auditors will test this. A common audit finding is that the company is compliant with the applicable regulations but out of compliance with its own policies, including its IG policies.

Transparency

Transparency means documentation of procedures and processes, something that auditors always want to see. This may be an investment manager's hard-copy compliance manual, or it may be the drug company's controlled set of standard operating procedures.

Either way, it's critical to have orderly documentation for policies and processes, to be able to show that the

SEC, FDA Regulatory Audits

Audits are particularly stringent in industry sectors where regulators have a duty to protect the public. In financial services and pharmaceuticals, for example, the stakes are high, and poor audit results can have severe business consequences. Investment advisors may lose their licenses; drug makers may be prevented from operating manufacturing plants.

With regulatory audits, size does not matter. In 2012, the Securities and Exchange Commission (SEC) began its "Presence Exam" initiative among newly registered investment advisers, many of whom are either independent small businesses or autonomous groups under the aegis of a major corporation.

Audits for these companies can include employees' use of social media; client communications via e-mail and texts; and brochures and advertising, including websites. Auditors check to see whether required records about trades, powers of attorney, custody, investment supervision, proxy voting, and personal trading are kept.

Auditors typically want to see client lists by account type and asset value, accounts opened or closed within a given period, pricing and quotation services, purchases and sales journals, chronological trade lists, and so on. They also want to see the company's own compliance manual to evaluate how well it adheres to its own policies.

The Federal Food, Drug and Cosmetic Act mandates the U.S. Food and Drug Administration (FDA) to inspect domestic drug companies at least once every two years. Inspections done prior to marketing approval for new drugs are particularly comprehensive, covering such topics as management controls, development processes, corrective and preventive actions, and production and process controls. Inspectors may test compliance with standards for good laboratory, clinical, and manufacturing practices.

The supporting materials for all of these are records. Standard operating procedures spell out what must be done, and records made and collected at each phase show what was actually done. FDA inspectors may enter, observe, collect samples, interview employees, and review any records – with limited exceptions – related to the regulated product.

documentation is reviewed and updated periodically, and to be able to prove that the version presented is, in fact, the latest one. In FDA parlance, "If it's not documented, it's rumor."

How Audits Work

- Depending on its type, the audit may come with or without advance notice.
 - Up to five inspectors usually arrive together.
 - Most organizations assign the auditors to a conference room, making sure there is no writing on the whiteboard, flipchart easel, or other surfaces for the auditors to see.
 - One or more people from the company – a compliance manager in financial services, for example, or a quality assurance manager in pharmaceuticals – will be assigned as the liaison for the auditors.
 - Auditors request records through the company liaison. The liaison will contact the appropriate internal persons with the request. Each of these may, in turn, have to contact others to find the requested information. Runners may actually ferry documents among sites.
 - All retrieved information goes to the liaison, who, in turn, gives it to the auditors. The liaison also keeps a copy of anything provided to the auditors, as well as a log of all requests made. At the end of each day, the liaison prepares a summary of what was requested and the topics discussed.
 - If a requested record or document can't be found, auditors will almost certainly want to dig deeper to understand why. The auditors may want to understand company systems and processes in more detail to determine where the inability to provide the document is a procedural failure or indicates a more serious breach. They may also want to examine retention and disposition policies and procedures.
 - Auditors can also conduct interviews as a way to compare actual practice with the company's documented policies and procedures. Interviewees should answer exactly what is asked and only what is asked. This can be particularly difficult with information management questions because an explanation of the system or method may be necessary to put the answer in context.
-

Accountability

Accountability says responsibility for records should be delegated to individuals and that defined roles and a chain of command should be established. For IG managers in large, multi-site companies, it can be particularly helpful in audit scenarios to know who their counterparts are at other sites and what records they manage.

In very small companies, there may be no chain of command; each department may take care of its own records, which is a dangerous practice when it comes to finding the “official” copy of a requested document. (See sidebar “How Audits Work.”)

Explicit and Tacit Principles

Compliance, transparency, and accountability are explicit values that produce tangibles easily evaluated during an audit. The Principles of Availability, Integrity, Protection, Retention, and Disposition are tacit – that is, their presence or absence is implied in the handling of an auditor's every information request. The following are audit considerations for these “tacit” Principles.

Availability

Even though information may be well organized, the company may not have standard organization methods at each of its sites. Consequently, a simple request for a particular document may require multiple phone calls to people who know how to find this document in their own disparate systems.

Furthermore, there may be multiple copies of requested documents, and they may not all be the same version, so it will take time to ferret out which one should go to the auditor. The more time that elapses, the greater the impression that records are not readily available.

Integrity

A key point in some audits is that electronic systems that produce records actually produce the same results every time. This can apply even to Excel macros, with the need to prove, usually through validation records, that the macro is documented and has been tested thoroughly.

Audit trails, and records of how often audit trails are checked, also play a part in ensuring that records are unalterable. Record dates, in particular, should not change from system to system as they move through the chain of custody. Where third-party archiving services are used, as for customer communications in financial services, it is wise to have a letter from the third party stating how integrity of information is maintained.

Protection

A financial firm's client accounts will contain many fields of personally identifiable information and it is important to understand how this should be redacted in the course of an audit. In addition, requested documents may contain privileged, secret, or classified information, so it is important to know what the ground rules are for providing these. If auditors take photographs, it is advisable for the company to take the same photographs to ensure that no protected information is inadvertently captured.

Audit Survival Guide and General Advice

Orderliness counts. Don't leave records, files, or boxes strewn about; such disorder gives the appearance of disregard for good organization and protection. Auditors are forming a general impression from the moment they arrive.

Mum's the word. Make sure that all staff are aware that auditors are on premises and therefore they shouldn't discuss company business or the audit itself in elevators, hallways, cafeterias, etc. Make sure that everyone receives notice when the audit is completed. One company actually announces "Elvis has left the building" when the auditors depart.

Be flexible. An audit is an all-hands-on-deck situation. If the auditors opt to work late, staff responsible for fulfilling information requests must also work late. Make sure your staff knows where to find things and whom to call at other sites. Vacations can be disrupted by an audit.

Don't try to cover or hide deficiencies. It is better to acknowledge them and have a plan in place to correct them. Corrective action taken while the auditors are onsite can have a positive effect.

Courtesy and cooperation are the watchwords. This holds true at all times but is especially important during audits when nerves may be frayed by endless critical scrutiny. Remember that this too shall pass – hopefully in about a week.

Retention and Disposition

The Principles of Retention and Disposition may be assets or liabilities in the audit process. Retention schedules are policy documents that can legitimately justify why requested material is not available, and disposition records are proof that the organization had the requested materials at one time, but in the due course of business and in accordance with retention policy they were destroyed.

Needless to say, there should be a documented process for attaching a disposition hold to documents that are needed for audit purposes. Those organizations whose policy is to keep everything forever will find that they are expected to find anything that is requested, and those who suspend disposition of all records because of litigation may find that they are cited for being out of compliance with their own policies.

Audits and the IGMM

The higher an organization's level of maturity on the IGMM, the better its audit results will be, right? Perhaps, but even organizations operating an IG program with a maturity of 4 or 5 have no way of knowing how well that

program will actually work under audit conditions.

For example, the organization may be at a level 4 for availability and have inventories of all systems, but some acquired legacy systems may not be part of the inventory. Sure enough, auditors request reports from a legacy system, sending many people scrambling to find them.

This is a real challenge in industries where there have been several mergers and acquisitions over a period of years. It is one reason why those who have a duty to preserve electronic records for long periods opt to establish electronic archives where crucial information of long-term value can be indexed, stored, protected, and available.

What is certain is that adopting the IGMM can't hurt. It provides a standards-based way to demonstrate that the company has a strategy in place to constantly improve IG elements. If nothing else, benchmarking against the IGMM gives the impression that the company takes its governance responsibilities seriously and works toward improvement goals as a matter of course, not just in response to audit findings.

Audits = Stress + Opportunity

The value of being prepared and knowing what to expect during an audit cannot be overstated. Working on an IG program guided by the Principles will automatically provide some of what is needed for audit success. Other strategies include reviewing a regulator's audit manuals to have a better idea of what will be sought and speaking to peers who have weathered the process in other companies.

Some organizations use internal audits or opt to use independent, third-party auditors to uncover deficiencies before regulatory audits occur. There are also seminars about the audit process that are tailored to those who work in regulated industries.

Even with excellent preparation, don't expect praise. Audits are stressful, time-consuming, and often done from a negative perspective. The auditors' mission is to discover faults. Remember that an art critic could find faults in the Mona Lisa. This is one reason why audits can be so psychologically draining. It helps to keep in mind the general guidelines described in the sidebar "Audit Survival Guide and General Advice."

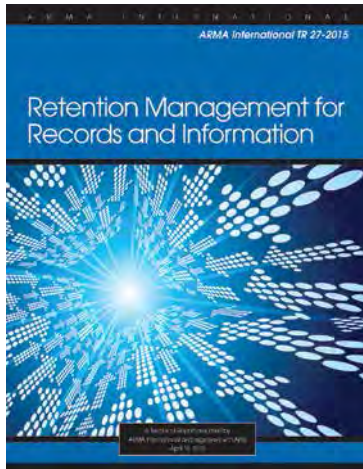
Finally, even audit outcomes that are less than stellar can be beneficial. Audit findings must be corrected, and IG and records management, as always, tend to get much attention after a calamity occurs. Take advantage of the spotlight to get what is needed for your program. A not-so-great audit may be the kick that gives the IG program the boost it needs to move to a higher level of maturity, making for a better program – and better audits – in the future.

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



NEW!

Resources for Advancing Your Career



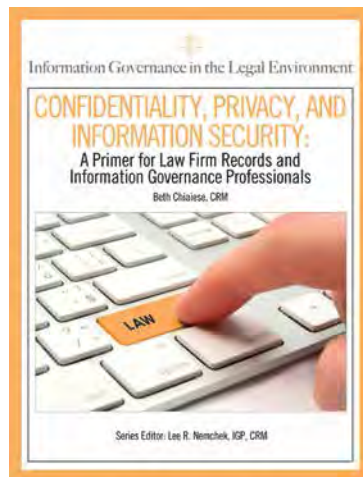
Retention Management for Records and Information

(ARMA International TR 27-2015)

This technical report, which replaces the 2005 guideline by the same title, covers activities pertinent to managing the retention of records and information – regardless of media or format – in accordance with business needs and associated legal/regulatory requirements. PDF version also available.

A4969 Soft cover **\$60.00** Professional Members: **\$40.00**

V4969 PDF **\$55.00** Professional Members: **\$35.00**



Confidentiality, Privacy, and Information Security: A Primer for Law Firm Records and Information Governance Professionals

Beth Chiaiese, CRM

This third monograph in our Information Governance in the Legal Environment Series provides an introduction to topics that U.S. law firm records and information governance (IG) professionals must be familiar with in order to establish IG programs that effectively protect confidential and private information. PDF version also available.

A4973 Soft cover **\$60.00** Professional Members: **\$40.00**

V4973 PDF **\$55.00** Professional Members: **\$35.00**

Order online today! **BOOKSTORE** ARMA INTERNATIONAL

www.arma.org/bookstore

RIM's Role in Harnessing the Power of Big Data

Kevin L. Dale, CRM

Organizations can maximize the returns on their big data strategies by giving records and information management (RIM) professionals a seat at the table. Applying RIM principles across the enterprise will help organizations improve the quality of their data and access to it, making big data analysis cheaper, quicker, more efficient, and more accurate.



Organizations are struggling to extract value from their exploding, exponential information growth. Many are turning to big data analytics to mine the gold from the data they store. But are they really positioned to mine for gold using a systematic and controlled approach, or are they simply punching holes in

the ground and hoping to strike oil? If they strike gold, are they doing their due diligence to ensure sustainable results?

Too often, RIM is the missing ingredient in this big data conversation.

Technology Is Not Enough

While data analytics software can perform complex algorithms that help

predict outcomes from enormous data sets, these tools alone cannot determine if the data being evaluated is of sufficient quality to provide the most accurate results. Organizations often must first make significant investments in preparing the data for analysis, scrubbing or normalizing the data set for missing or bad values.

In fact, Thomas Davenport, a well-

RIM also can play a role as part of the gating process for introducing technology.

known information management and analytics expert, wrote in the *CIO Journal* article “Taming the ‘Data Plumbing’ Problem,” “It is often so difficult to extract, clean, and integrate data that data scientists can spend 90% of their jobs doing those tasks.”

The organization has to pay data scientists or analysts a tremendous amount just to determine the structure of columns and rows within poorly defined structured data tables in order to apply the variables to the statistical software. And they may also need to do several costly iterations of mining unstructured data just to identify key repetitive text that can be evaluated for its relevance because the data often lacks sufficient context that comes with good metadata.

Most organizations have a records and information management (RIM) department with skilled professionals who know how to apply RIM principles to the information landscape. They accomplish this by inventorying where all of the organization’s data exists, establishing a data map, and understanding the business processes that result in data. Big data can partner with RIM to reduce the costs of identifying, preparing, and analyzing data.

This is why organizations seeking to leverage big data tools to make better business decisions are advised to invite RIM professionals to the conversation.

RIM Reduces Costs, Adds Value

Experienced RIM professionals can help solve big data problems because they know how to organize data to meet RIM requirements, use a naturally consultative approach to help-

ing business units understand how to manage information throughout its lifecycle, and know how to drive improvements – all things that will benefit the analytics team.

By creating synergies between RIM and the big data program staff and integrating RIM principles into all processes that “touch” data, organizations can forge and maintain a sustainable path to the information governance (IG) needed to ensure high-value data. This will reduce costs and add value to the big data program, by:

- Reducing data cleanup and preparation
- Reducing storage costs and risks
- Improving the identification of data through good metadata
- Improving access to data
- Increasing employee efficiency
- Producing better, analytic-driven decision making

RIM Controls ‘Four Vs of Big Data’

Through a systematic approach to IG and the application of RIM principles, skilled RIM professionals can help improve the “four Vs of big data”:

- Volume – How much data there is
- Variety – The locations and types of data
- Velocity – How much streaming data is being generated
- Veracity – The quality of data

Volume

The more information there is, the more it costs to manage and analyze it. A mature RIM program can help trim data analysis costs by reducing extraneous data through proper retention and disposition processes.

For example, RIM establishes requirements to ensure that appropriate de-duplication occurs in unstructured data repositories. This means the analytics team will have to sift through less poor-quality data, thus lowering the costs of obtaining the data, reducing the time to evaluate it, and enhancing the results since duplicate information won’t be included to skew the results.

RIM also can help the big data program be more efficient by ensuring that data in different life cycle stages remains identifiable and retrievable. For example, RIM can identify and locate relevant data in storage locations the analytics team may not know about.

Variety

RIM programs have a consolidated inventory of the repositories where data resides. It also can develop controls that slow down or prevent repository creation, such as collaboration sites and shared drives, thereby mitigating the risk of proliferation of uncontrolled repositories and the associated big data costs.

A systematic approach to allowing new data repositories can help ensure that data is appropriately controlled for information-related risks and that any new repositories are added to the data map so the big data analytics team will always have a current view of everywhere data resides.

RIM also can play a role as part of the gating process for introducing technology. RIM should work with application development and other technology teams to embed RIM requirements for technology that will impact the creation and storage of data.

The procurement team also needs to understand the RIM requirements for new tools that create and store data. It must inform RIM when any tools are decommissioned and ensure that contracts with third-party service or product providers address how the organization can keep control of

its data so it is appropriately retained and managed when a contract expires or a tool is no longer supported

Finally, RIM should enlist the sponsorship of senior leaders to drive the alignment of RIM principles within IT processes. Big data teams should define and embed the role of RIM within their own governance documents to cement this valuable relationship.

Velocity

The proliferation of high-speed data collection sensors is a major contributor to the big data opportunity, and devices that lack sufficient IG are a major contributor to big data risks. Fast data doesn't have to mean *uncontrolled* data, though. Applying RIM principles will:

- Ensure that the data's structure and storage format enhance and maintain the data's value
- Ensure the data is organized and actively managed during all phases of its life cycle
- Reduce the risks posed by the data

RIM teams are invaluable partners for analytics teams because RIM knows how information is flowing through and being used by the organization. This level of business understanding is a key tenet of data science; data scientists need to know if others are adding information to the data, manipulating it, or creating additional repositories.

A RIM and big data partnership can decrease the time it takes data scientists to identify and understand an organization's information flows, which once again drives down big data program costs and improves results.

Veracity

Organizations that are going to invest in a big data strategy should have improving data quality as a primary goal. Poor data quality is an obvious challenge to a big data initiative and a drain on resources. It doesn't make

sense for an organization to hire a big data analytics team, identify poor-quality data repositories, and then do nothing to improve them.

This is where the big data team can help RIM; it can communicate where poor-quality repositories are and recommend practices that will enable the analytics team to harvest better quality data. Examples of poor quality data are:

- That which has little or no meta-data
- Duplicate information
- Missing or insufficient data

Applying RIM principles to these repositories will improve the data's content, context, and structure.

reviewing e-mail as evidence is risky because a message can easily be taken out of context, resulting in creative conclusions about its true meaning. The same holds true for data analyzed in the course of a big data project.

Unstructured data by its very nature lacks sufficient context to permit understanding its true meaning without performing a word analysis on common terminology used within it or comparing it with similar documents. Even then, the level of confidence is often tens of percentage points away from 100%.

RIM can establish controls around data that will improve its context. The primary ways are through the

Organizations that are going to invest in a big data strategy should have improving data quality as a primary goal.

The Importance of Integrated Data Governance

Integrating a big data-RIM governance approach with solid RIM principles ensures that new processes, procedures, and technologies are aligned with requirements to manage the data life cycle. This will improve the data's content, context, and structure, allowing the organization to extract big data value by the most cost-efficient means possible.

Improving Data Quality

One way RIM principles can improve the quality of data is to prevent its unauthorized alteration or deletion. The end goal is to have a greater level of confidence in the results of analytics, knowing that they are performed on data sets that come from well-controlled repositories.

Ensuring Data Context

Everyone knows that context matters. During litigation, for example,

labels in structured data tables and the metadata in unstructured data. RIM must be empowered to drive standards for the labels and metadata of all organizational data that can help data analytics teams. For example, it should include fields that identify data owners so the big data team can quickly get from the owners any needed permissions to access their data.

Defining Data Structure

By working with the big data team, RIM can establish a governance approach to drive the design of file plans that will structure data and metadata so the data is easily accessible to be pulled into analytics software, facilitating its analysis. Empowering RIM professionals to establish enforceable standards for file plans will provide a repository structure that reduces risk, decreases storage costs, and improves analytic alignment.

Implement an enterprise-wide policy that defines the roles and responsibilities for each employee.

File plans for unstructured data are usually developed using records management and enterprise content management systems, although data may also reside within shared drives and collaboration environments that lack any coherent file plan. This means the storage and file plan structures for data should be aligned with content management and data analysis software requirements where possible.

How to Align Big Data and RIM Governance

One way to begin a big data-RIM alignment is to establish two groups – an IG council that makes strategic decisions on standards for driving big data-RIM requirements throughout the organization and prioritizes work, and a big data-RIM workgroup that is responsible for doing the work.

Establishing an IG Council

The IG council should develop and advance the strategic goals of the big data and RIM program throughout the organization. It should be composed of senior leaders from RIM, IT, information systems, legal, enterprise risk, audit, compliance, governance, and finance. It might also include members from sales, marketing, customer service, and communications if, for example, the nature of big data strategy involves predictive analytics to drive sales.

The IG council must be empowered to decide how data is governed to mitigate RIM-related risks in parallel with enhancing the effectiveness of data analytics. For example, the council would ensure that as poorly structured data sources are identified,

the resources to mitigate them are quickly made available.

The council must be visible to the entire organization and consistently communicate the importance of managing data as an asset.

Establishing a Big Data-RIM Workgroup

A big data-RIM IG workgroup should be made up of front-line management from RIM, data analysts, and key IT and business partners. It is responsible for the tactical functions the IG council has mandated and prioritized.

This group aligns managing information with the needs of the analytics team and the business units, is tasked with accomplishing initiatives in a timely manner, and reports its progress to the IG council on a regular basis.

Institutionalizing the Approach

Establish charters for the IG council and the big data-RIM governance workgroup, clearly identifying each group's mission, vision, purpose, roles and responsibilities, goals, and metrics. Institutionalize their activities through documented governance.

Implement an enterprise-wide policy that defines the roles and responsibilities for each employee. Reaffirm the policy each year and provide refresher training.

Each business unit should contribute to the transparency of the RIM programs by establishing and enforcing a procedure for communicating new repositories to RIM. They should also perform quality assurance on and oversight of the data they produce, use internal metrics in validat-

ing their quality control programs, and assign liaisons to ensure that business-level governance is followed.

Benefits of a Big Data-RIM Governance Framework

Adopting an integrated big data-RIM approach gives organizations a competitive advantage over organizations using big data analytics alone because the latter approach does not lend itself to the types of sustainable improvements necessary to continue to enhance the quality of and access to data.

A big data-only approach will also fail to reduce information-related risks. In time, the costs and risks associated with poor-quality data residing in uncontrolled repositories will eat away at any competitive advantage and become a significant liability. The costs of delaying a big data strategy that includes RIM principles will also increase exponentially with data growth.

Organizational leaders should aggressively seek to mitigate these risks and rethink their big data strategies to include RIM principles. By making this shift, they will reduce poor-quality data and increase their confidence level in their big data analysis results.

Better results should lead to better decision making and increased profits. Employees and the data analytics team will benefit from their ability to identify and access data in a timely manner, which will improve organizational efficiency in the use of its data while driving down information-related risks.

By leveraging a big data-RIM approach to establishing requirements to control the proliferation of information, the organization will reduce the costs associated with storing, mining, and analyzing that data. And that's just good business. **END**

Kevin L. Dale, CRM, can be contacted at kevin.dale@chi.frb.org. See his bio on page 47.

**PREX15****September 16-18, 2015**

Sharpen your skills and advance your knowledge of the legal preservation process with comprehensive sessions, nationally recognized experts and ample opportunity for peer-to-peer learning. We expect this one to sell out quickly. Use the PREX200 promo code to receive \$200 off your registration fee. Register now at www.prex15.com to secure your spot.

**OPEX CORPORATION**

From document conversion services to mobile scanning to digital mail centers, Falcon™ is the only prep-reducing scanner on the market to combine all your scanning needs into one universal document scanning workstation. Falcon allows operators to prep and scan documents at a faster rate than most current prep-only processes. For more information visit www.opex.com.

**IRON MOUNTAIN**

Sharpen your skills and advance your knowledge. Download the RIM Best Practices Guide today at ironmountain.com/BestPractices. Protecting your information is key to the success of your business, so why take the risk of not protecting it properly? Check out the RIM Best Practices Guide and discover the practical approach to building a comprehensive and compliant RIM program.

**SHERPA**

Records and information management professionals are faced with the monumental challenge of locating, organizing, and managing electronic data. How do you manage something that large and complex? Where do you start? With a mountain of data to scale, you need a guide with the right tools. You need a Sherpa. Contact Sherpa Software to reach new heights in managing ESI.

www.sherpasoftware.com

IS YOUR INFORMATION GOVERNANCE PROGRAM A HOUSE of CARDS?

ARMA LIVE! RETURNS OCTOBER 5-7 TO WASHINGTON, D.C.



www.arma.org/conference



Planning for and Managing During a **Paper Document Disaster**

William R. Gulley, Jr

The disaster recovery and restoration industry in the United States is big business, and to the detriment of those who need such services, business is good.

Whether disasters are natural or man-made, one thing is certain: storms, fires, and floods happen practically every day, and they are costly. According to statistics on the Insurance Information Institute website, insurance payouts for U.S. natural catastrophe losses totaled \$15.4 billion in 2014 and for domestic man-made catastrophes were \$12.9 billion in 2013.

Imagining a Common Scenario

Imagine 1,000 records center containers soaked by sewage water. Empirical data from industry veterans indicate that the treatments required to restore them to usable, as near to pre-loss condition as possible, can *easily* cost a quarter of a million dollars.

Now imagine those records belong to your company or organization. Moreover, they are permanent, warrant long-term retention, or are mission-critical. Because they do not exist elsewhere in any format, these records must be salvaged by restoring the paper.

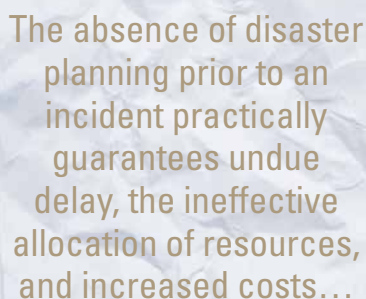
Imagine having either no insurance to cover the costs of recovery or coverage that falls short in fully funding restoration. Having an exorbitant amount of insurance coverage may not be a panacea, either, as the amount of coverage and the amount the insurance company is actually willing to pay out on a loss claim may not be the same. The payout may hinge on the impression the organization makes on its insurance carrier. An adjuster that sees evidence of poor records management may challenge why it is necessary to recover these materials.

The ramifications of these scenarios, with respect to business continuity and fiscal solvency in forcibly absorbing this type of loss, are staggering.

Beginning with a RIM Foundation

While the importance of carrying proper insurance coverage in the event of a disaster cannot be overstated, records and information management (RIM) professionals must do more than just review their organization's insurance policies and hope for the best.

An organization that can show it maintains physical and intellectual control over the records it creates and holds; has clean and organized stacks, file rooms, and storage areas; monitors its storage conditions, including its temperature and humidity; and has kept its building in good repair is more likely to have a favorable insur-



The absence of disaster planning prior to an incident practically guarantees undue delay, the ineffective allocation of resources, and increased costs...

ance settlement. In addition, these best practices that existed before the disaster promote an economy of movement in response to emergency conditions.

Certain preparations need to be made before disaster strikes, specifically, developing a thorough disaster plan that includes measures that will enable an organization to resume or maintain operations while the recovery unfolds. In short, the better prepared an organization is *before* a disaster, the quicker it will recover from the incident.

Note: *Because of space constraints, the scope of this article is limited to developing a basic disaster plan, using it to recover from a disaster that involves wet paper records, and managing the recovery.*

Developing a Basic Disaster Plan

The absence of disaster planning prior to an incident practically guarantees undue delay, the inefficient allocation of resources, and increased costs once the event occurs. Every organization needs a disaster plan that is up-to-date, readily accessible, disseminated throughout the organization, and easily understood.

A well-thought-out disaster plan contains realistic scenarios that depict varying types of incidents (fire, water damage, contamination) and the steps necessary to mitigate their effects. Like following a plane's pre-flight checklist, following the plan ensures that important things are not overlooked. Following are some of the basic topics that must be addressed in a disaster plan.

Roles and Responsibilities

As the "game plan" for handling various incidents, a disaster plan has a "team roster" that identifies the players and their responsibilities. This includes, of course, third-party vendors and service providers. For example, the plan might describe these roles and responsibilities:

- Facilities management will abate standing water.
- The emergency services contractor will bring in fans and dehumidifiers.
- The document restoration contractor will remove and restore damaged paper records.
- Facilities management will move furniture, equipment, and other contents after records have been removed.
- The general contractor will do general cleanup, debris removal, and demolition (removal of wet wallboard, carpeting).

Information Value, Location

Having intellectual and physical control over record holdings is crucial to a good disaster plan. For example,

the organization must document:

- The size or volume of its holdings in linear or cubic feet
- A list of all records series
- The value of its records and in what priority they are to be recovered. For example, vital records, which are critical to business continuity, and materials with long-term or permanent retention should have the highest priority.
- The location of records to be recovered
- The format of records to be recovered

The well-prepared organization is one that knows, literally, what records are in which box and which

shelf each box is on, regardless of the total number of boxes or storage locations.

The plan must include floor plans and office diagrams that show what records are stored where. It is important that the building itself, rooms, and cubicles are clearly marked with numbers or occupants name that mirror the information on the floor plan.

Having this information readily available will assist decision-making and optimize recovery efforts, saving both time and money.

Alternate Office Site

What many organizations overlook in contingency planning is their potential need for a “hot site” or “cold

site” – an alternate facility equipped either with or without computers (hot site and cold site, respectively) – and other resources they will need to resume operations quickly.

Unless there is no reliance on hard copies, temporary central file rooms, stack areas, etc. might need to be set up and undamaged paper records relocated so they will be accessible while the damaged office space is repaired.

Communication Plan

A disaster plan should include an organizational phone tree so everyone affected by the event can be notified. Although smart phones are commonplace and many people routinely send and receive e-mail on mobile devices, it might be a better idea to call people (or at least leave a voice mail message) in addition to sending out a general e-mail. Remember, it may not be possible to reach people by e-mail if the incident brought down the organization’s network.

Responding to an Environmental Disaster

The organization’s role in a disaster’s aftermath is to follow its plan, adjust measures and actions as necessary, and see the plan through to completion. Incorporating the following actions into the plan are critical.

Determine Site Safety

In the aftermath of a fire or a flood, there likely will be contaminants. The smoke residue and black carbon soot from partial-combustion fires can contain multiple types of corrosive acids and carcinogens. Similarly, storm surge, floodwater, and sewage contain a host of impurities.

Contact an industrial hygienist or environmental testing company (which should be listed in the disaster plan) and have the area tested. Do not allow anyone in the disaster area unless testing declares it safe or protective equipment measures have been determined and are implemented.



Giving Back to Information Professionals

- *Innovative Research*
- *Scholarships*
- *Training and Certification Grants*

AIEF

**ARMA INTERNATIONAL
EDUCATIONAL FOUNDATION**

Donate today!

www.armaedfoundation.org

Touch Base with Contractors

If possible, have a general briefing or meeting where all parties involved with the recovery – internal and external – are brought together. Although the contractors listed in the disaster plan should have been thoroughly vetted as part of your organization's selection process, ask questions about their processes and their projected progress. Good contractors should be able to articulate what they will be doing, why they will be doing it, and how long it should take.

Document recovery, general site cleanup, and damage abatement can proceed remarkably fast if they are coordinated properly and contractors' efforts are unimpeded.

Limit Access to the Disaster Area

When notifying office staffers of the incident, set a location and time for them to assemble as a group to be briefed on the situation. They will need their active files and items from their desks, so give them a specific time when they will be allowed – as a group – to have access to their areas to retrieve them. For safety and liability reasons, materials inside the affected area should not be released until they have been verified as safe to handle.

Best practices favor a controlled site versus a “revolving door” where people are allowed to enter freely and mill about. After the staffers' window of opportunity to visit expires, the site should be declared off limits to everyone except document recovery and contractor personnel and relatively few people from the organization. Allowing others onsite could put them in danger and interrupt document recovery operations and other contractors' work.

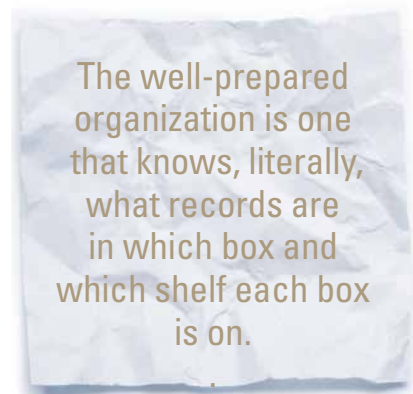
Establish a 'No Touch' Policy

The results of environmental testing often provide a lot of good reasons to refrain from touching damaged documents. Conditions range from plain old nasty to downright harmful

or dangerous. For these reasons, it is highly recommended that only document recovery personnel handle damaged records and that a “no touch” rule applies to everyone else.

Do not touch or move contaminated materials without protective equipment, and don't move them to an unaffected area of the disaster site, as this could cause cross-contamination.

If files must be moved by persons other than document recovery specialists, have them move only the dry documents and leave the wet ones, as these can be easily damaged if handled or moved improperly. It's also important to maintain the records' original order and not allow them to stray from their offices of origin.



Restoring Documents

A document restoration contractor provides two vital services: physical records recovery, as discussed above, and restorative treatment. The contractor will respond to the incident, find the damaged paper records, and remove them. This is commonly referred to as a “pack out,” and the purpose is to prevent further damage by removing materials from the scene. In addition to removing damaged materials, a conscientious document recovery company will strongly recommend removing undamaged records from any site with environmental conditions that pose a threat.

This is particularly time-sensitive when water is involved; per the U.S. Environmental Protection Agency's

“A Brief Guide to Mold, Moisture, and Your Home,” wet records should be dried within 24-48 hours of water exposure due to the risk of mold. The same tenet applies when smoke, soot, mold, and other contaminants are involved, as dry paper will absorb moisture and contaminants from the environment.

Because time is of the essence, records removal should be done as soon as the affected areas are accessible and ahead of all other abatement and repair work. This will prevent potential further damage to wet paper records.

After the contractor takes the damaged records to a document treatment facility, their physical condition will be assessed and a treatment regimen that will mitigate or reverse the damage will be recommended and executed.

For records tainted by sewage, for example, typical restorative measures include dehydration (specifically, water removal by vacuum freeze-drying), decontamination, deodorization, and surface cleaning. Document restoration also may include physical replacement of folders and boxes.

Succeeding By Design

The absolute, worst-case scenario would be to have a disaster without having a disaster plan. Akin to possessing adequate insurance to fund the costs of document restoration, the importance of a well-crafted disaster plan also cannot be overstated.

Best when coupled with money to fund recovery efforts, the plan states how the recovery will be conducted, but the organization must manage the process, making adjustments as necessary as the situation progresses. Only then will its response to the incident be effective – and it will not be by luck, but by design. **END**

William (Bill) R. Gulley, Jr. can be contacted at Bill.Gulley@ers-us.com. See his bio on page 47.

Records Management or Information Governance?

William Saffady, Ph.D, FAI



Editor's note: This article was excerpted from the upcoming third edition of *Records and Information Management: The Fundamentals of Professional Practice*, which will be published by ARMA International this fall. Taken from Chapter 1, which examines the purpose and scope of records management as a business discipline, it defines records management and information governance, placing records management within the context of an information governance program.

Records management is a specialized discipline that is concerned with the systematic analysis and control of information created, received, maintained, or used by an organization pursuant to its mission, operations, and activities. By definition, records management is concerned with information that is recorded or “written down” as opposed to merely memorized or exchanged verbally.

A comprehensive records management program includes policies, procedures, and processes that ad-

dress significant recordkeeping issues, specifically:

- Determining how long recorded information needs to be kept to satisfy an organization's requirements
- Ensuring compliance with recordkeeping laws and regulations in all locations where an organization has business operations
- Managing inactive records in a cost-effective manner
- Organizing active records for retrieval when needed

- Protecting recorded information that supports mission-critical business operations

These programmatic aspects are embodied in Generally Accepted Recordkeeping Principles® (Principles), which were issued by ARMA International in 2009 to foster general awareness of records management systems and standards and to assist organizations in developing effective programs for records management programs and information governance. The set of eight recordkeeping principles are paraphrased below:

Accountability

A senior executive should be in charge of the records management program. The accountable executive will delegate program responsibility to appropriate individuals, adopt records management policies and procedures to guide program personnel, and ensure that the program can be audited for compliance. A governance structure must be established for program development and implementation.

Transparency

An organization's recordkeeping processes and activities must be documented in an open and verifiable manner. Such documentation must confirm that the organization's recordkeeping policies and practices comply with applicable legal requirements and accurately and completely reflect the organization's activities. The documentation must be available to employees and appropriate interested parties.

Integrity

An organization's records must have a reasonable and suitable guarantee of authenticity and reliability. Recordkeeping processes, including audit processes, must provide reasonable assurance that the origin, time or creation or transmission, and content of recorded information are what they are claimed to be.

Records management is an important component of an information governance program, but it is not the only component.

Protection

An organization's records management program must protect records that are private, confidential, privileged, secret, or essential to business continuity. Recordkeeping procedures must provide appropriate protection controls from creation through final disposition of recorded information.

Compliance

An organization's records management program must comply with applicable laws, regulations, industry-specific rules of conduct, and other binding authorities related to creation, storage, retrieval, retention, disposition, dissemination, and protection of recorded information, as well as with the organization's own recordkeeping policies, procedures, and rules.

Availability

An organization's records must be organized, indexed, stored, and maintained in a manner that ensures timely, efficient, and accurate retrieval of information when needed.

Retention

An organization must retain records for an appropriate period of time to satisfy legal, regulatory, fiscal, operational, and historical requirements.

Disposition

An organization must provide secure and appropriate disposition for records that no longer need to be kept. In this context, disposition may involve destruction of records, transfer of records to another organi-

zation as part of a divestiture or other transaction, transfer of records to an archives or other scholarly repository, or transfer of records to clients or other parties who are the subjects of the records.

Records Management and Information Governance

According to the *OECD Glossary of Statistical Terms*, which was assembled by the Organization for Economic Cooperation and Development from documents issued by various international organizations, *governance* is the process by which decisions are made and implemented.

ISO/IEC 38500, *Information Technology – Governance of IT for the Organization* defines *governance* as “a system of directing and controlling.”

ISO/IEC TR 38502, *Information Technology – Governance of IT – Framework and Model* defines a *governance framework* as the “strategies, policies, decision-making structures and accountabilities through which the organization's governance arrangements operate.”

Similarly broad definitions are presented in other ISO standards – such as ISO 21500, *Guidance on Project Management*, and ISO/IEC 27000, *Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary* – and in various other sources, including dictionaries of business terminology.

Building on these definitions, *information governance* can be viewed as a system for directing and controlling an organization's information assets. As such, information gover-

Information governance is a collaborative initiative that requires the involvement and expertise of multiple stakeholders.

nance is a component or subset of organizational governance. Published definitions provide additional details.

ARMA TR 22-2012, *Glossary of Records and Information Management Terms*, for example, defines *information governance* as “a strategic framework composed of standards, processes, roles and metrics that hold organizations and individuals accountable to create, organize, secure, maintain, use, and dispose of information in ways that align and contribute to the organization’s goals.”

The American Health Information Management Association (AHIMA) defines *information governance* as “an organization-wide framework for managing information throughout its lifecycle and supporting the organization’s strategy, operations, regulatory, legal, risk, and environmental requirements.”

According to the *Commentary on Information Governance* issued by the Sedona Conference in December 2013, *information governance* is “an organization’s coordinated, interdisciplinary approach to satisfying information compliance requirements and managing information risks while optimizing information value.”

ISO/TS 14265, *Health Informatics – Classification of Purposes for Processing Personal Health Information* and ISO/TR 11633-1, *Health Informatics – Information Security Management for Remote Maintenance of Medical Devices and Medical Information Systems – Part 1: Requirements and Risk Analysis* define *information governance* as “processes by which an organization obtains assurance that the risks to its information, and

thereby the operational capabilities and integrity of the organization, are effectively identified and managed.”

An *information governance framework*, sometimes described as an information governance model, defines strategies, policies, decision-making structures, and accountabilities for creation, storage, use, analysis, distribution, disclosure, retention, disposition, and protection of information.

Records management is involved, to some degree, with all of those information-related activities. Records management is an important component of an information governance program, but it is not the only component.

Information Governance Stakeholders

Information governance is a collaborative initiative that requires the involvement and expertise of multiple stakeholders. Adapting a definition presented in ISO/Guide 73, *Risk Management – Vocabulary*, a *stakeholder* is a business unit or a functional area that is involved with or affected by an organization’s information assets.

In addition to records management, information governance stakeholders include, but are not necessarily limited to, information technology, information security, risk management, legal affairs, compliance, risk management, and the individual departments or other organizational units that have recorded information in their custody or under their supervisory control.

An information governance framework specifies roles and responsi-

bilities that promote interaction, cooperation, and consultation among the following stakeholders, which are widely acknowledged to play key roles in defining the strategic direction for management of information assets in government agencies, companies, not-for-profit entities, and other organizations.

Records Management

Records management develops and communicates policies, procedures, and guidelines for lifecycle management of an organization’s information assets as discussed in subsequent chapters. Information governance is not synonymous with records management, which focuses on the day-to-day execution of specific operations or activities that involve recorded information. These operations and activities are performed within the strategic framework defined by information governance.

Information Technology

Information technology creates and operates the technological infrastructure for processing, storage, retrieval, and distribution of an organization’s information assets. It optimizes the utilization of technological resources for cost-effective management of information assets, provides backup protection and disaster recovery capability for recorded information, and provides the technological expertise and support required to implement information management policies developed by other stakeholders.

Information Security

Information security deals with issues related to confidentiality, data protection, and disclosure of an organization’s information assets. It develops and communicates data protection and privacy policies to prevent unauthorized access to recorded information, monitors and evaluates situations or events that may threaten

information assets, responds to security breaches that involve recorded information, and works with other stakeholders to identify information assets that require special security arrangements.

Risk Management

Risk management identifies, analyzes, and quantifies risks that may affect, are attributable to, or are otherwise related to creation, storage, retrieval, distribution, disclosure, retention, disposition, or protection of an organization's information assets. It develops and communicates policies and procedures to mitigate the adverse impact of specific information management policies and practices.

Legal

Legal affairs is concerned with legal issues and concerns that relate to recorded information. It reviews record retention policies and schedules for legal acceptability. It establishes and communicates policies related

to legal proceedings that involve recorded information. It provides opinions and advice to other stakeholders about legal issues related to recorded information.

Compliance

Compliance is concerned with ensuring that an organization's practices comply with external requirements, including laws, regulations, and industry-specific guidelines that specify retention and security requirements for recorded information, and with the organization's internal policies and directives for creation, storage, distribution, retention, disposition, and protection of information assets. Compliance will investigate suspected violations of organizational policies and present the findings with recommendations for corrective action.

Business Units

Individual organizational units are responsible for day-to-day management of information in full com-

pliance with applicable policies, procedures, guidelines, and directives. They must identify and dispose of recorded information with elapsed retention periods, determine access privileges and restrictions that apply to specific information assets, organize information assets for retrieval when needed, and protect information assets from loss, damage, or improper disclosure.

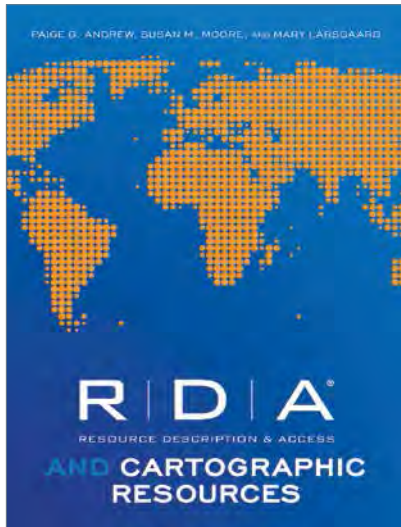
In conjunction with the Principles, ARMA International has issued an Information Governance Maturity Model (Maturity Model) that defines and describes five levels of program development – from sub-standard to transformational – for each of the eight principles. Organizations can use the Maturity Model for program evaluation and development, benchmarking, gap analysis, and risk assessment. **END**

William Saffady, Ph.D., FAI, can be contacted at wsaffady@aol.com. See his bio on page 47.

A promotional poster for the ARMA LIVE! DC 15 conference. The background features a blurred image of a city skyline at night. Overlaid on this is a large, bold, red word "SCANDAL" in a serif font. Above it, in a smaller, black, sans-serif font, is the text "DON'T GET CAUGHT IN AN INFORMATION GOVERNANCE". Below "SCANDAL", in a bold, black, sans-serif font, is "ARMA LIVE! RETURNS OCTOBER 5-7 WASHINGTON D.C.". In the center, there is a red and white logo that says "ARMA LIVE! DC 15". Below the logo, in a red, sans-serif font, is the website "www.arma.org/conference".

A New Cataloging Standard for Today's Varied Resources

Robert Bailey, Ph.D., CRM



Cataloging resources is not something every records manager comes across or necessarily needs to know how to do. But I found the topic interesting, and this book renewed my thoughts about the highly developed content standards for cataloging library resources.

RDA and Cartographic Resources is about the resource description and access (RDA) unified cataloging standard, which evolved from the Anglo-American Cataloguing Rules (AACR2). It was designed for the digital world and the expanding universe of metadata users, is meant to be compatible with international principles, models, and standards, and potentially solves some of the fundamental problems of traditional *cartography*, or the practice of making maps.

The Evolution of RDA

RDA's evolution began in 1967 with the AACR, which became the AACR2 in 1978. AACR2 was revised three times, in 1998, 2002, and 2010.

RDA emerged from the Interna-

tional Conference on the Principles & Future Development of AACR held in Toronto in 1997. It was quickly realized that a substantial revision of AACR2 was required, which encouraged the adoption of a new title for what had been envisaged as a third edition of AACR.

It was adopted as a standard on April 1, 2013, by the U.S. Library of Congress (LOC) and the British Library, but its implementation was delayed during the several months LOC catalogers needed for training.

One major difference between RDA and its predecessor is that AACR2 arranges materials by format type while RDA arranges them according to the International Federation of Library Associations and Institutions' "Functional Requirement for Bibliographic Records" (FRBR).

According to a book the authors cited, *From AACR2 to RDA: An Evolution* by Kathy Glennan, RDA provides a set of guidelines and instructions on recording data to support resource discovery and improves the instructions for non-printed resources. It separates rules for recording and presenting data elements, helps eliminate redundancy, and incorporates rules for authority control. Glennan also wrote that RDA functions best as an interactive, online tool.

Chapter Highlights

There are several informative chapters beginning with Chapter 3 "Comparing Standards," Chapter 4 "Navigating RDA to Describe Cartographic Resources Elements, and Chapter 5 "Cartographic Resources Cataloging."

The heart of the manual is Chap-

RDA and Cartographic Resources

Authors: Paige G. Andrew, Susan M. Moore, and Mary Larsgaard

Publisher: ALA Editions

Publication Date: 2015

Length: 152 pages

Price: \$62

ISBN: 978-0-8389-1131-0

Source: www.alastore.ala.org

ter 4, which compares the Machine-Readable Cataloging (MARC) Format for Bibliographic Data fields that describe cartographic resources to the RDA guidelines for recording descriptive element information.

Where RDA is silent on certain points, the authors refer to the Library of Congress Program for Cooperative Cataloging Policy Statements (known as LC-PCC PS) and best practices. This chapter provides numerous examples of how RDA procedures are different from earlier procedures.

In the last chapter, the authors describe the advantages and disadvantages of RDA. They point out that because relationships are at the center of the FRBR model around which RDA is structured, it is easier to bring together in a meaningful way those things related to and within a given resource.

One illustration I could identify with dealt with the futility of attempting to explain the subtleties of the work done at the old reference desk to users engaged in searching a library's online system. Although that old structure worked well when

people used a traditional card catalog, very few libraries live in that world now. The library's signature service, its catalog, uses rules for cataloging that are remnants of a long-departed technology: the card catalog. It was time to move on.

Useful Extra Features

The three authors of this book are very experienced in cartographic resources and participated heavily in the evolution of RDA. Because of their education and work experience as specialist catalogers, they included in this publication numerous examples, pictures, and sample records about managing the materials in their areas

of responsibility. Again and again, the publication correlates what is familiar from AACR2 to what is new and different in RDA.

The book also includes seven appendixes filled with images, checklists, and examples to help readers better understand the applications, a strong index for cross-references, and a few key definitions.

Recommendation

It does not matter if readers are practicing map catalogers or catalogers new to cartographic resources, this guide offers a summary and overview of how to catalog cartographic resources using the new standard.

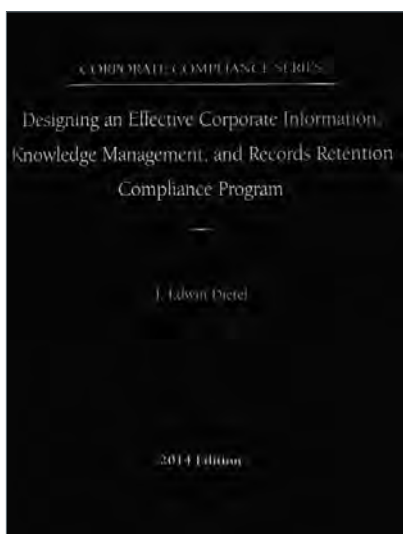
Even the non-expert cataloger will be able to understand how to handle such topics as: Background to Title and Other Statements, Dealing with Cartographic Projections, Background to Physical Description, and Background to Content Type.

The *RDA and Cartographic Resources* publication is a great reference for those who need to understand and apply this new standard for cataloging all the various types of materials and metadata formats in the library and records management profession.

Robert Bailey, Ph.D., CRM, can be contacted at robertbai@mccarran.com. See his bio on page 47.

Weighty Tome Is Light on Comprehensive RM Best Practices

Sheila Taylor, IGP, CRM



Designing an Effective Corporate Information, Knowledge Management, and Records Retention Compliance Program is the third volume in Thomson Reuters' multi-volume Corporate Compliance Series, which is designed

to help organizations prevent and detect possible violations in law in such areas as intellectual property, securities, and antitrust.

The intended audience of this volume is attorneys practicing records management (RM) and professional corporate records managers. Specifically, one of the author's objectives is "to introduce basic records management fundamentals to those just starting in this field or those lawyers expanding their practice into this area."

The Fundamentals

Introductory information is presented on such topics as:

- The fundamentals of effective corporate RM (e.g., the records life cycle concept, the objectives of a corporate RM program)
- How to establish and maintain a corporate RM program (e.g., developing a records retention

Designing an Effective Corporate Information, Knowledge Management, and Records Retention Compliance Program

Author: J. Edwin Dietel, J.D.

Publisher: Thomson Reuters

Publication Date: 2014

Length: 1,441 pages

Price: \$507 or \$42 a month for the book plus updates

ISBN: 978-0-314-63428-3

Source: thomsonreuters.com

schedule, marketing and selling a records retention compliance program)

- Steps in establishing an effective and Sarbanes-Oxley-compliant RM program
- Educating staff about RM (e.g., the theory of different learning

styles, implementing a RM hotline)

- Conducting records audits (e.g., 26 essential “quality” criteria that information in corporate records should satisfy, how to conduct an audit)

Coverage of the fundamental topics is not comprehensive. For example, the author does not address digital preservation in Chapter 7 “Considerations for Computer Files and Electronic Records.”

Some Misalignment

Some of the author’s recommendations do not align with RM best practices; he lumps the development of a corporate RM policy in with topics such as reports management, storage issues, and tickler systems in Chapter 5 “Other Issues Involving Corporate Records,” for example, rather than presenting it as an integral element in Chapter 3 “Establishing and Maintaining a Corporate RM Program.”

Also, the author recommends setting minimum retention periods and periodically reviewing records at the end of those periods to determine whether additional retention should apply.

It is also curious that the author defines a *record* as “information one has recorded in some medium because there is a chance of it being needed in the future and whose disposition

is determined by a corporate records schedule” and cites Doculabs’ 1998 definition of the term while making no reference to the widely accepted definition in the international RM standard, ISO 15489-1:2001 *Information and documentation – Records management – Part 1: General*.

The author’s interchangeable references to “corporate records program” and “corporate retention program” also cause some confusion since those terms are not synonymous.

Good Leadership Advice

Where this volume succeeds is in imparting considerable information about leadership to better prepare individuals to assume a leadership role in RM, one of the author’s objectives as stated in the Preface: “attorneys practicing record [sic] management and professional record [sic] managers need to be significantly more than merely cogs in the corporate wheel. They need to be effective leaders not only in their field, but also in the overall corporate organization.”

The author draws on the works of well-known authors such as Stephen Covey to address diverse leadership-related topics such as leadership styles (i.e., analytical, driver, amiable, and expressive), 16 competencies that distinguish extraordinary leaders (e.g., displaying high integrity

and honesty), how to motivate people, the importance of trust, and how to develop customer loyalty.

At 1,441 pages, this is a weighty tome (2.5 pounds). Almost 60% of the volume is text (10 chapters), while the final chapter (620 pages) is a collection of 20 forms and exhibits from a variety of sources. I question the utility of including materials that are freely available on the Internet, such as the U.S. National Archives and Records Administration’s 213-page General Records Schedules, and quickly outdated materials like the 279-page results of a 50-state survey of records retention requirements for selected record types such as insurance and bank operations.

Not Best Choice for RM Practices

Readers – whether lawyers or RM practitioners – seeking a more comprehensive and “how to” approach to RM program development and implementation would be better served by other publications. However, readers seeking a précis of leadership theory to help them prepare to lead RM will find this volume of interest. Whether their RM program budgets can afford the \$507 purchase price remains to be seen. **END**

Sheila Taylor, IGP, CRM, can be reached at staylor@eimc.ca. See her bio on page 47.



twice as hot

Double your professional development with
ARMA International's
free mini web seminars

Our **hottopic** series is now available and includes three to five 20-minute web seminars brought to you by the industry’s best and brightest. Sign up just once, and come back again and again to take advantage of this fantastic education.

www.arma.org/rl/professional-development



174 Strong. And Growing.

Congratulations to these Certified Information Governance Professionals

Elizabeth Adkins
Pey-Jia Angell
Christine Ardern
Deborah Armentrout
DeAnna Asscherick
Randy Aust
Christie Baird
Salvador Barragan
Christopher Beahn
Richard Berlin
Margaret Boeringer
Isabel Bracamontes
Susan Burd
Doug Caddell
Stacie Capshaw
Melissa Carlis
Diane Carlisle
Laurie Carpenter
Alexander Carte
Mark Carter
Anita Castora
Elizabeth Castro
Tod Chernikoff
Carol Choksy
Vicki Clewes
Julie Colgan
Bud Conner
Dani Cook
Marvin Cross
Kristen Crupi
Becky Darsch
Lisa Marie Daulby
Nicholas De Laurentis
Melissa Dederer
G. Derk
Deborah Dotson
Christina Doyle
Sandra Dunkin
Priscilla Emery
Sofia Empel
Tony Epler
Debra Farries
Elizabeth Farthing
Carol Ann Feuerriegel
Glenn Fischer

Matt Fisher
David Fleming
Patricia Franks
Rhonda Galaske
Caroline Gallego
Stephen Garner
Charles Garrett
Irene Gelyk
Sue Gerrity
Kimberly Giertz
Susan Goodman
Joshua Grisi
Komal Gulich
Jocelyn Gunter
Allen Gurney
Michael Haley
Grace Hammar
Joshua Hargrafen
Paula Harris
Charles Herbek
Margaret
Hermesmeier
Caroline Higgins
Gordon Hoke
Patricia Huff
Janice Hulme
Bethany Hynes
Leigh Isaacs
Mary Frances Janicik
C'Les Jensema
Chris Johnson
Todd Johnson
Deborah Jostes
Deborah Juhnke
Soo Kang
Andrew Keller
James Kennedy
Anju Khurana
Ellie Kim
Michelle Kirk
Tamara Koepsel
Greta Krapac
Peter Kurilecz
Tera Ladner
Ronald Layel

Anna Lebedeva
Gilles Legare
Donnell Long
John Loveland
Eric Lynn
Cindy MacBean
Rudolph Mayer
Brian McCauley
Stephanie
McCutcheon
Cheryl McKinnon
James Merrifield
Sandy Miller
Dana Moore
Dermot Moore
Rafael Moscatel
Linda Muller
Jen Murray
Stephen Murray
Joe Nadzam
Lindy Naj
Peggy Neal
Lee Nemchek
Sheri Nystedt
Carolyn Offutt
James Owens
Eleanor Ozaeta
Lewis Palmer
Jadranka Paskvalin
Alan Pelz-Sharpe
Graham Pescod
Denise Pickett
Debra Power
James Presley
Cindy Pryor
Fred Pulzello
Tony Ratcliffe
Joshua Rattan
Jessica Rickenbach
Deborah Rifenbark
Carol Rittereiser-
Coritt
David Rohde
Donna Rose
Kathryn Scanlan

Danna Schacter
Teresa Schoch
Terry Schrader
Karen Schuler
Mary Sherwin
William Silvio
David Skweres
Michael Smith
Natalie Spano
Brian Starck
Jason Stearns
David Steward
Melissa Suek
Paula Sutton
Marjorie Swain
Sheila Taylor
Robin Thompson
Brian Tretick
Susan Trombley
Nathan Troup
Brian Tuemmler
Martin Tuip
Amy Van Artsdalen
James Vardon
Jennifer Watters Farley
Bridgett Weldner
Erik Werfel
Steven Whitaker
Kristi Whitmore
Jesse Wilkins
Marc Willemse
Dylan Williams
Steven Williams
Rick Wilson
Terri Wilson
Brett Wise
Jennifer Witt
Kristin Wood
Robin Woolen
Jeffrey Yawman
Andrew Ysasi
Ryan Zilm

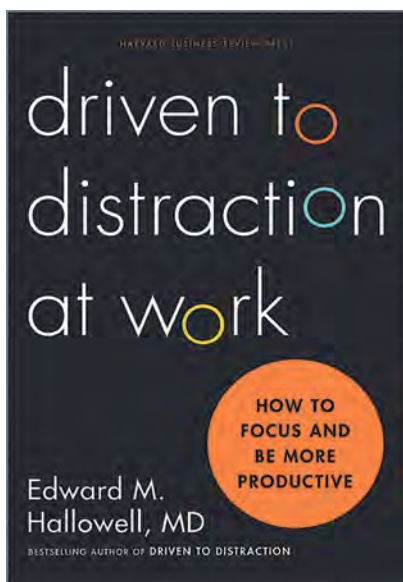
Application deadlines: Nov. 14, 2015 and March 28, 2016.

Register today at www.ama.org/igp.



Distracted? You May Have ADT (No, Not the Home Security System...)

Beth Mellinger



Driven to Distraction at Work: How to Focus and Be More Productive by Edward M. Hallowell, M.D., introduces the term attention deficit trait (ADT), which he feels people in all work places are developing due to the constant interruptions, distractions, and chaos everyone is exposed to daily at work and home.

Assessing Distractions

In the introduction, Hallowell writes that ADT in the workplace is caused by one or more of the six most common distractions, which he calls screen sucking, multitasking, idea hopping, worrying, playing the hero, and dropping the ball.

At the end of this part, readers are prompted to take a free assessment at hbr.org/assessments/ad1 to see which distractions are problems for them. I found the assessment interesting and accurate. Taking this assessment will allow readers to identify their areas of distraction and use the book to learn how to minimize them.

Identifying Six Common Distractions

In Part One, each one of the six distractions is examined as a case study. The author introduces six “patients” based on actual patients he has treated. Each chapter begins with a synopsis of the patient and how the distraction affects him or her.

Hallowell also provides symptoms for each distraction that readers can use to identify whether the distraction affects them. An example of the symptoms of screen sucking, for example, is:

- If my cell phone is out of reach, I feel disconnected.
- I can waste an hour online and not even realize it.
- I have a lack of discipline when it comes to the Internet.

The next part of the chapter is what the author recommends to his patient as treatment to overcome the distraction. At the end of each chapter is a list of 10 tips about what readers can do to overcome the distraction themselves.

Training Yourself to Focus

In Part Two, the author describes five essential ingredients for clearing your mind and helping you focus: energy, emotion, engagement, structure, and control.

To achieve the optimal level of these five essentials, the author says people need what he calls the six basic practices of energy management, or the “Sensational 6”: sleep, nutrition, exercise, meditation, cognitive stimulation, and positive communication. Each of these is described in detail.

The patients from Part One are brought back in at this point, and readers find out how they were able

Driven to Distraction at Work: How to Focus and Be More Productive

Author: Edward M. Hallowell, M.D.

Publisher: Harvard Business Review Press

Publication Date: 2015

Length: 247 pages

Price: \$26

ISBN: 978-1-4421-8641-1

Source: <https://hbr.org>

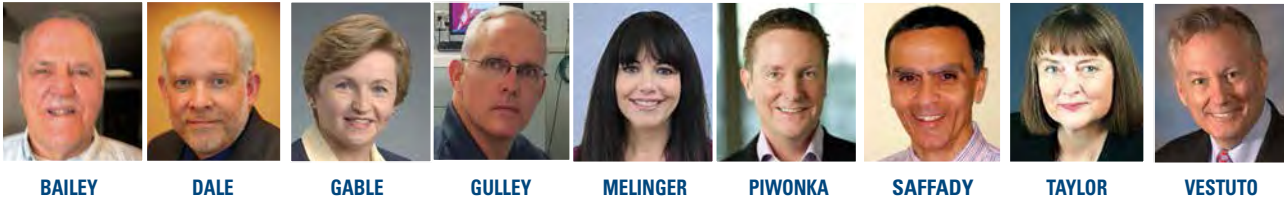
to adapt their behavior and fix their work and home lives. Throughout this section, there are several references to other works by the author’s colleagues and to an application the author has developed to help readers reach their “Sensational 6.”

Recommendation

When I read the title, I expected that this book was going to discuss the constant distractions that bombard us daily, such as e-mail, meetings, and colleague interruptions. Instead, this book is more of a self-help/self-improvement” book or guide to better mental health.

I did enjoy reading the book; it was a quick and easy read that contained helpful suggestions for me in my own workday. Though the book does not deal directly with information management, it is a good guide for organizing work and home lives and would be helpful to any professional. **END**

Beth Mellinger can be contacted at beth.mellinger@alcosan.org. See her bio on page 47.



Critical Steps to Creating a Consistent Preservation Hold Process Page 16

Richard Vestuto, J.D., is director for Deloitte Financial Advisory Services LLP, which provides forensic, dispute, and other consulting services, and its affiliate Deloitte Transactions and Business Analytics LLP, which provides a wide range of advisory and analytics services. He specializes in providing leading guidance and other technology-based litigation and data retention strategies to corporate and law firm clients. He earned his juris doctor degree at Touro Law School. Vestuto can be contacted at rvestuto@deloitte.com.

Bill Piwonka is chief marketing officer for Exterro, the preferred provider of software specifically designed for in-house legal and IT teams at Global 2000 organizations. He has more than 20 years of experience in leading marketing and strategic growth initiatives. He holds a master's of business administration degree from The Wharton School at the University of Pennsylvania and a bachelor of arts degree in quantitative economics from Stanford University. He can be contacted at bill.piwonka@exterro.com.

The Principles: The Principles and External Audits Page 26

Julie Gable, CRM, CDIA, FAI, is the retired president and founder of Gable Consulting LLC, a firm that served clients' information governance needs for the past 25 years. The author of numerous articles on information-related topics, she has 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.

Business Matters: Planning for and Managing During a Paper Document Disaster Page 40

William (Bill) R. Gulley, Jr. is an archives and records management specialist with Document Freeze Drying Inc. He has managed document losses from coast to coast, helping scores of information managers recover their collections after natural disasters. Previously, he served as a university archivist for over 25 years. Gulley can be contacted at Bill.Gulley@ers-us.com.

RIM's Role in Harnessing the Power of Big Data Page 26

Kevin L. Dale, CRM, is the records and information management (RIM) manager at the Federal Reserve Bank of Chicago. He has been active in the RIM profession for more than 7 years and has

experience in the nuclear and banking industries. He has also had leadership roles in the implementation of multiple ECM systems. Dale earned a master's of business administration degree from the University of Phoenix and is also a Certified Records Manager. He can be contacted at kevin.dale@chi.frb.org.

RIM Fundamentals: Records Management or Information Governance? Page 43

William Saffady, Ph.D., FAI, is an information management consultant, providing analytical services and training. The recently retired professor from the Palmer School of Library and Information Science, Long Island University has authored more than three dozen books and many articles on electronic record retention, digital document management, storage and preservation of recorded information, and other related topics. ARMA International will publish his third edition of *Records and Information Management: Fundamentals of Professional Practice* this fall. Saffady can be contacted at: wsaffady@aol.com.

A Comprehensive Information Governance Resource Page 43

Robert Bailey, Ph.D., CRM, is records program administrator and EMC project leader at McCarran International Airport in Las Vegas. Previously, he was records manager advisor in the Office of Chief Information Officer, St. Johns, Newfoundland and Labrador, Canada. He is an active consultant, speaker, and seminar leader at numerous national conventions. Bailey can be contacted at Robertbail@mccarran.com.

Weighty Tome Is Light on Comprehensive RM Best Practices Page 44

Sheila Taylor, IGP, CRM, is the partner and CEO of Ergo Information Management Consulting. She has more than 25 years of records and information management experience as a consultant, practitioner, and educator. Taylor can be reached at staylor@eimc.ca.

Distracted? You May Have ADT (No, Not the Home Security System...) Page 46

Beth Mellinger is manager of records and document control for Allegheny County Sanitary Authority (ALCOSAN). She is currently preparing for the launch of ALCOSAN's Wet Weather Program, which will be the largest public works project in Southwestern Pennsylvania. She can be reached at beth.mellinger@alcosan.org.



ADVERTISE IN *IM* MAGAZINE

Information Management

magazine is **the** resource for information governance professionals.

With a circulation of over 27,000 (print and online), this audience reads and refers to *IM* much longer than the month of distribution.

Talk to Karen or Krista about making a splash.

Advertise today!



Karen Lind Russell/Krista Markley
Account Management Team
+1 888.279.7378
+1 913.217.6022
Fax: +1 913.341.6823
Karen.Krista@armaintl.org

23 Institute of Certified Records Managers
518.694.5362 – www.ICRM.org

FC, BC Iron Mountain
800.899.4766 – www.ironmountain.com/virtualRIMForum15

3 NAID
<http://directory.naidonline.org>

19 Next Level
www.arma.org/nextlevel

IBC OPEX Corporation
www.opex.com/agility

IFC Sherpa
800.255.5155 – www.sherpasoftware.com

5, Zapproved
Insert 888.806.6750 – www.zapproved.com



www.arma.org

Is Your Resumé Ready?



ARMA International's CareerLink is the only job bank specifically targeting records and information governance professionals. Post your resume today and search a database of available positions.

It makes job hunting easy!



AGILITY.
ACUITY.
PRECISION.
CLARITY.
SPEED.

Oh yeah...
the bird, too.

FalconTM

VIRTUAL RIM FORUM: NOW AVAILABLE ON-DEMAND



Without leaving your desk, view on-demand keynote sessions, visit the virtual exhibition hall, and access innovative thought leadership resources. You will learn how to see your information differently in our virtual online environment:

- Gain key insights from leading RIM experts
- Learn what components are vital to Information Governance
- Identify how to gain maximum return on your information

Virtual RIM Forum: on-demand,
at your convenience.

Immediate access:

ironmountain.com/virtualRIMForum2015

SEE INFORMATION
DIFFERENTLY

