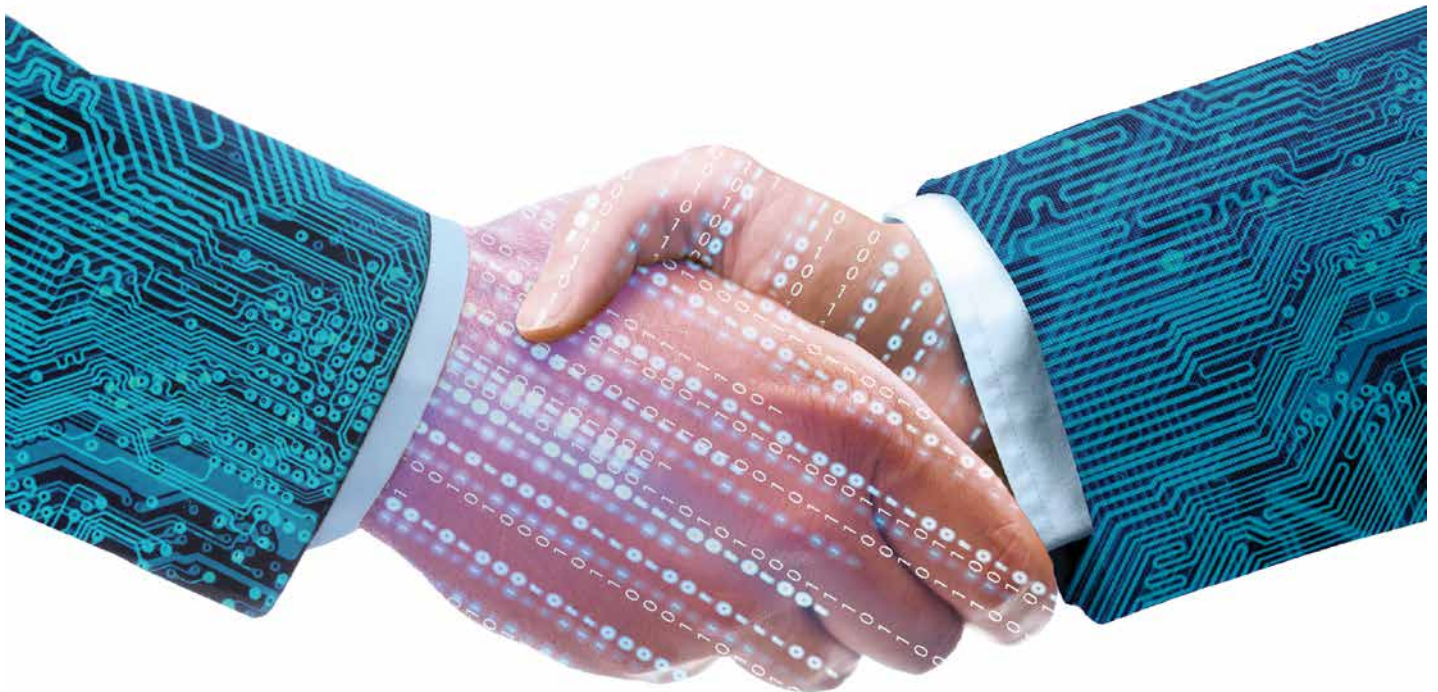


INFORMATION MANAGEMENT

50TH YEAR

AN ARMA INTERNATIONAL PUBLICATION

JULY/AUGUST 2016



Integrated ECM Solutions:

Where Records Managers, Knowledge Workers Converge

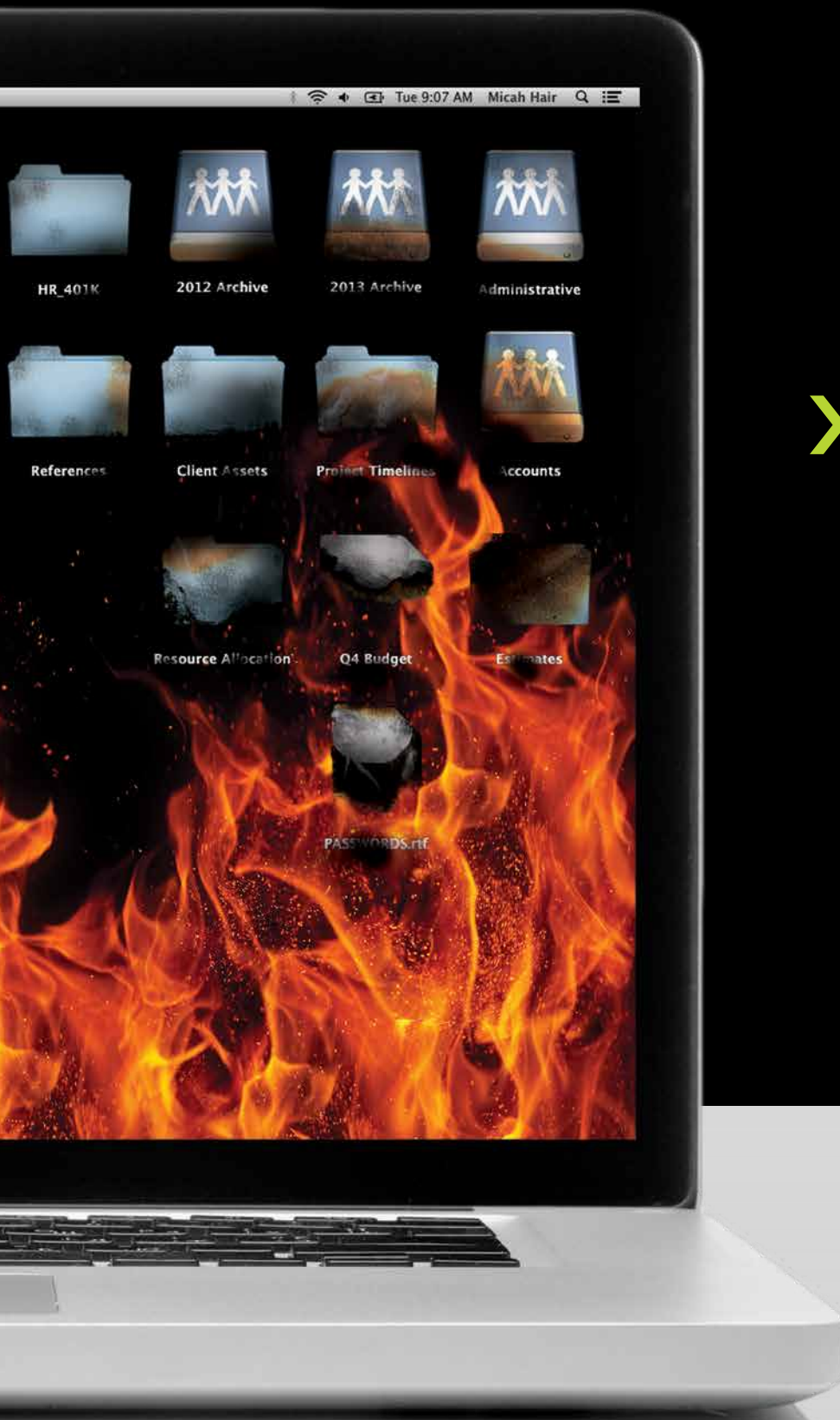
Page 18

Five Steps In-house Counsel Should Take to Mitigate Information Risk

Page 24

Minimizing the Use of Trigger Events to Increase Records Retention Compliance

Page 29



➤ Don't get burned by
**MISMANAGED
INFORMATION.**

**NEXT
LEVEL** ➤ information governance assessment

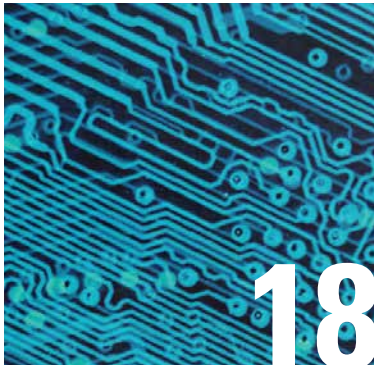
Your amount of sensitive customer and business data is doubling by the year. And a little loss could have a big impact on your bottom line. Now more than ever, the way you manage your company's information matters. Find out where you stand with the Next Level Information Governance Assessment. Through this self-administered online assessment tool, you'll discover areas of strength. You'll also uncover opportunities for improvement. In the end, you will be empowered to increase your organizational transparency and data integrity.

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

INFORMATION MANAGEMENT

50TH YEAR

JULY/AUGUST 2016 VOLUME 50 NUMBER 4



DEPARTMENTS

4

INFOCUS A Message from the Editor

6

UPFRONT News, Trends, and Analysis

FEATURES

18

FELLOWSFORUM

Integrated ECM Solutions: Where Records Managers, Knowledge Workers Converge

Patricia C. Franks, Ph.D., IGP, CRM, CA, FAI

24

Five Steps In-house Counsel Should Take to Mitigate Information Risk

H. Kirke Snyder, J.D.

29

Minimizing the Use of Trigger Events to Increase Records Retention Compliance

Tom Corey, J.D., CRM

SPOTLIGHTS

32

TECHTRENDS

Software Updates May Be Compromising Your IG

John T. Phillips, CRM, CDIA, FAI

36

MANAGEMENTWISE

3 Keys to Managing Change for a Successful RIM Program Implementation

Melissa Dederer, IGP, CRM and Aaron Swan

SPECIAL SECTION

40

50THYEAR

50, 25, 10 Years: A Look Back...

43

INREVIEW

A Primer for Corporate Librarianship and Information Management

Melanie Sucha

44

INREVIEW

How the Hybrid Information Environment Is Transforming Libraries, History, Scholarship

Mary Broughall

46

INREVIEW

Visualize It! The Key to Driving Better Business Decisions

Robert Bailey, Ph.D., CRM

CREDITS

47

AUTHORINFO

48

ADVERTISINGINDEX

BONUS CONTENT

B-49

UPFRONT News, Trends, and Analysis

B-50

Legal Requirements for Electronic Records Retention in Western Europe: An Overview

William Saffady, Ph.D., FAI

B-50

Standard Human Resource Record Categories

Teri Mark, CRM

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, IGP, CRM, PMP

Editor in Chief: Vicki Wiler

Contributing Editors: Nikki Swartz, Jeff Whited, April Dmytrenko, CRM, FAI

Art Director: Brett Dietrich

Advertising Account Manager: Jennifer Millett

Editorial Board: Sonali Bhavsar, IBM • Alexandra Bradley, CRM, FAI, Harwood Information Associates Ltd. • Sara Breitenfeldt, PepsiCo • Marti Fischer, CRM, FAI, Wells Fargo Bank • Uta Fox, CRM, Calgary Police Service • Mark Grysiuk, CRM, CIP • Parag Mehta, Esq. • Preston Shimer, FAI, Records Management Alternatives • Sheila Taylor, IGP, CRM, Ergo Information Management Consulting • Stuart Rennie, Stuart Rennie Consulting • Karen Shaw, CRM, BSP Consulting • Mehran Vahedi, Enbridge Gas Distribution Inc. • Jeremy Wunsch • 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 \$150/year (plus \$20 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 Jennifer Millett at +1 888.277.5838 (US/Canada), +1 913.217.6022 (International), +1 913.341.3742, or e-mail jennifer.millett@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.

© 2016 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.



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



Forging Stronger Relationships with IT and Legal to Advance Your RIM Program



If you are a records and information management (RIM) professional who is looking for practical opportunities to work alongside and increase your influence with IT and legal, you will find support in this issue's articles.

As the person most knowledgeable about your organization's information-handling processes, you are in a prime position to work with IT to integrate your enterprise content management (ECM) system with other business solutions to enhance employees' ability to do their jobs and comply with RIM requirements. Patricia Franks, Ph.D., IGP, CRM, CA, FAI, tells you how in the cover article.

Franks uses examples from Gartner's 2016 "Magic Quadrant for Enterprise Content Management" to introduce three ECM systems, provide examples of integrated solutions used

by knowledge workers, and discuss how RIM professionals can support business processes by helping select the right tools, developing policies, and implementing the appropriate controls.

Sharing our second feature article with your in-house counsel will encourage him or her to take a more active role in working with you to promote the importance of information governance (IG), secure needed resources for IG, and drive collaboration among key IG stakeholders to reduce your organization's risk profile. In "Five Steps In-house Counsel Should Take to Mitigate Information Risk," author H. Kirke Snyder, J.D., IGP, recommends: preparing for a U.S. Federal Rules of Civil Procedure's Rule 30(b) (6) deposition, creating a data map, securing financial and human resources, revising the records retention policy and schedule, and modifying storage vendor service level agreements.

When revising your retention schedule, you should consider the advice given by Tom Corey, J.D., CRM, about "Minimizing the Use of Trigger Events to Increase Records Retention Compliance." He provides practical guidance for using straight retention periods for six trigger events commonly used in retention schedules: expiration of contract, final resolution, protection period, life of product, superseded, and project completion. Making this change will allow your organization's CMS to handle records' disposition more effectively and ef-

ficiently, Corey writes.

Leverage your relationship with IT to gain support for controlling auto-updating software. In the "Tech Trends" article, "Software Updates May Be Compromising Your IG," author John Phillips, CRM, CDIA, FAI, uses the auto-updating features of Windows 10 as an example of the dangers of this practice.

Of course, strong relationships with all IG stakeholders are critical if you're looking to implement any major change, but particularly for implementing or modifying a RIM program. Read our "Management Wise" sub-feature to learn the "3 Keys to Managing Change for a Successful RIM Program Implementation," by Melissa Dederer, IGP, CRM, and Aaron Swan.

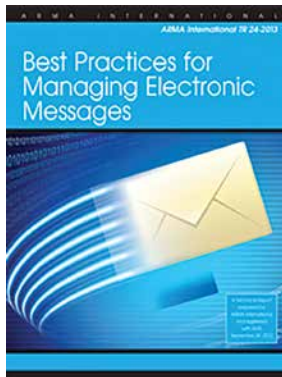
Please e-mail us at editor@armaintl.org to let us know the topics you want to read about in these pages. We're eager to provide the content you need to advance your professional skills, your career, and your organization's RIM or IG program.

Also, don't forget you can browse archived issues going back to 2005 by clicking on <http://content.arma.org/IMM/online/Archives.aspx> and the current issue at <http://imm.arma.org>. Even if you prefer the print version, you'll want to access the "Bonus Content" found only online in each of the issues published this year.

Vicki Wiler
Editor in Chief



E-mail Management



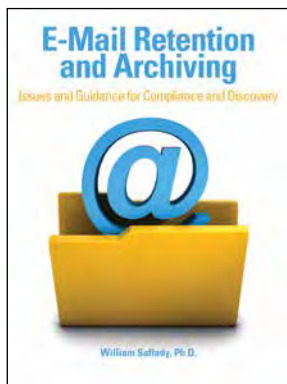
Best Practices for Managing Electronic Messages

(ARMA International TR 24-2013)

This technical report provides current information for managing all types of text-based electronic messages or communication, such as e-mail, instant messages, and text messages.

A4938 **\$55.00** Professional members: **\$35.00**

V4938 PDF **\$50.00** Professional members: **\$30.00**



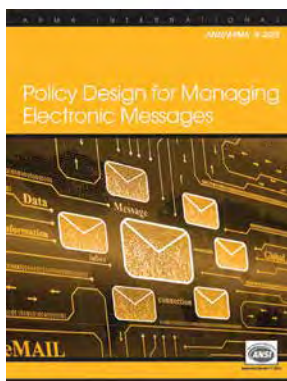
E-Mail Retention and Archiving: Issues and Guidance for Compliance and Discovery

William Saffady, Ph.D.

With its focus on the retention of e-mail to satisfy an organization's legal, operational, and historical requirements, this book will help organizations avoid over-retention problems and simplify the discovery process.

A4965 **\$55.00** Professional members: **\$35.00**

V4965 PDF **\$50.00** Professional members: **\$30.00**



Policy Design for Managing Electronic Messages

(ANSI/ARMA 19-2012)

This American National Standard sets forth the requirements for a policy guiding the management of electronic messages as records throughout their life cycle – from creation to final destruction or disposition.

A4930 **\$60.00** Professional members: **\$40.00**

V4930 PDF **\$55.00** Professional members: **\$30.00**

Order online today! **BOOKSTORE** ARMA INTERNATIONAL
www.arma.org/bookstore

PRIVACY

FCC Rules Would Restrict Use of Consumers' Private Data

Internet service providers (ISPs) that provide broadband Internet access service to consumers have extraordinarily broad access “to very sensitive and very personal information that could threaten a person’s financial security, reveal embarrassing or even harmful details of medical history, or disclose to prying eyes the intimate details of interest, physical presence, and fears,” according to the Federal Communications Commission (FCC).

ISPs can follow their customer’s Internet activity by collecting individualized data and develop highly specific profiles of where

each user goes and what services are acquired upon arrival at their Internet destinations, according to *The New York Law Journal*. That is why the FCC adopted, by a 3-to-2 vote, Notice of Proposed Rule Making (NPRM) that, if adopted, will address consumers’ rights to have notice, choice, and security when their private information is used by broadband providers.

The FCC said in a statement that the NPRM proposes rules that would give broadband customers “the tools they need to make informed decisions about how their information is used by their ISPs”



and whether and for what purposes ISPs may share their customers’ information with third parties.

The FCC’s proposal allows for certain data collection that is necessary to provide broadband services and for marketing those services, as well as for public safety; this would not require customer consent beyond creation of the customer-ISP relationship. All other uses and sharing of consumer data would require “express, affirmative ‘opt-in’ consent from customers.”

The NPRM defines the data to be protected as customer proprietary information, which would include both “customer proprietary network information” and personally identifiable information collected by broadband providers through their provision of services.

Because there is no uniform federal breach notification standard, the NPRM proposes that broadband providers notify affected customers within 10 days of discovering a breach that triggers customer notification requirements. The NPRM requires that the FCC be notified of all data breaches and that other federal law enforcement be informed of breaches that impact more than 5,000 customers within seven days of their discovery and three days before notification to the customer, the *New York Law Journal* reported.

PRIVACY

GDPR, Privacy Shield Will Impact Businesses, Survey Finds

According to the “2016 EU GDPR and EU-U.S. Privacy Shield Survey” by Baker & McKenzie, 84% of privacy professionals who responded said they expect the new General Data Protection Regulation (GDPR) recently adopted by the EU to impact their organizations.

Of the 100 respondents surveyed, between 60% and 70% said their organizations will need to spend at least some or significantly more of their budget in an effort to comply with the GDPR. The requirements that will call for additional attention include consent, data mapping, and cross-border data transfer, according to the survey.

Lawyers say preparing for the GDPR and Privacy Shield regulations calls for creating readiness plans and data maps, and the majority of organizations do not believe they have the tools and solutions necessary “to meet all of the requirements,” Theo Ling, an attorney at Baker & McKenzie, told *Legaltech News*. In fact, the survey revealed that 45% of respondents said they either do not have the tools or could obtain them only at significant cost.

The good news is that more than 80% of the respondents said they are at least somewhat familiar with all of the major GDPR requirements. That’s good, because the GDPR allows non-compliance fines of up to €20 million (\$22.79 million U.S.) or 4% of an organization’s total global annual turnover.



PRIVACY

EU Approves GDPR

The EU Parliament passed the General Data Protection Regulation (GDPR), overhauling the Data Protection Directive rules established in 1995. The rules apply to all organizations and businesses targeting EU consumers, regardless of their geographic location.

According to *Legaltech News*, the legislation defines new data and privacy rights for EU consumers, regulates the transfers and processing of EU data, and establishes more stringent enforcement of data handling, allowing organizations to be fined up to 4% of its total worldwide revenue for violating GDPR regulations.

GDPR is meant to replace the patchwork of EU member states' national laws so that businesses accessing EU data will have only one centralized supervisory authority to follow. The EU estimates that savings from this standardization will hit €2.3 billion (\$2.6 billion U.S.) per year, *Legaltech News* reported.

The GDPR is effective now, but member states have two years to translate the regulations into their national laws. The UK and Ireland will follow the regulation on a limited basis because of their special "home affairs and justice legislation" status. Denmark will vote on the adoption of the GDPR within six months.

The GDPR:

- Allows an EU citizen's right to be forgotten, which means data controllers, processors, and Internet third parties must remove the personal data of an EU citizen upon request if there are no legitimate reasons to retain such information, such as historical, statistical, public health, scientific need, a right to free expression, or legal or contractual obligations
- Requires clear and affirmative consent, such as an EU citizen "ticking a box" on a website allowing it to retain or process his or her personal data
- Gives EU citizens the right to data portability, which allows them to transfer personal data between service providers easily, such as moving contact information from one e-mail provider to another
- Requires clear, plain language in Internet and business privacy policies
- Requires EU businesses and providers to expedite notifying their national supervisory authority of "serious" data breaches
- Limits the use of "profiling," which is collecting an individual's personal information in order to predict his or her behavior, without the expressed consent of the individual, or that of a law or contract
- Requires parental consent for children between the ages of 13 and 16 to open social media accounts, although the exact age varies among EU member states. Such laws are already



in place in most EU countries.

The GDPR was also passed with a new EU directive on cross-border data processing and handling in criminal and judicial investigations, *Legaltech News* reported. The directive sets minimum standards for data processing by law enforcement agencies, defines EU citizens' rights and data transfer limitations in criminal or judicial processes, and enables cooperation between member state law enforcement agencies.

E-DISCOVERY

EDRM Releases

E-Discovery Glossary

EDRM has released a free, downloadable PDF version of its *EDRM Glossary*, a comprehensive glossary of e-discovery terms. At more than 330 pages, the glossary is the industry's most comprehensive listing of electronic discovery terms.

"Experienced legal and e-discovery professionals have developed a fairly broad understanding of the processes and terms related to our craft," says George Socha, EDRM co-founder, "but none of us knows it all, and the technologies and language surrounding e-discovery continue to advance. Our goal with the glossary is to provide a tool that will enhance e-discovery knowledge and understanding, and evolve with the industry."

First launched in 2006, the *EDRM Glossary* includes terms from specialized glossaries on collection, metrics, search, and information governance, as well as glossary content on search and predictive coding from Herb Roitblat and from the Grossman-Cormack glossary on technology-assisted review.

The complete EDRM glossary can be downloaded at www.edrm.net/resources/glossaries/glossary.

PROFESSIONAL DEVELOPMENT

Survey: U.S. Government Not Prepared for Future IM Requirements



Many federal information management (IM) professionals feel unprepared to handle the future requirements of their jobs, according to the recent Iron Mountain survey report “Constructing the Next Generation Information Management Professional.”

Iron Mountain said it conducted the study to identify the government’s IM priorities for the next three to five years, share agency respondents’ feedback on where gaps exist, and offer suggestions on how to improve on the necessary skillsets.

The survey asked these professionals what skills would be required for future effectiveness. More than half (56%) said they believe information security and access control will be in greatest demand from IM professionals, followed by data quality management (39%) and analytics capabilities – including data sourcing and integration (39%).

In addition, projects related to data privacy (34%), records and information management (RIM) (31%), and data analytics (30%) are thought to be in the greatest demand over the next three to five years.

“This survey provides an important view into the state of federal records and information management, both where the government is now in terms of capabilities and, more importantly, where agencies need to focus their information management practices in the future,” said Michael J. Lewis, vice president and general manager, Iron Mountain Government Services.

The survey of 200 federal employees identified some key focus areas for future success, including:

- *Areas for improvement:* Risk management (34%) is most often cited, followed by electronic records retention (24%) and RIM practices (24%).
- *Most desired skill sets:* Risk management/security/data privacy (54%), analytics (42%), and content/records management (33%)
- *Technical and soft skills in demand:* Information security (52%), innovative thinking (39%), and fostering stakeholder buy-in and delivering C-level and stakeholder communications (15%)
- Ensuring compliance (32%), physical and IT records for-

mat management integration (26%), and information and data valuation assessment (24%)

The data suggests significant gaps between the skills RIM professionals currently have and what they believe they will need in the future. As such, Iron Mountain said agencies should consider focusing on the following in order to close that gap:

- Promote a more holistic approach to IM and sell it internally
- Meet the demand for specialized skills with a focus on information security, quality management, and analytics
- Focus on soft and technical skills in need of improvement and understand why improvement is needed
- Leverage the knowledge and mentoring skills of older staff before they retire
- Provide professional development training in the formats employees most prefer
- Create a forum for sharing ideas and best practices

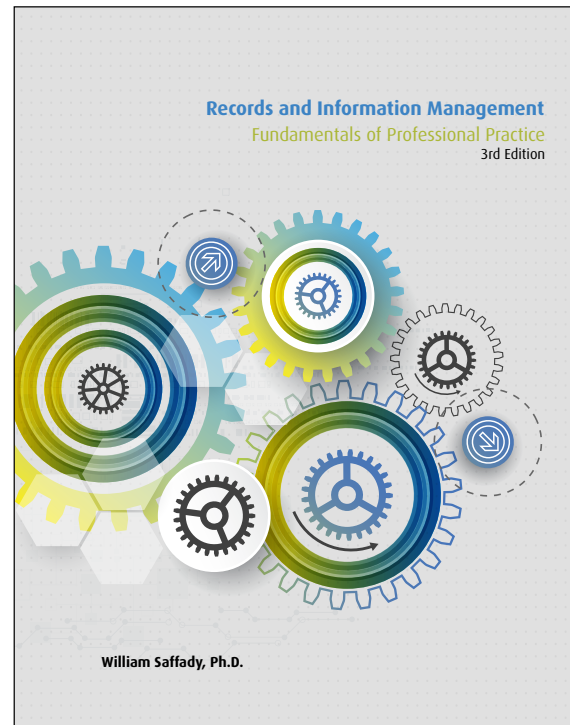
The report is available at www.ironmountain.com/NextGenIMPro.



NEW in the Bookstore

Records and Information Management: Fundamentals of Professional Practice, 3rd. Ed.

William Saffady, Ph.D.



The new edition of this best-selling text has been thoroughly updated and expanded to include more international content and to cover topics not in previous editions, such as information governance and data protection. It is the “go to” book for newly appointed records managers; experienced professionals who want a review of specific topics; supervisors who oversee records management functions; decision makers who develop strategies and tactics for managing information assets; and for students in records management or allied disciplines, such as library science, archives management, information systems, and office administration.

A5026 **\$85.00** Professional members: **\$60.00**
V5026 PDF **\$80.00** Professional members: **\$55.00**

Order online today! **BOOKSTORE** ARMA INTERNATIONAL

www.arma.org/bookstore

INFO SECURITY

Tennessee Enacts Tough Data Breach Law



This month, Tennessee becomes the first state to abolish the “encryption safe harbor” rule, giving it the honor of having the strictest data breach law in the United States, according to data privacy experts.

Encryption safe harbor requires companies who suffer a data breach to notify customers only if the exposed data was unencrypted. Tennessee’s amended Identity Theft Deterrence Act of 1999, which became effective July 1, requires notification even if the breached data was encrypted, according to a *Corporate Counsel* report. The rule requires notice of a data breach to be reported to affected individuals within 45 days unless law enforcement needs more time to investigate. Only a few states have established a set notification time period.

Lastly, the bill amends the statute to specify that an “unauthorized person” includes an employee of the information holder who is discovered to have obtained personal information and intentionally used it for an unlawful purpose. According to the Jackson Lewis law firm, this amendment is likely focused on people who failed to provide notification of data breaches that resulted from improper access by employees.

Some lawyers believe the revised rules will place an undue burden on companies.

“If you’re a company with a laptop stolen in Tennessee, you really

have to ask yourself how you’re going to demonstrate that the bad guys” aren’t going to get access to certain information. Whereas in every other state, “you just have to show that the data is encrypted,” Stephen Embry of Frost Brown Todd told *Corporate Counsel*.

The law doesn’t require notice without question in all circumstances, but experts say the law in Tennessee now makes a distinction between strong and weak encryption that other states are not making, *Corporate Counsel* reported.

GOVERNMENT RECORDS

B.C. Revising its Freedom of Information System

British Columbia (B.C.) will revamp its Freedom of Information (FOI) system by releasing more documents proactively, restricting interference from political staff, and better helping the public access important records, according to B.C. Finance Minister Mike de Jong.

According to *The Vancouver Sun*, de Jong also suggested legislation to force government officials to better document their decisions, and he left open the possibility of eliminating FOI fees altogether as

part of changes he said will increase confidence in the government’s recordkeeping.

“If we are spending public money then the public deserves to know,” he said, adding that contracts, calendars, and scanned receipts for ministerial travel now will be routinely posted online.

De Jong said non-partisan civil servants will oversee the gathering and release of records from the partisan offices of cabinet ministers, and ministers won’t be able to delay signing off on records for more than five days.

“If anything, what we are trying to move to is a system that eliminates entirely the political level of oversight particularly with respect to minister’s offices,” said de Jong.

The federal government recently announced that it would eliminate FOI fees, charging only \$5 per application. De Jong said he’s pondering how to reform B.C.’s fee structure but is considering waiving all fees. The *Vancouver Sun* reported that the B.C. government collects approximately \$60,000 a year in fees on an FOI system that costs \$15.3 million to administer. The government added an additional \$3 million into the FOI system in April, and de Jong said he’d like to see faster FOI responses as a result.



Distrust of Vendors Raises Security, Compliance Questions

Many companies don't trust the vendors they share confidential data with, according to a recent Ponemon Institute survey.

The survey of 600 individuals across industries found that more than a third of U.S. businesses (37%) believe that their primary third-party vendors wouldn't notify them in the event of a security breach involving "sensitive and confidential information." In addition, 73% of respondents said that fourth-party to "nth"-party [an unknown number in a series of numbers] vendors – subcontractors or indirect service providers employed by a third-party vendor – would "fail to notify" if a breach occurred.

The survey, "Data Risk in the Third Party Ecosystem," was commissioned by law firm BuckleySandler and Treliant Risk Advisors to reveal the challenges facing

firms trying to protect client information when sharing data with third parties, according to *Legaltech News*. Companies surveyed have a vendor data risk management program and were asked to consider only their outsourcing relationships in which they share "sensitive or confidential information or involve processes" that require vendor access to that data.

The survey revealed difficulties with "mitigating, detecting and minimizing" risks posed by third parties handling company data. According to the survey, companies lack faith in outside data handling and are not able to properly manage it. The findings show:

- About half (49%) of companies said they experienced a breach caused by vendors, while 16% said they weren't sure if a vendor was to blame.
- 73% of companies said they see

vendor-related cybersecurity incidents increasing.

- Most companies find it difficult to manage vendor-related cyber incidents, with 65% saying they "don't have the internal resources to check or verify" when evaluating vendors' security and privacy practices.
- 58% of companies said they cannot determine whether vendor "safeguards and security policies are sufficient to prevent a data breach," leaving 41% who said they are sufficient.

"The reliance solely upon contractual agreements instead of audits and assessments to evaluate the security and privacy practices creates significant risk," Margo H.K. Tank, partner with BuckleySandler, told *Legaltech News*. "Companies will need to establish and track metrics regarding the effectiveness of the vendor risk management program and establish vendor risk management committees."

According to the survey, for many companies, information governance in vendor relations should be strengthened. For example, only 31% view their vendor risk management program as "highly effective," while 38% said they don't track metrics on their programs' effectiveness. In addition, the majority (62%) admitted that "their boards of directors do not require assurances that vendor risk is being assessed, managed, or monitored appropriately, or they are unsure."

"Companies must understand managing data risk is not merely a compliance and contract issue but a fundamental strategic challenge in which personal data, intellectual property and transactional records must be protected from third, fourth and nth-party risk," Tank said.

GOVERNMENT RECORDS

U.S. National Archives Appoints Permanent Chief Records Officer

Laurance Brewer, the acting chief records officer (CRO) for the U.S. government, has been appointed to fill the position permanently, Archivist of the United States David Ferriero announced in late April.

Brewer's responsibilities include issuing federal records management policy and guidance; serving as a liaison to the Office of Management and Budget, Congress, the Government CIO Council, and other stakeholders on records management issues; and serving as an ombudsman between agencies and the U.S. archivist to ensure that the National Archives and Records Administration (NARA) and the agencies it serves meet their statutory mandates and records management requirements.

Brewer became the acting CRO in October 2015 when the previous CRO, Paul Wester, left NARA to become the director of the U.S. National Agricultural Library. He joined NARA in 1999 as an appraisal archivist and later worked as an electronic records policy analyst. He previously served as a records management consultant at the Environmental Protection Agency and the Virginia Department of Transportation.



Brewer

MOBILE DEVICES

Security Issues May Hamper BYOD Adoption

Analysts are predicting that the global bring your own device (BYOD) and enterprise mobility market will hit \$360 billion by 2020. While BYOD policies are boosting employee productivity and flexibility, security issues may be impeding their growth and implementation, according to a recent survey.

Crowd Research Partners surveyed 800 cybersecurity professionals for the “2016 BYOD and Mobile Security Report.” Around three-quarters of those surveyed reported that their companies implemented BYOD policies for employees, 23% allowed BYOD for contractors, and 16% set up their policies on the company’s partners’ devices. In addition, 14% extended the service to their customers.

More than half of respondents noted that BYOD policies at their companies increased employee mobility, satisfaction, and productivity, while just under half cited reduced costs as an added benefit.

The survey also found, though, that security risks and mobile data breaches are increasing. It revealed that 39% of employees are worried about BYOD security, and 12% have concerns about the privacy of their data. More than 70% of the cybersecurity professionals surveyed cited data leakage or loss as their top BYOD concerns, while a little more than half also cited unauthorized access, user downloads of unsafe apps or content, and malware.

The survey revealed additional key insights on BYOD adoption and risks, including:

- Almost 40% of respondents noted that BYOD devices or corporate devices have downloaded malware, while 21% noted that mobile devices were

involved in security breaches at their companies. About 25% said these devices had connected to a malicious WiFi network.

- One in five organizations suffered a mobile security breach, mainly driven by malware and malicious WiFi.
- Security threats to BYOD imposed heavy burdens on organizations’ IT resources (35%) and helpdesk workloads (27%).
- Despite increasing mobile security threats, data breaches, and new regulations, only 30% of organizations are increasing security budgets for BYOD in the next year; 37% have no plans to change their security budgets.

The majority of respondents (80%) said malware protection and the ability to log, monitor, and report devices were key requirements for confronting mobile security threats. But just 63% said they had password protections for BYOD devices, while fewer than half had remote wipe capabilities (49%) or device encryption (43%).

“While these threats can significantly impact the success of BYOD initiatives and place a burden on IT support staff, this is also an opportunity for organizations to implement effective cybersecurity solutions to strengthen their security posture and capitalize on the promise of enterprise mobility,”



said Holger Schulze, the founder of the 300,000-member Information Security Community on LinkedIn, in a news release.



PRIVACY

Canada Joins Asia-Pacific Privacy Regime

Canada will join the Cross-Border Privacy Rules (CBPR) System, which requires Canadian entities doing business in Asia-Pacific Economic Cooperation (APEC) member economies to comply with minimum requirements regarding cross-border data privacy procedures. The requirements are outlined in the APEC Privacy Framework, published in December 2005, which seeks to provide clear guidance and direction to businesses on common privacy issues and their impact on the conduct of legitimate business.

APEC is a 21-country regional economic forum that seeks to promote economic integration and prosperity for the Asia-Pacific region. A joint oversight panel of the APEC CBPR system submitted a report in April 2015 confirming that Canada met the conditions for participating in the system. That report noted that Canada’s Personal Information Protection and Electronic Documents Act contains provisions relevant to the enforceability of each of the 50 CBPR program requirements.

The United States, Mexico, and Japan have also been certified to participate in the system, and other APEC countries are evaluating their ability to meet the system’s compliance and enforcement requirements.

BUSINESS CONTINUITY

More Businesses Moving to the Cloud for Data Backup

An increasing number of organizations are looking to the cloud to back up their company data, according to Kroll Ontrack research.

Kroll studied the data backup practices of more than 500 companies in North America, Asia, and Europe that have suffered data losses. According to the survey, among companies with no data backup plans, 51% are still considering hard drives for primary data backup, while 23% are considering moving their backup data to the cloud.

When compared to the results of the same survey conducted in 2015, Kroll found that businesses are slowly moving away from external hard drives (down 17% from the previous year) and toward cloud consideration, which has increased by 5%.

Most organizations have procedures in place to back up their

data, but challenges remain.

“Maintaining a traditional backup solution takes time and due diligence. For instance, think about the exponential growth in data volumes that IT teams are handling and backing up. That growing volume translates into time—significant time,” said Todd Johnson, vice president of data



and storage technologies at Kroll Ontrack. “And it’s not a ‘set it and forget it’ process. Backup health requires regular testing and auditing to not only ensure the backup is working properly, but to confirm it includes all the necessary media to meet preservation and compliance requirements. It’s a huge balancing act, particularly for smaller to midsize organizations with limited IT support infrastructure.”

Interestingly, Kroll found that at the time of data loss, 14% of companies did not have a data backup in place. Perhaps not surprisingly, 58% relied on external hard drive solutions while about 16% used the cloud. Eleven percent said they used network-attached storage.

Of those without backup solutions, 54% said not having enough time for administration and research was their reason for not implementing a solution. Notably, fewer companies cited expense as a reason for not backing up data than in 2015—a 7% decline, according to Kroll.

DIGITAL PRESERVATION

Microsoft Experimenting with DNA for Digital Storage

Microsoft said it plans to acquire 10 million strands of DNA from Twist Bioscience to use for digital storage experiments. Twist Bioscience is a San Francisco-based biology startup that makes synthetic, storage-ready DNA, according to *Tech Times*.

“As our digital data continues to expand exponentially, we need new methods for long-term, secure data storage,” said Doug Carmean, a Microsoft partner architect in its Technology and Research organization. “The initial test phase with Twist demonstrated that we could encode and recover 100% of the digital data from synthetic DNA. We’re

still years away from a commercially viable product, but our early tests with Twist demonstrate that in the future we’ll be able to substantially increase the density and durability of data storage.”

Compared to traditional storage systems, the data density offered by DNA is significantly higher. According to *Tech Times*, 1 gram of DNA is equivalent to nearly 1 billion terabytes (or 1 zettabyte) of data. It also is far more robust than conventional storage systems as is evidenced by the fact that DNA fragments that are several thousand years old can be sequenced successfully.

Another advantage of DNA is that it will stay unharmed and



readable for between 1,000 to 10,000 years.

Microsoft research estimates that 1 cubic millimeter of DNA can store 1 exabyte, or 1 billion gigabytes, worth of data, making the use of DNA for digital data archival a viable option long term, *Tech Times* reported.

EHRs

U.S. Nears 100% EHR Adoption

Ninety-six percent of U.S. hospitals are using certified electronic health records (EHRs), compared with 72% in 2011, revealed a survey released at the 2016 annual meeting of the Office of the National Coordinator for Health Information Technology (ONC) in Washington, D.C.

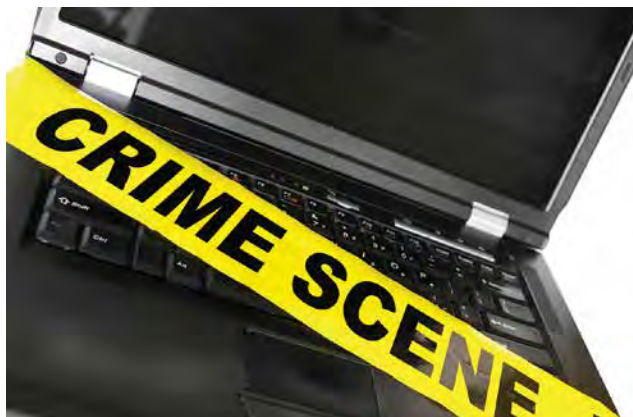
“Data showing the nearly universal adoption of certified electronic health records are an indication of how far we have come for clinicians and individuals since the HITECH Act was passed,” National Coordinator for Health Information Technology and Acting Assistant Secretary for Health Karen DeSalvo said in a statement.

Introduced in 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act has led to an increase in the adoption of health IT, *eweek.com* reported.

According to the survey, just 9% of non-federal, acute-care hospitals used basic EHRs in 2008, while 84% use them today; in 2011, 72% used certified EHRs, and today 96% do.

Small, rural, and critical-access hospitals are not as up to speed; however, since 2014, small, rural hospitals have increased their adoption of basic EHRs by 14%, and critical-access hospitals have increased adoption by 18%, *eweek* said.

The rate at which information – such as radiology reports, care summaries, and lab results – is being exchanged has doubled since 2008, from 41% to 82% in 2015, the report found. And even between 2014 and 2015, the percentage of hospitals using, sending, receiving, and finding key clinical information “grew significantly,” from 23% to 26%.



E-DISCOVERY

U.S. Appeals Court Allows Search of Old PC Files

In a closely watched case, a U.S. appeals court has ruled that federal agents acted in good faith when executing a warrant to search records that had been seized two and a half years earlier.

The 12-to-1 decision by the Second U.S. Circuit Court of Appeals in New York restored a Connecticut accountant's 2011 jury conviction and two-year prison sentence for tax evasion, Reuters reported. A three-judge panel had overturned both in June 2014.

Stavros Ganias' computer files were seized in November 2003 by U.S. Army investigators examining possible overbilling by a military contractor that had employed Ganias as an accountant, according to Reuters. But instead of purging unnecessary files, the government held onto them, and in April 2006 got a warrant to search them for evidence of unrelated tax evasion by Ganias.

While the appeals court decision tested how long the government can keep a criminal suspect's computer data, the court did not answer the question of whether keeping the records for that long violated the suspect's Fourth Amendment rights.

In the 2014 ruling that voided the jury verdict, Circuit Judge Denny Chin, who was the lone dissenter in the most recent decision, said the government went too far by searching computer records it had long considered irrelevant for evidence of a new crime.

The majority, in its 60-page opinion, did not address that issue but did warn law enforcement to be more careful, citing “significant” privacy concerns and Fourth Amendment issues arising when the government retains hard drives and other digital media containing vast troves of personal information, “much of which may be entirely irrelevant to the criminal investigation that led to the seizure,” Reuters reported.

Chin, in his 40-page dissent, said the “cloud” that has hung over Ganias' head for the last 13 years should be lifted.

“The government did precisely what the Fourth Amendment forbids: it entered Ganias' premises with a warrant to seize certain papers and indiscriminately seized – and retained – all papers instead,” he wrote.

Ganias' lawyer said he was reviewing the decision and might appeal to the U.S. Supreme Court.

229 Strong. And Growing.

Congratulations to these Certified Information Governance Professionals

Mitchell Abrams
Elizabeth Adkins
Angela Akpapunam
Xavier Alabart
Anthony Allen
Pey-Jia Angell
Christine Ardern
Deborah Armentrout
DeAnna Asscherick
Randy Aust
Wendy Austin
Christie Baird
Robert Baird
Patty Baldacchino
Salvador Barragan
Christopher Beahn
Shawn Belovich
Richard Berlin
Mike Biancaniello
Margaret Boeringer
Isabel Bracamontes
Aaron Bryant
Susan Burd
Kiji Burstn
Doug Caddell
Stacie Capshaw
Melissa Carlis
Diane Carlisle
Laurie Carpenter
Elizabeth Carrera
Alexander Carte
Mark Carter
Peter Casey
Anita Castora
Elizabeth Castro
Tod Chernikoff
Carol Choksy
Vicki Clewes
Andrew Cogan
Julie Colgan
Bud Conner
Dani Cook
Russ Cottle
Marvin Cross
Kristen Crupi
Becky Darsch

Lisa Marie Daulby
Nicholas De Laurentis
Melissa Dederer
G. Derk
Deborah Dotson
Christina Doyle
Sandra Dunkin
Priscilla Emery
Sarah Emes
Sofia Empel
Tony Epler
Debra Farries
Elizabeth Farthing
Carol Ann Feuerriegel
Clinton Field
Glenn Fischer
Matt Fisher
David Fleming
Mariel Fox
Patricia Franks
Audrey Gaines
Rhonda Galaske
Caroline Gallego
Claire Galloway Jenkins
Stephen Garner
Charles Garrett
Irene Gelyk
Celine Gerin-Roze
Sue Gerrity
Kimberly Giertz
Susan Goodman
Joshua Grisi
Komal Gulich
Jocelyn Gunter
Allen Gurney
Michael Haley
Grace Hammar
Joshua Hargrafen
Paula Harris
Julie Harvey
Matthew Hebert
Charles Herbek
Margaret Hermesmeier
Caroline Higgins
Gordon Hoke
Patricia Huff

Janice Hulme
Bethany Hynes
Nicolas Inglis
Leigh Isaacs
Mary Janicik
C'Les Jensema
Chris Johnson
Elizabeth Johnson
Kurt Johnson
Todd Johnson
Deborah Jostes
Deborah Juhnke
Soo Kang
Andrew Keller
James Kennedy
Anju Khurana
Ellie Kim
Michelle Kirk
Monica Kirsch
Tamara Koepsel
Greta Krapac
Peter Kurilecz
Tera Ladner
Richard Lang
Ronald Layel
Anna Lebedeva
Gilles Legare
Donnell Long
Howard Loos
John Loveland
Eric Lynn
Cindy MacBean
Mark MacFarlane
Rudolph Mayer
Brian McCauley
Stephanie McCutcheon
Cheryl McKinnon
Felecia McKnight
James Merrifield
Bruce Miller
Sandy Miller
Dana Moore
Dermot Moore
Rafael Moscatel
Linda Muller
Jen Murray

Stephen Murray
Deborah Naas
Joe Nadzam
Lindy Naj
Peggy Neal
Lee Nemchek
Kurt Neumann
Sheri Nystedt
Shanna O'Donnell
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
Angel Ramos
Tony Ratcliffe
Joshua Rattan
Scott Raynes
Jessica Rickenbach
Deborah Rifembark
Carol Rittreiser-Coritt
David Rohde
Donna Rose
Shawn Ryan
Kathryn Scanlan
Danna Schacter
Tonia Schneider
Teresa Schoch
Terry Schrader
Karen Schuler
Jason Scott
Karen Shaw
Mary Sherwin
William Silvio
David Skweres
Doug Smith
Kathleen Smith
Michael Smith
Kirke Snyder

Natalie Spano
Brian Starck
Jason Stearns
David Steward
Courtney Stone
Melissa Suek
Lisa Summers
Paula Sutton
Marjorie Swain
Sheila Taylor
Robin Thompson
Kathleen Timothy
Louis Tirado
Brian Tretick
Susan Trombley
Nathan Troup
Brian Tuemmler
Martin Tuip
Amy Van Artsdalen
Paul Van Reed
James Vardon
Katharine Voldal
Jennifer Watters Farley
Alexander Webb
Katherine Weisenreder
Bridgett Weldner
Erik Werfel
Steven Whitaker
Kristi Whitmore
Jesse Wilkins
Marc Willemse
Dylan Williams
Steven Williams
Natausha Wilson
Rick Wilson
Terri Wilson
Brett Wise
Jennifer Witt
Kristin Wood
Robin Woolen
Jeffrey Yawman
Cheryl Young
Margo Young
Andrew Ysasi
Ryan Zilm

Application deadline: November 12, 2016.

Register today at www.arma.org/igp.



INFO GOV PROGRAMS

Firms Must Focus More on Information Governance, Lawyers Say

Firms just aren't paying enough attention to information governance (IG), according to corporate in-house counsel interviewed for Kroll's 2016 Corporate Risk Survey.

The 170 lawyers taking part in the survey cited the following

as the most pressing issues facing their firms: data security, cybersecurity, and privacy risks, including the loss of personally identifiable information.

Almost half of respondents (47%) said their companies do not have an IG program in place. Ac-

cording to the survey, another 26% think their programs lack the resources needed to be effective.

The survey also found that 59% of lawyers reported that their organization's data breach or incident response plans are inadequate or non-existent.

Other findings include:

- Data security is "the most significant risk facing modern corporations." Most (76%) in-house counsel said there are effective safeguards in place to protect their organization's intellectual property, but only 41% said their company's plan is regularly updated and tested.
- Two-thirds of respondents said their firms are more at risk of external fraud, while 33% believe their risk of internal fraud is higher.
- For fraud, 85% of organizations conduct due diligence on proposed business partners and 76% maintain internal resources to investigate fraud in the United States. But almost two-thirds lack the internal resources needed to investigate global fraud incidents.
- Organizations are using most of their compliance budgets for risk assessments and policy creation and management. In-house counsel said they want to spend additional funds on compliance training and technology systems to facilitate compliance screening.

According to Kroll, the survey shows that "organizations are making noteworthy strides as a result of the new risks facing the enterprise. Nevertheless, the survey also reveals that organizations have additional room to evolve if they seek to combat these modern risks in an efficient, cost-effective manner."



INFO GOV PROGRAMS

Survey: Unstructured Data a Growing Challenge

While most companies are aware of the importance of information governance (IG), many do not have insight or control over employee-produced data, according to a recent survey from Acaveo and Osterman Research.

They surveyed more than 100 organizations that stored an average 20 TB of unstructured data and found that only 37% of them regularly audited the amount of data employees or business units produce. Just 35% said they had a budget in place to deal with unstructured data challenges.

Overall, while many companies admitted to struggling with governing unstructured data, only half of the surveyed companies said they have an IG program in place to help deal with it.

But they do understand the importance, as 70% cited regulatory risks and 66% cited the need to avoid any data risks as reasons to adopt an IG program. In addition, 75% of respondents noted the savings IG can bring to storage costs. Other findings include:

- 55% of organizations perform regular file share cleanup exercises.
- 40% of organizations have a "defensible deletion" program in place.
- Of the companies that have an IG program, 75% justify the program based on storage costs.

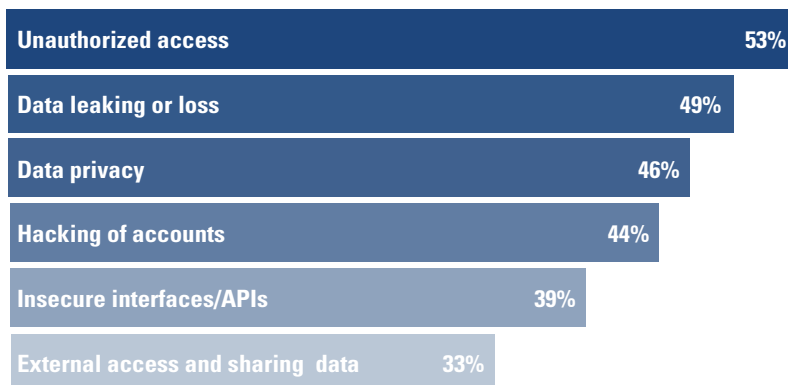
Notably, the survey predicts that the proportion of unstructured data stored in-house will increase from 22% currently to 25% in just two years, while cloud storage will comprise a bit less than half of an organization's information repositories in at least five years.

CLOUD COMPUTING

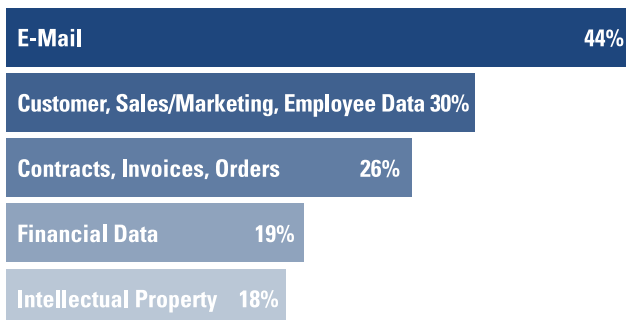
Are Cloud Security Concerns Overblown?

Greatest Threats to Cloud Security

More than 2,000 professionals surveyed by Cloud Research Partners cited the following obstacles to cloud security:



Percentage of Companies Storing These Data Types in the Cloud



While security concerns over cloud adoption are the greatest barrier to adoption among businesses, a recent survey found that few have actually suffered a cloud-related security incident.

The *Cloud Security Spotlight Report* by Crowd Research Partners surveyed 2,200 consultants, specialists, executives, IT, and other professionals across a variety of industries and found that more than half (53%) of respondents expressed concern over the security of their data in the cloud, an increase from 45% in 2015, *Legaltech News* reported.

Interestingly, however, when asked if they had suffered a cloud-related security incident, only 9% said yes, while 36% could not disclose or did not know of any inci-

dent, and 55% said they had not had any cloud-related security issues, the survey found.

If the survey findings are any indication, respondents may be confused about how secure the cloud really is. For example, 22% of respondents said there was a lower risk of breaches from the cloud compared to data hosted on premises servers, while 21% said the opposite, and 27% said they believed security for cloud and on-premises storage was about the same.

Legal and regulatory compliance concerns were also cited as a barrier to cloud adoption by 42% of respondents in 2016, up from 29% in 2015. The survey noted, however, that “the rise in specific concerns about compliance and integration suggests that companies

are moving from theoretical exploration of cloud models to actual implementation.”

According to *Legaltech News*, factors driving these concerns include the recently approved General Data Protection Regulation in Europe and cybersecurity disclosure and data regulations, which require companies to consider where their data is being stored and processed. The full report may be downloaded at www.crowdresearchpartners.com/portfolio_item/cloud-security. **END**



CISCO® GLOBAL CLOUD INDEX

Data Center Virtualization and Cloud Computing Growth

- By 2019, 86% of workloads will be processed by cloud data centers; 14% will be processed by traditional data centers.
- Overall data center workloads will more than double from 2014 to 2019; cloud workloads will more than triple (3.3-fold) over the same period.
- The workload density (that is, workloads per physical server) for cloud data centers was 5.1 in 2014; it will grow to 8.4 by 2019. Traditional data centers' workload density was 2.0 in 2014 and will grow to 3.2 by 2019.

Integrated ECM Solutions: **Where Records Managers, Knowledge Workers Converge**



By using examples from Gartner’s 2015 “Magic Quadrant for Enterprise Content Management,” this article offers a brief introduction to three ECM systems, provides examples of integrated solutions used by knowledge workers, and discusses the contributions records managers can make to support business processes.

Patricia C. Franks, Ph.D., IGP, CRM, CA, FAI

There are numerous challenges to ensuring that captured data is useful. As noted by former U.S. Magistrate Judge Ronald J. Hedges in a 2016 presentation, “The Positive Power of the Destruction of Data,” data is voluminous and distributed, is fragile yet persistent, takes many forms, and is created and maintained in complex systems.

Data can be found on personal computers at work

and home; laptops, smart phones, and tablets; networked devices (i.e., the Internet of Things); digital copiers; removable media (e.g., disks, flash drives); and with third-party providers. Increasingly, content resides within an enterprise content management (ECM) system – on premises, in the cloud, or both – and is in continual use by *knowledge workers*, whose jobs primarily involve creating, distributing, or applying knowledge.

The Need to Understand Content's Value, Use

Knowledge workers must understand the value of content to the organization and be able to handle it responsibly regardless of their role within the information life cycle – whether as creator, user, or manager. At the same time, records managers must be able to provide access to the right content – regardless of its status as information or record, its format, or its location – to the right person at the right time and in the right place.

The integration of an ECM system with other business solutions establishes a point of convergence for knowledge workers and records managers:

1. Having the ability to categorize content without referring to a records retention and disposition schedule allows knowledge workers to focus on their core business function while complying with records management policies.
2. Understanding how the ECM system is being used enables records managers to design better rules and workflows to perform their tasks.

ECM as the Basis for Integration

AIIM first defined ECM in 2000 and has expanded upon its description several times. Currently on AIIM's website, *ECM* is described as “the strategies, methods and tools used to capture, manage, store, preserve, and deliver content and documents related to organizational processes.”

Anand Rao, in a 2007 white paper “Knowledge Management using Enterprise Content Management System,” wrote, “Content generated by the organization, once effectively tagged and stored for efficient retrieval, forms the knowledge bank of the organization.”

This paper reinforces that ECM was not a new product category, but an integrative force. Integration can take place between an ECM system and applications a vendor already offers, creates specifically for the system, or acquires in order to differentiate its product from others on the market. Integration also takes place between the ECM and the products of other vendors.

Gartner's 2015 “Magic Quadrant for Enterprise Content Management” ranked ECM vendors as leaders, visionaries, challengers, or niche players based on seven application areas:

1. Document management
2. Web content management
3. Records management
4. Image-processing applications
5. Social content
6. Content workflow
7. Extended components, including mobile applications, digital asset management, search, analytics, and packaged integration capabilities.

By using examples from the Gartner report, this article offers a brief introduction to three ECM systems, provides examples of integrated solutions used by knowledge workers, and discusses the contributions records managers can make to support the business process.

Example 1: Social Media Solutions and ECM

Microsoft is identified as a leader in Gartner's “2015 Magic Quadrant for Enterprise Content Magic.” It has incorporated content management capabilities in SharePoint for more than a decade. Although the capabilities of SharePoint Online are not as complete as those of SharePoint On-premises, the cloud version best illustrates the point of convergence for knowledge workers and records managers.

The Office 365 Security and Compliance Center allows the administrator to add security and retention policies, search and investigate both content and audit logs, and view reports.

Sharing Knowledge

Office 365 and SharePoint Online comprise an easy-to-implement combination that can be used to create and manage content. Users can “like” a library document or add a “star” tool to indicate approval. They can use Yammer, a private social network, to engage in conversations around projects and files.

Social features such as user profiles, blogs, wikis, and newsfeeds enable knowledge workers to communicate and collaborate. The *Ask Me About* section of the user's profile provides a means to identify colleagues with specific expertise. Participation in community discussions can result in points and badges to reward contributions and help build reputations.

Knowledge workers can personalize content across Office 365 from One Drive for Business, SharePoint Online, Exchange, Yammer, and more by using Office Delve as a personal portal. When a document or board of interest is found, it can be added to Delve as a favorite (see Figure 1 on page 20) so it can be returned to easily.

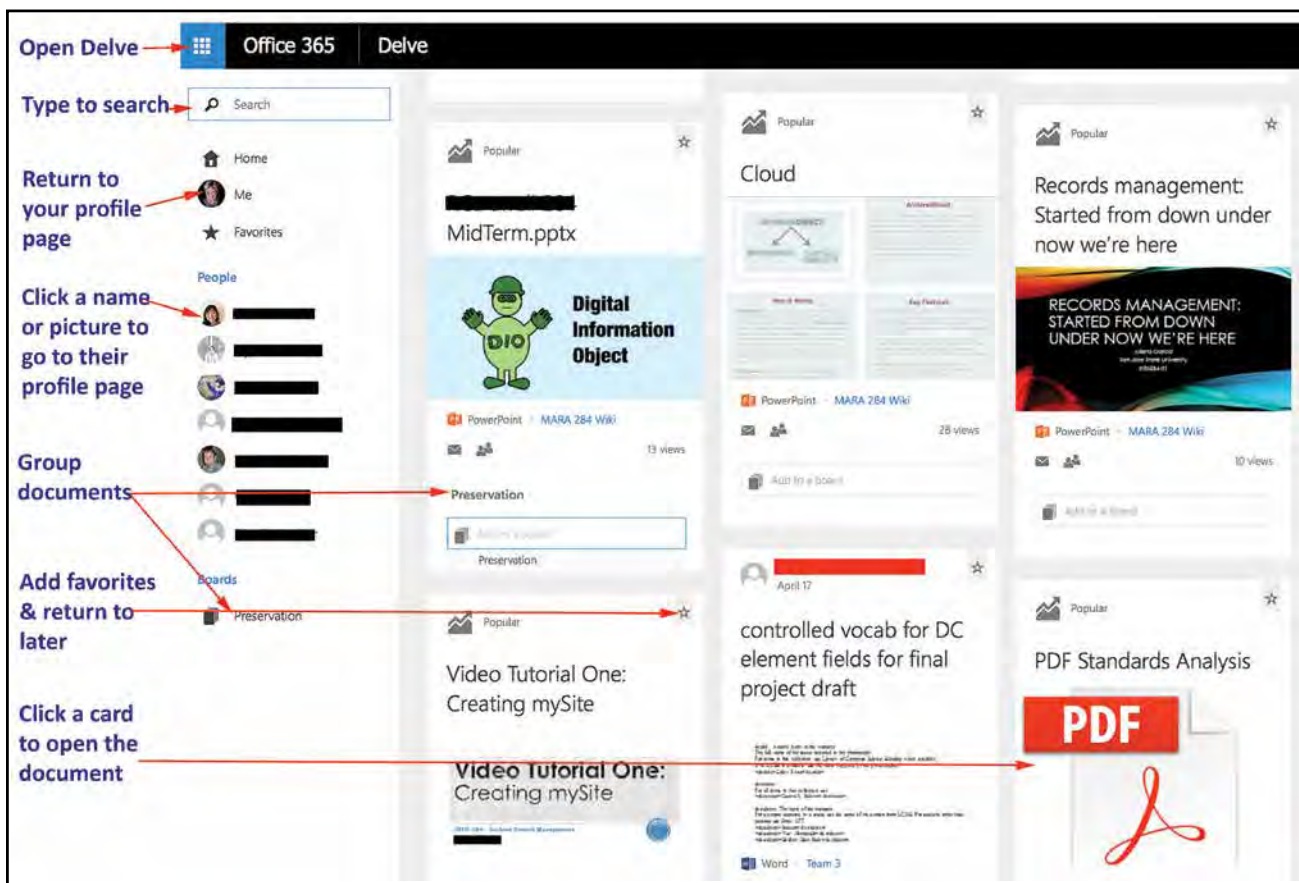


Figure 1: Delve helps users discover information across Office 365.

Numerous apps are available for Office 365/SharePoint Online to enable users to analyze and present data. When the ECM is integrated with web-based BlackCompass Visualizer for SharePoint, for example, data can be presented as visual columns in lists and data points on maps.

Managing Records in Office 365/SharePoint Online

SharePoint Online offers out-of-the-box records management features. A dedicated records center site can be created to serve as an archive, with documents copied to it based on the retention policy. Records can be managed “in place” by declaring them records and applying security and retention properties in their current location. Or a hybrid approach can be taken.

If the records manager is responsible only for records, moving them to a records center is often the preferred option. Metadata is used to manage records based on content types, content organizers, and virtual folders. Hierarchical file plans are used to manage retention and generate reports. Enterprise-wide taxonomies and content types ensure consistency and context transfer between collaborative spaces and the archive.

If records managers are responsible for all information,

managing records in place provides control over content in collaborative spaces. Documents such as wikis, blogs, web pages, and list items can be declared records while in use to prevent deleting or editing. This can be accomplished manually, through the use of a workflow, or according to the document’s retention period. Records can be managed across multiple sites, and automatic versioning of records can be enabled.

The Office 365 Security and Compliance Center allows the administrator to add security and retention policies, search and investigate both content and audit logs, and view reports. SharePoint Online offers compliance with the Health Information Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA), ISO/IEC 27001 *Information technology – Security techniques – Information security management systems – Requirements*, the Family Educational Rights and Privacy Act (FERPA), SSAE16, EU Model Clauses, and U.S.-EU Safe Harbor framework out of the box.

SharePoint extenders provide additional features, such as case file management, event-based retention, and support for physical records management. Third-party extenders are available from Collabware, Gimmel, and Records365.

Example 2: Business Process Management and Content Management

OpenText is the second-largest ECM vendor in terms of worldwide market share and is identified as a leader on the 2015 Magic Quadrant (Gartner, 2015). OpenText provides ECM solutions for cloud-based, hybrid, and on-premises deployments. The company's focus on aggregating, managing, and sharing information to drive productivity illustrates a move from the view of document and records management systems as a cost of doing business to the realization that ECM systems can provide a means to improve productivity and control.

Improving the Business Process Through Process-Centric Workspaces

OpenText's Cloud Accelerated ECM allows knowledge workers to manage content in the context of their business processes. The centralized repository uses a variety of devices to provide users with access to content when needed from almost any location. Rather than focusing on documents or records, it focuses on the operational problems the organization faces by providing collaborative, process-centric workspaces with pre-built taxonomy, built-in metadata, and compliance capabilities. A knowledge worker can set up a new business workspace to aggregate content and people. Information flows can automate the creation, review, approval, publishing, and storage of content.

Transforming the Business Process: Open Text Extender for SAP® Solutions

An alternative to working within the ECM environment is the ability to access content stored within the ECM from within a business solution. The OpenText Extender for SAP Solutions integrates the ECM with the SAP Business Suite to allow the knowledge worker to "access the right information at the right time in the right place." The right place in this case means while working within SAP.

The SAP Business Suite contains businesses processes – including case management, vendor invoice management, and HR processes – that deal with large volumes of content in various formats that must be captured, managed, preserved, and delivered to the user.

A knowledge worker providing customer support, for example, could access the customer file to view both structured and unstructured information about the customer's past transactions. Documents like "contracts" can be created using templates from within SAP. This solution connects unstructured content from within the ECM with structured content within the SAP business process. The results are efficient customer service and increased employee and customer satisfaction.

E-mail messages, attachments, documents, and other assets can be dragged and dropped into a customer folder in SAP-extended ECM without changing programs. Documents stored in SAP can be located using simple search functions; for example, an invoice stored in SAP could be located by entering the invoice amount in Extended ECM.

The Records Management Perspective

The Open Text Extender for SAP Solutions adds data and document archiving, imaging, document management, collaboration, U.S. Department of Defense 5015.2-certified records management, and application-spanning virtual views of related information to the SAP system.

... because of the pre-defined business workspaces and pre-built metadata, classification of content is transparent to knowledge workers and allows retention policies to be applied to related content.

Records managers play a vital role in executing strategy, but because of the pre-defined business workspaces and pre-built metadata, classification of content is transparent to knowledge workers and allows retention policies to be applied to related content.

Records managers create a file plan and manage retention schedules without interfering with any department's line of business. Once the system is configured, users continue to carry out business activities while records managers control ultimate file indexing, archiving, and disposition.

Example 3: Decision Making and Content Management

Laserfiche is considered a niche player in the ECM arena. The majority of its customers come from the government, financial services, higher education, and health care. Laserfiche ECM solutions focus on document management, records management, imaging, and workflow applications.

In addition to on-premises deployments, Laserfiche offers public hybrid options and works with partners to offer dedicated (hosted) private cloud options. Laserfiche

ECM has long provided packaged integrations to Salesforce, SharePoint, and other applications.

In 2015, it announced *Laserfiche Connector* to enable partners and developers to extend the functionality of Laserfiche with new actions that are context-specific. Laserfiche offers tools for information capture, mobile access, integration, and analytics.

The reality is that both paper and electronic records will be created as a normal part of daily activities in some organizations, resulting in complex hybrid record environments.

Capturing Content

The reality is that both paper and electronic records will be created as a normal part of daily activities in some organizations, resulting in complex hybrid record environments. Government services, for example, exist to support citizens in need of financial assistance, medical care, housing needs, child care, and more. Some client records are completed in physical form and must be scanned for capture by the ECM.

During the capture process, data can automatically be extracted from electronic, PDF, and scanned forms. Photos can be uploaded from mobile devices and cameras directly into client files. Clients can submit information using e-forms with attached documents. Clients can sign documents electronically to reduce processing time.

Salesforce and Content Management

Salesforce is the world's most popular customer relationship management (CRM) solution. Most knowledge workers spend their time in business applications like Salesforce. But those applications don't hold all of the information the workers need. With Laserfiche's Connector, Salesforce users have the ability to view associated and background information held in Laserfiche without leaving the primary application. Workers in Salesforce can scan documents into Laserfiche; metadata values are populated from the data in Salesforce.

Information stored in both Laserfiche and Salesforce

can be analyzed, shared via reports, and used to drive the organization's business strategy. Team members can see their own work and the activities of other team members in the form of charts and graphs. Managers can gain insight on workloads and staff performance to identify problems and take corrective action. Data can be overlaid on data from other sources, such as a city map.

The Records Management Perspective

Laserfiche is a DoD 5015.2-certified records management application. As such, it provides automatic capture, transfer, storage, and disposition of new and legacy records; enables employees in different departments to access records without navigating the master records structure; and automatically creates custom views of records structures for auditors or compliance officers.

Laserfiche applies retention and disposition schedules and rules to incoming records using metadata, creates record folders and moves documents into the appropriate locations, sends document destruction notifications, enforces records management policies across all devices, and generates reports to identify and locate records ready for disposition.

The role of the records manager is a strategic one: to develop the policies and workflows that automate records management functions and are transparent to knowledge workers so they can concentrate on their primary objective.

Integrated Solutions = Integrated Environment

ECM systems have evolved from little more than document management systems to robust integration hubs. Through the use of connectors provided by the ECM vendor or developed by others, ECM systems provide a means for knowledge workers to access unstructured content residing in the ECM while remaining within the business application. Mobile apps for smart phones and tablets allow employees to conduct work while away from the office.

Records management functionality is present in most ECM solutions, but the range of features varies widely. Third-party solutions exist to extend records management functionality to meet governance and compliance standards.

Integrated solutions provide an environment in which knowledge workers and records managers co-exist. Due to the increased automation of records management functions within ECM systems and business applications, records managers can assume a more strategic role by developing policies, implementing controls, and selecting tools for the governance of the organization's digital assets. **END**

Patricia Franks, Ph.D., IGP, CRM, CA, FAI, can be contacted at patricia.franks@sjsu.edu. See her bio on page 47.



NEW



HotTopic

FREE!
Digital Info
Register today at www.arma.org



Technologies and Trends for
Managing, Using, and Securing Digital Information

Online with **updated** content

Don't miss these valuable articles featured in the newest *Hot Topic*:

- **Securing Confidential Customer Data and Gaining Content Clarity** Isabell Berry
- **Managing Legacy Data Through the Migration Process** Soo Kang, IGP, CIPP/US
- **In-House Elevated: Catching the Third Wave of E-Discovery** Brad Harris
- **Digital Preservation of Long-Term Records at the Associated Press** Mike Quinn
- **Bring Your Own Policy: How Corporations are Managing Mobile Devices for E-Discovery** Kevin DeLong
- **Information Governance: Don't Move to the Cloud Without It** Mark Daniel
- **More Data Equal More Privacy Concerns: Is Your Organization Prepared to Handle Them** Mark Daniel

<http://bit.ly/28LBEot>

Five Steps In-house Counsel Should Take to Mitigate Information Risk

H. Kirke Snyder, J.D., IGP

In-house counsel need to collaborate with key information governance stakeholders to help resolve their sometimes-conflicting information management goals and ensure that the IG program has the executive support and resources needed for the organization to achieve its core mission while preventing or mitigating risks.

Because of the risks associated with electronically stored information (ESI), organizations need a strategic information governance (IG) framework that addresses records and information management (RIM), data privacy and security, and e-discovery. If senior management fails to provide the framework, each department's perspectives will drive its data management goals. Their differing perspectives, though, can drive conflicting data management goals and can complicate or circumvent the organization's ability to govern its information effectively.

Perspectives That Produce Conflicting Goals

For example, the RIM perspective is driven by the records retention schedule, so one of its data management goals is to ensure that information is kept as long as – but no longer than – needed to meet legal/regulatory, fiscal, historical, and operational requirements. But, IT's perspective is driven by the need to manage storage costs, so it may establish e-mail account volume limitations that lead to e-mail records being disposed of before their retention requirements have been met, in conflict with RIM's goals.

The legal department perspective is driven by the need to avoid judicial sanctions for spoliation, so it may issue broad legal holds that cause information that is not relevant to litigation or regulatory actions to be retained longer than it should be, in conflict with both RIM and IT's goals.

Finally, business units, which are focused on data accessibility and convenience, may utilize third-party cloud data storage applications that put the organization's information outside of the organization's control, where it may not be secure and cannot be managed properly – in direct conflict with RIM, legal, and IT goals.



This is why effective IG requires senior management to collaborate with key stakeholders, hear all perspectives, gain an understanding of how the organization should best manage its information to achieve its core mission while preventing or mitigating risks, and to enlist executive support for appropriate people and financial resources.

The chief legal counsel has a critical role to play in this. Because the American Bar Association's Model Rule 1.1 requires lawyers to provide "competent" representation to clients – in this case their employing organization – in-house counsel can't afford to assume that IT and RIM personnel will get all the legal intricacies right, given the potential legal and financial risks of unmanaged information. The insights and practical advice offered below could help legal counsel save their organizations millions in fees and expenses.

Trends That Stem from Flawed IG

Flawed IG is causing three disturbing trends that carry significant legal and financial risk to corporate America, and in-house lawyers should not be sitting on the sidelines waiting for their number to be called.

Growing Number of Data Breaches

The first trend is the theft of ESI. Data breaches occur virtually every day (e.g., Sony, Target Corp., Home Depot, JPMorgan Chase), with significant reputational and financial costs for organizations. According to the 2015 "Cost of Data Breach Study: Global Analysis" conducted by Ponemon Institute and commissioned by IBM, the average cost of a data breach incident was \$3.8 million.

Rising Cost of E-Discovery

The second trend is the rising cost of e-discovery, which directly affects an organization's law department budget. The 2012 report "Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery" by the Rand Corporation found that U.S. corporations typically spend at least 70% of their litigation budgets on document review.

Exploding Volume of E-Records

Part of the reason document review takes so much of the budget is that it's common for lawyers to sift through documents and e-mail produced for discovery multiple times. But this cost could and should be much lower, as the vast majority of e-mail and documents collected, preserved, and reviewed is typically obsolete and should have been destroyed during the normal course of business in accordance with the organization's records retention schedule.

Even when organizations have a formal written records retention policy and retention schedules, they may not be fully implemented and are rarely audited, which may be

due to lack of executive support for the RIM program to be sufficiently staffed or funded.

5 Steps That Will Mitigate Information Risk

While lawyers may hesitate to get involved in helping resolve the issue of ungoverned information because they don't feel trained or empowered to do so, they must roll up their sleeves and step in – pre-litigation discovery. Once a data breach has occurred or a legal hold of information that should have been destroyed is in place, in-house counsel will have to be involved, but at that point it's too late to save the organization from its poor housekeeping. Here are five actions they can take.

1. Role Play a Rule 30(b)(6) Deposition

Rule 30(b)(6) of the Federal Rules of Civil Procedure (FRCP) and the corresponding state rules require an organization faced with e-discovery to designate officers, directors, managing agents, or other persons to testify under oath as to matters known or reasonably available to the organization (e.g., information management and document retention). These 30(b)(6) depositions can be a nightmare for the unprepared.

Don't wait for the onset of litigation; identify the individuals who will be designated to testify for a deposition and play the role of a plaintiff lawyer by asking typical Rule 30(b)(6) questions about document management systems, information management policies and procedures, and the data deletion process. This exercise will help prepare the "deposed" individuals and reveal a more accurate picture of any RIM vulnerabilities.

Counsel may find that many record types are not destroyed according to policy and schedule, and that multiple copies of "records" are stored in the basement, offsite, on the shared network, in the e-mail application, within SharePoint sites, and on third-party cloud systems.

2. Challenge IT to Create a Data Map

Under the FRCP, parties must cooperate to reveal everything about their ESI, including location, type, source, and format. In addition, litigators must come to the FRCP Rule 26 "Meet and Confer" with an understanding of the nature, variety, and kinds of electronic storage media involved; how to retrieve data; the types of electronic data; the format in which the electronic data is stored; and the expense of collecting and preserving the data. In effect, these requirements are tantamount to requiring the parties to produce a data map of their potentially relevant information.

Without specialized technology, an IT department can exhaust significant resources creating a data map for a single litigation. The map must consider listing the core records from important production systems and applica-

tions, along with data stored in the cloud, data from the computers of individual employees, data from applications that are no longer in use, and even the contents of CD-ROMs and backup tapes.

Don't wait for litigation to prompt learning about the ability of IT and RIM to create a litigation data map. As with the mock 30(b)(6) depositions, give the IT department a date range, a list of key employees, a description of topics and key words, a specific deadline, and an evaluation of its work product. This preparation is not "busy work." It will save the organization 10 times the investment.

- Act upon a group of selected files (e.g., copy, move, delete)
- Discover the department (or employee within the department) that created or owns the data
- Identify duplicate or near-duplicate documents and move the final record copy to a secure location

Enterprise records management software provides manual or systematic storage and retrieval of documents and e-mail with record value. It makes records widely available at any location as a searchable repository for shared knowledge, compliance, and litigation support. Such

To cost-effectively manage its data assets (both proactively and in response to a legal action), the organization must have the technology to easily identify, copy, move, protect, and destroy ESI throughout the enterprise.

3. Convince Senior Management of Resource Needs

Armed with insights acquired from the mock Rule 30(b)(6) deposition and the data map exercise, counsel can begin convincing senior management that a legally defensible RIM program is not optional. Senior management must understand that the improved RIM program may require new computer hardware, software, and training. Specialized technology tools will help lock down records in a safe place and identify files with personal data for encryption or destruction.

Too often, the RIM and IT departments lack the budget to acquire the very tools that could save the organization millions by mitigating the likelihood of a data breach or litigation e-discovery. To cost-effectively manage its data assets (both proactively and in response to a legal action), the organization must have the technology to easily identify, copy, move, protect, and destroy ESI throughout the enterprise.

One such tool is *storage resource management* software that "crawls" the storage objects to collect and store information about those objects in an informational database. The database could be searchable by metadata only (e.g., file type, creation date, size) or by the metadata and the full text of every stored file within the enterprise.

Such applications typically come from vendors selling information security, litigation e-discovery, or network storage management applications. These applications can:

- Identify documents with personal information for deletion or encryption
- Identify documents or e-mail with key words or concepts
- Determine the age of the documents or e-mail (by the date created, received, or last edited)

a central records repository for the important documents will allow IT to apply an automatic document deletion schedule to non-record (transitory) data stored on shared servers and e-mail. The records repository application will protect records from accidental deletion or modification and allow file-level audits, encryption, user access, and version control.

4. Revise the Records Retention Policy and Schedule

Many "for profit" business organizations in the United States have a records policy and retention schedule that are not enforced or audited. Many of the policies and schedules were written before the explosion of e-discovery, e-records, and e-mail. The modern records policy and retention schedule must be updated with an emphasis on identifying and storing electronic records. Consider modifications in the following areas.

Format. Based on the sheer volume of e-mail, documents, and other ESI being generated every day, the organization's policy must state that records will be maintained in electronic format only. The organization won't eliminate hard copy *documents*, but it will eliminate hard copy *records*. In the end, this key policy will also lower the cost of identifying, collecting, and reviewing materials related to e-discovery.

Storage Location. One of the greatest challenges will be to distinguish records from non-records if both are stored in the same application, drive, or folder. The new policy should specify that the official "record copy" of a document or e-mail will be stored within a centralized record repository application, not in Outlook or on a shared network drive.

Ownership. The new policy should specify who identifies the records. The legal department will know if a

particular document type should be saved only relative to its regulatory requirement. RIM won't know which of the various near-duplicates of a document is the official record copy. Only the business unit has the subject matter expertise to manage its own records. Therefore, the new policy should state that each business unit is responsible for its own records.

Legal should assist business unit leaders by providing a spreadsheet of minimum statutory and regulatory retention requirements for their own department's record categories. Each business unit leader should identify an experienced

normal course of business, but it can create nightmares for RIM and the e-discovery process.

The legal department can directly reduce the risk by reviewing proposed or existing cloud contracts for red flags and asking a few pointed questions to identify the contracts for terms and conditions that need to be negotiated or renegotiated, such as the following:

- The right to use data and metadata
- Ownership of data and copyrights
- Physical location of stored data
- Changing of terms or assignments without consent

The legal standard that will be used to judge the defensibility of the RIM program is "reasonableness." It is not reasonable to issue a legal hold notice and not follow up on it.

team member to help the organization's records manager finalize the department's records retention schedule.

Mandatory Audit. The last but most critical component to add to the new records retention policy is an audit imperative. The legal standard that will be used to judge the defensibility of the RIM program is "reasonableness." It is not reasonable to issue a legal hold notice and not follow up on it. The audit (or compliance) department will propose an audit schedule and methodology to ensure that records and non-record information are being maintained in accordance with the department's retention schedule. Ultimately, the audit process will document that the organization's RIM program is legally defensible.

In addition to revising the retention policy, the legal department must re-think the logistics of the retention schedule. Most schedules are confusing because they have too many "retention buckets." A schedule that counts on users to classify a document or e-mail based on a spreadsheet of hundreds of document types is doomed. The answer is to simplify the classification process.

For example, some documents and e-mail are important enough to be saved forever. With little training, users can typically identify this type of document. Most e-mail and documents can be deleted within a few months. With just one more bucket – say, one that specifies a 10-year retention – the simplified retention schedule would be easier to understand and easier to audit. Each department must train its own users with the retention rules and exceptions.

5. Modify Storage Vendor Contracts

Many organizations are utilizing a third-party file hosting service with cloud storage for file synchronization and data sharing. Cloud storage can be cost effective during the

- Notification of subpoenas
- Responsibility for e-discovery costs
- Destruction and auto-delete procedures
- Compliance and audit rights
- Data portability
- Procedures for security, business continuity, and disaster recovery

Counsel should ask about the nature of the data being stored in the cloud and the philosophy concerning its storage management. For example, ask if the documents are to be managed as *records* or are they considered *transitory data*, with the final record version to be transferred and managed within the in-house records repository application. Ask who will identify and preserve records as well as turn off any auto-delete function in case of a legal hold.

Involvement That Bucks the Trends

Organizations greatly benefit when inside counsel take an IG leadership role. First, by using common-sense litigation preparedness exercises to gain valuable insights into the strengths and weaknesses of the current IG processes and protocols, counsel will not only satisfy ABA Model Rule 1.1 that requires lawyers to provide "competent" representation, the organization will emerge with a data map and staff members that are prepared to be deposed about the RIM program.

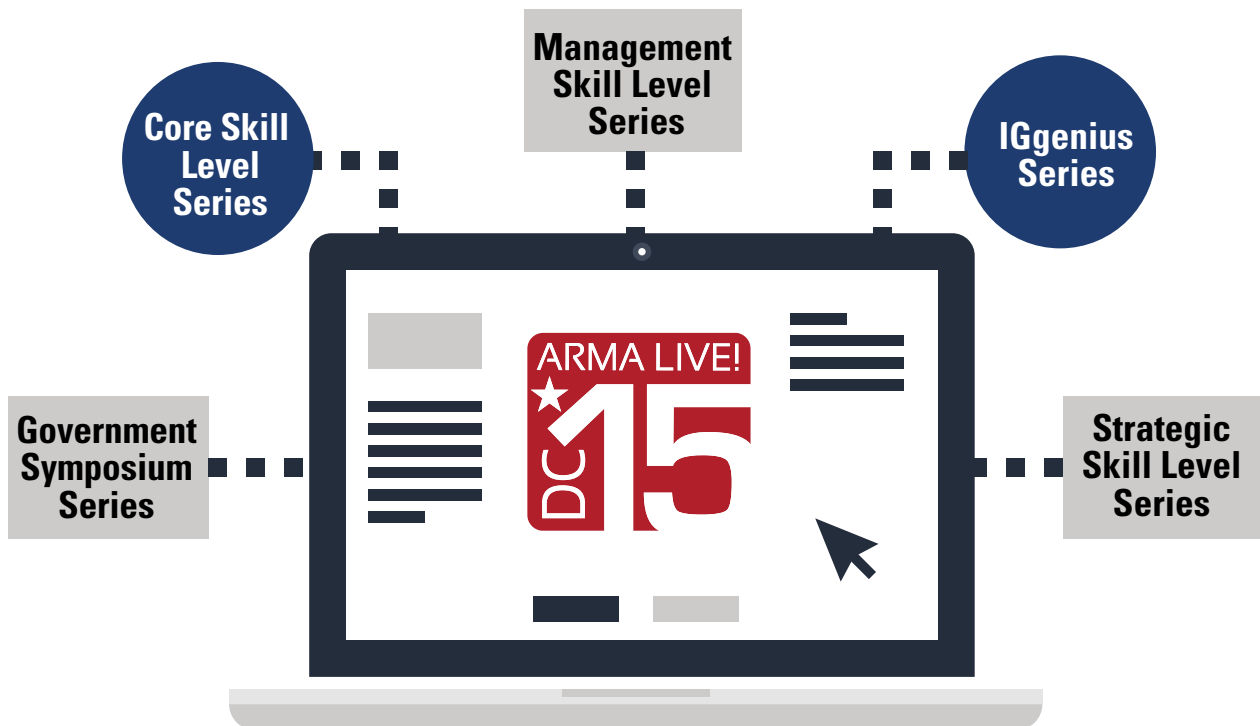
Second, by advocating to the organization's executive leadership the importance of funding the required resources for IG, litigation e-discovery costs can be reduced or avoided because the volume of stored data will be diminished. **END**

H. Kirke Snyder, J.D., IGP, can be contacted at kirkesnyder@gmail.com. See his bio on page 47.



NOW SHOWING WEB SEMINARS

What's Your Type?



Regardless of how you define yourself, there's a web seminar series for you! Visit the ARMA Bookstore to catch up on what you missed at **ARMA Live! Conference 2015**.

Reg: \$479 Pro: \$349

View online now! **BOOKSTORE** ARMA INTERNATIONAL

www.ama.org/bookstore

Click on "Web Seminars" or search for ARMA 2015

Minimizing the Use of **Trigger Events** to Increase **Records Retention Compliance**



It can be difficult to comply with records retention requirements that are based on trigger events, so many organizations are seeking to replace them with straight retention time periods. This article outlines approaches for doing this for six trigger events that are commonly used in retention schedules.

Tom Corey, J.D., CRM

When records management primarily addressed paper records, it was manageable to comply with retention periods that included *event codes*, or *trigger events*, which are requirements that must be fulfilled before the time

for the disposition of that record begins. People kept files, and when they completed a project or a contract ended – which triggered the retention period to begin – they evaluated the records, removed what they did not need, kept what they needed, and cleared up space for future records.

Today, employees create most records electronically, storing and saving official records and non-record information in multiple locations, including on hard drives, flash drives, shared drives, laptops, personal devices, tablets, e-mail accounts, and the cloud. In this electronic environment,

using trigger events in a retention schedule is much more difficult for organizations to manage.

For example, if the trigger event for a record is “termination of employment plus three years,” the employee must have been terminated before the calculation of three years begins.

If the performance of a contract is completed within a year, the records retention schedule ... should merely state the number of years to retain that contract and the information related to it.

Then, someone must notify the person responsible for managing that record about the termination to ensure that the retention clock starts ticking, wherever that official record lives.

This is actually an easy example because most organizations can put a date on when an employee leaves. But, when does a contract expire or is a policy superseded?

Some organizations’ electronic records management systems (ERMS) efficiently address trigger events, while others struggle to create clear rules for handling trigger events. If the organization struggles with this, an ERMS will not provide the solution, proper disposition of the records will not occur, and the organization will have compliance issues.

To resolve this, many organizations are seeking ways to eliminate retention times based on trigger events and are using instead *straight retention time periods*, in which the time for calculating the disposition of a record begins at its creation.

Trigger Events to Be Minimized

The following sections outline approaches for eliminating or minimizing six trigger events that are com-

monly used in retention schedules. By following these approaches, a records manager can create a schedule that restricts trigger events to those that are necessary, allowing an ERMS to work more efficiently and the organization to be in better compliance with its retention requirements.

Expiration of Contract

The most common trigger event in a records retention schedule is “expiration of contract,” and too often it is used unnecessarily for what are essentially transactional contracts, such as purchase agreements, shipping contracts, and short-term service projects.

If the performance of a contract is completed within a year, the records retention schedule should not use “expiration of contract” as a trigger event. The schedule should merely state the number of years to retain that contract and the information related to it.

Some contracts do require longer durations to perform, such as financing, long-term leases, or construction contracts. A trigger event may be necessary in those cases, but these would then be a separate category in a schedule.

There is also no reason an insurance contract should contain “expiration of contract” as a trigger event. Insurance companies limit the duration of their contracts, typically to one year, so they can review and adjust their risk frequently and regularly.

This means that if an organiza-

tion chooses to keep an insurance contract for 10 years after expiration, it should just assign it an 11-year retention period. The organization will have the same result – and it will be able to manage the disposition of that record in its system.

Final Resolution

While some conflicts result in lengthy litigation, most are resolved, or the parties agree to disagree, within a short period. “Final resolution” as a trigger event for these types of records is inefficient because it is difficult to determine when a conflict is actually resolved unless it is settled by a third party, such as a court, mediator, or arbitrator.

Second, this trigger is unnecessary because the record retention issue can be resolved by adding a reasonable amount of time for the resolution to the retention period. For example, if the desired retention period is three years after resolution, simply add two years and make it a five-year retention period. This approach works well for customer service call center records or records addressing employees’ minor complaints.

This approach does not necessarily apply to litigated matters, which must be retained through final resolution. But that is manageable because “final resolution” has a clearly defined date.

Protection Period

Many schedules use “protection period” as a trigger event for intellectual property. For the most part, patents have a set protection period of 20 years under 35 U.S.C. § 154, and most countries also use 20 years as their standard.

Therefore, instead of using the trigger event, the organization – even if it is global – can simply add 20 years to the desired protection period. So, for example, an organization that wants to keep patent records for 30 years after the protection period expires can use the 20-year standard for

the protection period and make the retention period a straight 50 years.

The same can be done with copyright protection by adding 95 years to the desired retention period after the protection period (see 17 U.S.C. § 302). For example, if the organization wants to retain its copyrighted material for five years after the copyright protection period, it can simply make the retention period 100 years. (This approach does have limitations with trademarks, which can be renewed. See 15 U.S.C. § 1058 and 15 U.S.C. § 1059.)

Life of Product

Manufacturing categories often refer to “life of product” for quality and engineering files. *Life of product*, or *model life*, is commonly considered to be the estimated duration of a product from the moment of its entry into the market until its withdrawal.

In most cases, a manufacturer can predict this duration. For the purpose of records management, the organization must define the life of product because employees will otherwise apply inconsistent durations or will never dispose of the records.

To determine a standard product life, an organization’s records manager should work with its engineers to understand the product’s reasonable life expectations and with legal counsel to ensure it complies with any product life standards established through regulations or liability considerations. Once an organization establishes a product life, it can use that product life, plus any additional time it requires, and have a straight retention time instead of one based on a “life of product” trigger event.

People sometimes cite examples of products that have outlived such predictions, but for the purposes of records retention, the goal is to have a standard that’s based on reasonable expectations of the product life, not a guarantee that the product will never exceed that duration.

Superseded

For many organizational policies and plans, the retention schedule uses “until superseded” or “after superseded” as a trigger event. If a policy or plan has an indeterminate or long life, that may be necessary. But many plans and policies are updated regularly. Each revision and update creates a new policy or plan.

For example, organizations may update compliance programs annually to ensure that they comply with the latest regulations and case law. Yet, they use “superseded” (instead of one year) plus the desired retention time for these company plans and policies in their retention schedules.

The same applies to non-pension benefit plans and policies. If these are updated annually, the schedule could delete the term “superseded” and add one year to the desired retention time since the revised and updated policies are essentially new records.

Straight Time Benefits

Taking this approach offers records managers an opportunity to minimize the use of trigger events in their records retention schedules, but it will not eliminate trigger events entirely. In some cases, trigger events are necessary or are the easiest way to manage retention – for example, for annual reviews, contracts with long performance periods, final resolution of litigation, life of property or equipment, life of plan for pensions, superseded policies with indefinite durations, and termination of employment.

Where it is possible, minimizing the use of trigger events in records retention schedules by deferring to a straight retention time for most of its records will allow an organization’s ERMS to more effectively handle the disposition of electronic records and greatly increase compliance with retention requirements. Compliance with retention requirements will en-

...minimizing the use of trigger events in records retention schedules by deferring to a straight retention time for most of its records will allow an organization’s ERMS to more effectively handle the disposition of electronic records.

Project Completion

Many records are tied to projects, and many retention schedules reflect these records by using “project completion” as the trigger event. But are these projects so long in duration that they actually need this trigger event? If the project is normally completed within a year, or even two years, it would be easier to add that time to the desired retention period and eliminate the trigger.

sure regulatory observance, reduce discovery costs, make records easier to find, and mitigate the risk of security breaches. Minimizing the use of event codes on the retention schedule is a tool to achieve those benefits and allow the retention schedule to function properly. **END**

Tom Corey, J.D., CRM, can be contacted at tcorey@consilio.com. See his bio on page 47.

Software Updates May Be Compromising Your IG

John Phillips, CRM, CDIA, FAI



Information governance (IG) cannot be thoroughly implemented in an organization that is operating uncontrolled technology systems and data repositories. Even when employees, contractors, and business partners work diligently toward consistent IG practices, external forces – namely, updates to cloud-based or resident software on laptops, cell-phones, and other digital business devices – can modify internal IT operational activities in ways that violate compliance with IG expectations.

This happens, in part, because vendors encourage technology users to enable background, automated downloading of updates to software to ensure that virus protection, hardware drivers, and bug patches are implemented. Unfortunately, because software updates are so frequent and often seem minor, most non-technical

users just trust that Microsoft, Apple, Google, and other vendors will not release anything that will negatively affect their systems.

Another issue is that even though downloading the latest innovations in software releases and updates typically requires users to click through a software license “acceptance,” they are rarely read or understood.

Organizations that allow end users to download software and software updates in this manner may face grave consequences with respect to software operations, privacy, security, and compliance with IG mandates.

Using Windows 10 as an Example

A good example of the ubiquitous nature of software updates is Microsoft’s Windows 10 operating system. Users of Windows 7 and 8 have been

offered an opportunity (through July 29) to upgrade their current systems to Windows 10 for free. This update, though, comes with intrusive data-gathering demands, and it should generate concerns about reliability and compatibility with a user’s current software configurations.

Spontaneous Downloading

An additional concern is that the Windows 10 operating system appears to already have been *downloaded to some computers spontaneously without users initiating a request for it!* As first announced on the *INQUIRER* website in September 2015, some computer users who enabled automatic downloads of Microsoft updates may have downloaded update KB3035583, which automatically adds to the computer a hidden directory with up to 6 GB

of files comprising the components necessary for Windows 10.

Allegedly done to speed up the eventual installation process, according to media reports, the premature downloads were exposed when it caused some users to momentarily exceed their data volume allocation with their communications networks. Although there is a way to delete these files, it is not for the technologically faint of heart.

Effects Not Transparent

Of more concern, Microsoft at the time provided little information on how Windows 10 affected privacy and security, simply stating, "This update includes improvements to enhance the functionality of Windows 10." A user's only reliable way to determine the effects of the updates was to match the update numbers with information on the Microsoft Knowledge Base.

Whereas in the past it was usually possible to discern how an update would alter functionality, it is now more difficult to know what to expect. It is even more concerning that updates are cumulative; every updated feature is expected to be updated again each time an update is issued. Not installing any particular update could make a computer unstable.

Windows 7, 8 Invasion

In fact, many of the functions that are new to Windows 10 are also being applied retroactively to any Windows 7 or 8 systems, which could impact IG compliance for systems running older software as well.

For instance, Windows 7 and 8 updates KB3075249 and KB3080149 operationally deliver data to Microsoft servers without any required user interaction. The first update adds features that enable remote monitoring of operating system activities, and the second update enables older versions of operating systems

to receive updates that are intended for Windows 10 systems. Thus, users running Windows 7 or 8 may find themselves subject to many of the same intrusive functions associated with Windows 10, though they would prefer to avoid these functions.

By imposing updates on users without their knowledge or consent, Microsoft is damaging the trust that may exist between the company and its customers.

... users running Windows 7 or 8 may find themselves subject to many of the same intrusive functions associated with Windows 10, though they would prefer to avoid these functions.

Troubling Service Agreement

In light of the many organizations that have been unable to protect the data they collect, customers are increasingly concerned about how Microsoft, Google, and other major software vendors will respond to government requests for private information. Such concerns are perhaps justified by statements found in the new Microsoft Services Agreement.

This agreement, which can be read in full at <https://www.microsoft.com/en-gb/servicesagreement/default.aspx>, contains these troubling statements that could impact an organization's IG policy compliance expectations:

1. "By using the Services or agreeing to these Terms, you consent to Microsoft's collection, use and disclosure of Your Content and Data as described in the Privacy Statements.
2. "When you share Your Content with other people, you expressly agree that anyone you've shared Your Content with may for free

and worldwide, use, save, record, reproduce, transmit, display, communicate (and on HealthVault delete) Your Content.

3. "To the extent necessary to provide the Services to you and others (which may include changing the size, shape or format of Your Content to better store or display it for you), to protect you and the Services and to improve Microsoft products and services, you grant

Microsoft a worldwide and royalty free intellectual property license to use Your Content, for example, to make copies of, retain, transmit, reformat, distribute via communication tools and display Your Content on the Services."

It's important to know that the content of the services agreement may be changed without notice. In addition, few people read these agreements because they are typically long and filled with "legalese" that would require consultation with professional legal counsel. If printed, this Microsoft agreement would be more than 100 pages long. Though most people don't understand what they are signing when they accept an agreement, such "agreements" are generally supported by the courts, which does not leave an organization using a Microsoft product much leeway in configuring a software system that avoids intrusive components.

Private Data Exposed

Microsoft's perspective toward

Read More About It

Bott, Ed. "How to block Windows 10 upgrades." ZDnet, 28 April, 2016. Available at www.zdnet.com/article/how-to-block-windows-10-upgrades-on-your-business-network-and-at-home-too/?tag=TRE5369823.

Meer, Alec. "Windows 10 Is Spying On You: Here's How to Stop It." Rock, Paper, Shotgun, 30 July, 2015. Available at www.rockpapershotgun.com/2015/07/30/windows-10-privacy-settings.

Merriman, Chris. "Windows 10 'updategate': Microsoft stays tightlipped as the world rages." The Inquirer, 15 September, 2015. Available at www.theinquirer.net/inquirer/analysis/2425886/windows-10-updategate-microsoft-stays-tightlipped-as-the-world-rages.

Microsoft End User Licensing Agreement. Available at <https://www.microsoft.com/en-gb/servicesagreement/default.aspx>.

Microsoft Privacy Policy. Available at <https://privacy.microsoft.com/en-us/privacystatement>.

Williams, Chris. "How to get a grip on your files, data that Windows 10 phones home to Microsoft." The Register, 24 February, 2016. Available at www.theregister.co.uk/2016/02/24/windows_10_telemetry.

its customers' privacy can be seen in its privacy policy at <https://privacy.microsoft.com/en-us/privacystatement>. It starts out by saying "Your privacy is important to us. This privacy statement explains what personal data we collect from you and how we use it." It then makes the following statements (see these and others at the "Learn More" link under the Microsoft privacy policy section "Personal Data We Collect"):

1. "We collect data about your interests and favorites, such as the team you follow in a sports app, the stocks you track in a finance app, or the favorite cities you add to a weather app.
2. "We collect data about your contacts and relationships if you use a Microsoft service to manage contacts, or to communicate or interact with other people or organizations.
3. "We will access, disclose and preserve personal data, includ-

ing your content (such as the content of your emails in Outlook.com, or files in private folders on OneDrive), when we have a good faith belief that doing so is necessary"

Microsoft, like many corporations, mines user data by engaging in what some privacy experts call "spying." It does so without making it clear about what is taking place, relying heavily on abstractions like "...when we have a good faith belief that doing so is necessary." Consequently, the murky nature of concepts like data ownership and protection makes it more likely that an organization's IG policies are being compromised, especially if that mined data crosses international boundaries.

Escaping Windows 10 Surveillance

Opting out of many privacy-invading Windows 10 functions requires effort and dedication to self-

protection. For example, users must slog through 13 screens to decline participation in many of Microsoft's ongoing attempts to gather data. By taking these steps, users can turn off anything that seems concerning, but they may want to be careful about accidentally turning off their access to data they access frequently, such as calendars, while doing so.

Among the other concerns is continued surveillance from the camera, microphone, speech, contacts, calendar, and messaging functions, including Cortana, Microsoft's speech-recognition function, which constantly "listens" for reasons to initiate Microsoft's Bing search engine to answer questions. Realistically, the act of opting out of any of these functions is best performed by well-trained IT staff.

Much of this intrusive data gathering is done so Microsoft can sell to advertisers the ability to use more individually targeted advertising. Some people like targeted advertising, but that does not mean the advertising a user sees is always appropriate for the moment when the ad pops up. For example, an employee might be looking at ads for vacations in Bermuda while at her desk during lunch. Later, the ads might pop up on her screen at inopportune moments, such as when her supervisor is in her office for a visit.

Reducing Impacts on IG Compliance

The fundamental problem with Windows 10 and any other commercially produced software is that users do not own the software and therefore must accept prescribed licensing agreements. To refuse the agreement could impair their business processes, as migrating data to other software environments is costly, time-consuming, and can bring other unforeseen risks. Sometimes data migration results in a loss of software support for critical business

components or an actual data loss.

The practice of slowly retiring older applications or operating systems is nearing an end. For instance, though there are still some users of the Windows XP operating system and older Office suite applications, Microsoft has ended support and maintenance for those versions. And, it may be impossible over time to continue using older systems if users are connected to the Internet and updates that interfere with the software operation are involuntarily downloaded. This means that ensuring compliance with IG guidelines is becoming even more challenging because IT staff will have to know all of the currently used technologies and how any updates will affect their operation.

Users of today's software systems can expect their communications content, travel agendas, business plans, and office location information to be increasingly subjected to data exchange during software updates in order for the vendor to ensure effective operation. For this reason, it is ideal to have IG-knowledgeable IT personnel monitor or manage all common software updates. It may be best to offer updates downloadable from a centrally coordinated IT server that monitors all devices to gauge how the updates affect the software configurations with respect to IG policy compliance.

The most globally effective IG/IT approach to new technology threats will be to enforce a policy that all software users must have permission from IT before installing any updates. To make this easier on users and to have the least impact on IT staff, organizations could post for download on an accessible website those upgrades known to pose no dangers to IG policy implementation. **END**

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



Your Connection to RIM & IG Products and Services

BUYER'S GUIDE ONLINE!



The **2017-2017 Buyer's Guide for Records Management and Information Governance Professionals** is the place to start for software solutions, records centers, archiving supplies, and more! ARMA International's online listing of solution providers puts the power of purchasing at your fingertips!

www.arma.org/buyersguide

Want to advertise in the online Buyer's Guide?

Contact Jennifer Millett at jennifer.millett@armaintl.org today!

3 Keys to Managing Change

for a Successful RIM Program Implementation

Melissa G. Dederer, IGP, CRM, and Aaron Swan

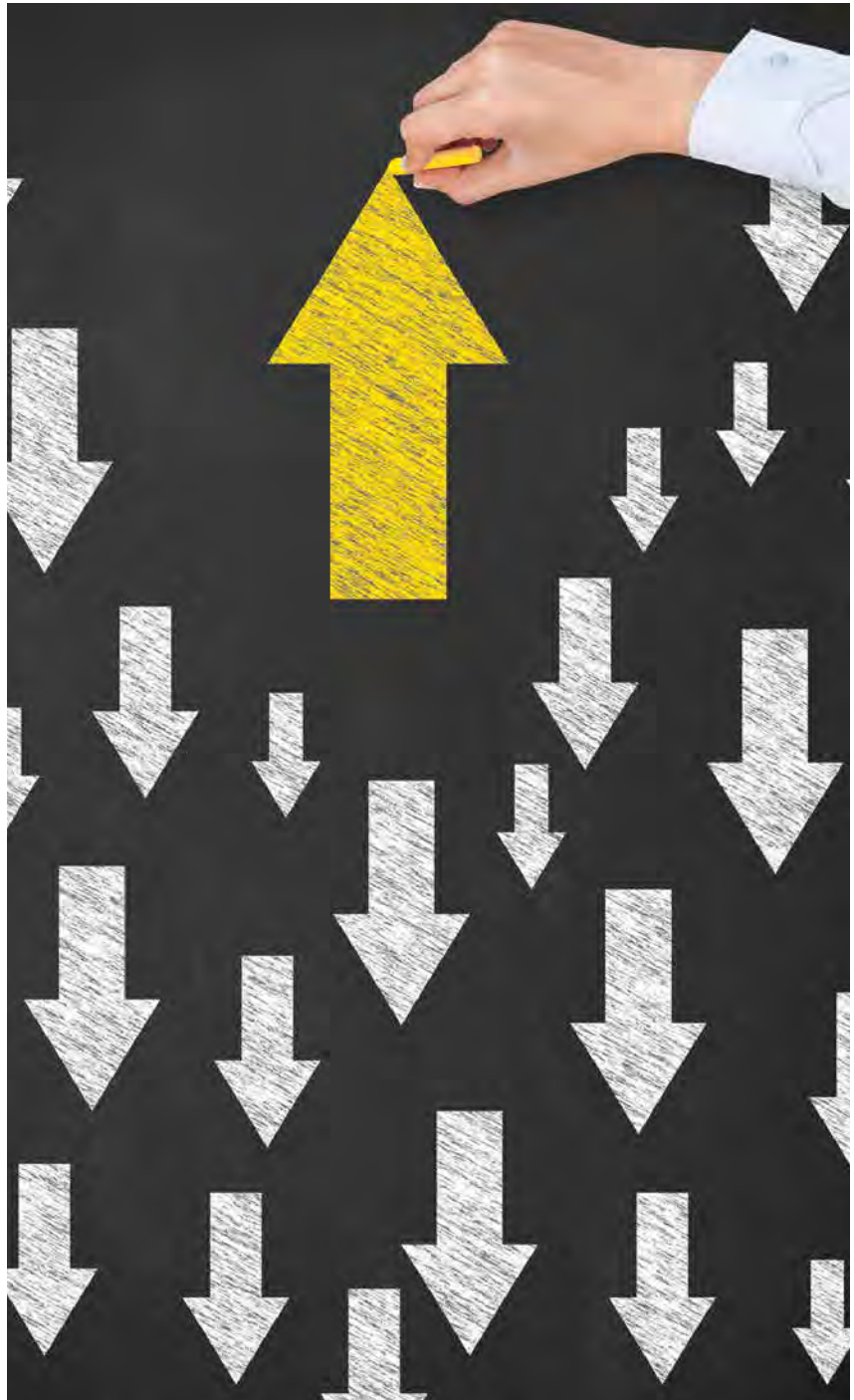
Whether implementing a new program, software application, or process, or simply modifying something that is already in place, it is the execution of the change management process that will determine whether users adopt the change and the initiative can succeed. But, it can be a daunting task to get all those who will be affected by the change to understand how it will benefit them – from the C-level all the way down to the entry level and including contractors and third-party service providers.

This article discusses the three change management elements necessary for the successful implementation of a records and information management (RIM) program:

1. Ensuring that the *power employees*, who are the owners, executives, and managers, understand and buy into the need for the program
2. Engaging and addressing the concerns of *knowledge workers*, who are those whose jobs primarily involve creating, distributing, or applying knowledge, according to the knowledge management expert Thomas H. Davenport
3. Respecting the inevitability of natural human behavior

Selling Change to Power Employees

RIM professionals understand that there is a real risk to *not* implementing a RIM program, as minimizing risk is at the core of what they do. Yet, power employees often fail to see the risk and, consequently, to recognize the value such a program



provides. Getting them to fully comprehend how a good RIM program mitigates risks, avoids costs, and provides other benefits to the organization is the first key element in ensuring user adoption of the program.

Conduct an Analysis

Helping power employees understand the real risks of not having a RIM program may be as simple as explaining that there are rules and regulations requiring the organization to properly manage its information. But it can go even further. A strategic analysis, for example, can expose the shortcomings in a current RIM program. Recommendations on how to correct those shortcomings can lead to a more optimal state.

ARMA International's Generally Accepted Recordkeeping Principles® (Principles) provide a good place to start that analysis. The Principles are derived from RIM and information governance best practices and international standards. To evaluate a program against the Principles, use the ARMA-developed Next Level Information Governance Assessment tool, which provides a risk-level mapping for each Principle. The assessment can provide valuable insights as to what an organization is doing well and where it needs improvement, allowing users to address deficiencies and thereby minimize risk.

With numerical, color-coded ratings for the organization's maturity level for each Principle, it presents easily grasped, compelling results that help power employees see at a glance that there is a real risk in not having a proper program in place, as well as understand the benefits of having a proper program.

Take the Next Step

Surprisingly, many organizations stop at this crucial point and presume user adoption will be the easy outcome of having gotten the power employees to the table. But

User adoption can best result when the power employees' actions show they are not only supporting the RIM program but that they also are allocating proper resources to it.

real adoption relies on getting the end user – the knowledge worker – to buy in. User adoption can best result when the power employees' actions show they are not only supporting the RIM program but that they also are allocating proper resources to it.

Selling Change to Knowledge Workers

Knowledge workers get their cues from the power employees, but if the knowledge workers do not completely buy into the change, the program will not work.

Discover Their Perspective

Understanding the knowledge workers' perspective about the change can enhance efforts to get their adoption. Investigate to learn how they feel about the new program, system, or process that touches their world. For example, if they believe the new program will require them to spend additional time on the change, giving them less time to fulfill what they believe are their more important responsibilities, they may be resistant to the change. Knowledge workers need to understand and believe that the program will make their work *less* cumbersome, not more.

Listen to Understand Their Concerns

Knowledge workers need to have a voice and believe it is truly being heard, appreciated, and considered. Seek to understand what the employees are actually saying – beyond their words – to get to the root of any resistance.

For example, knowledge workers that have years of experience may be protective of the information they have. Though they may not say this is the cause of their resistance, if they refuse to share or document the processes that are in their heads, it may be. Without resolving this issue, the success of the change itself will be in jeopardy and their knowledge may be lost.

Get Them Involved

It is vital to engage the knowledge workers early in the process because their involvement will give them a stake in the initiative's success and help turn them into advocates. More importantly, they may be able to improve and expedite the change initiative if they're invited to take part and have an investment in its success.

For example, a leading global investment firm had the following challenge. Because of localized processes and rogue software tools, data was floating around outside the system, in such places as Excel documents and on employee desktops. The risk was that over time this data could become inaccurate, outdated, and lost – potentially compromising client transactions and resulting in fines and suspended licenses due to regulatory non-compliance.

After partnering with a design research firm, the organization deployed design research teams to their offices worldwide to evaluate back-office processes, understand variability across locations, and uncover hidden risks. Insights from this research led

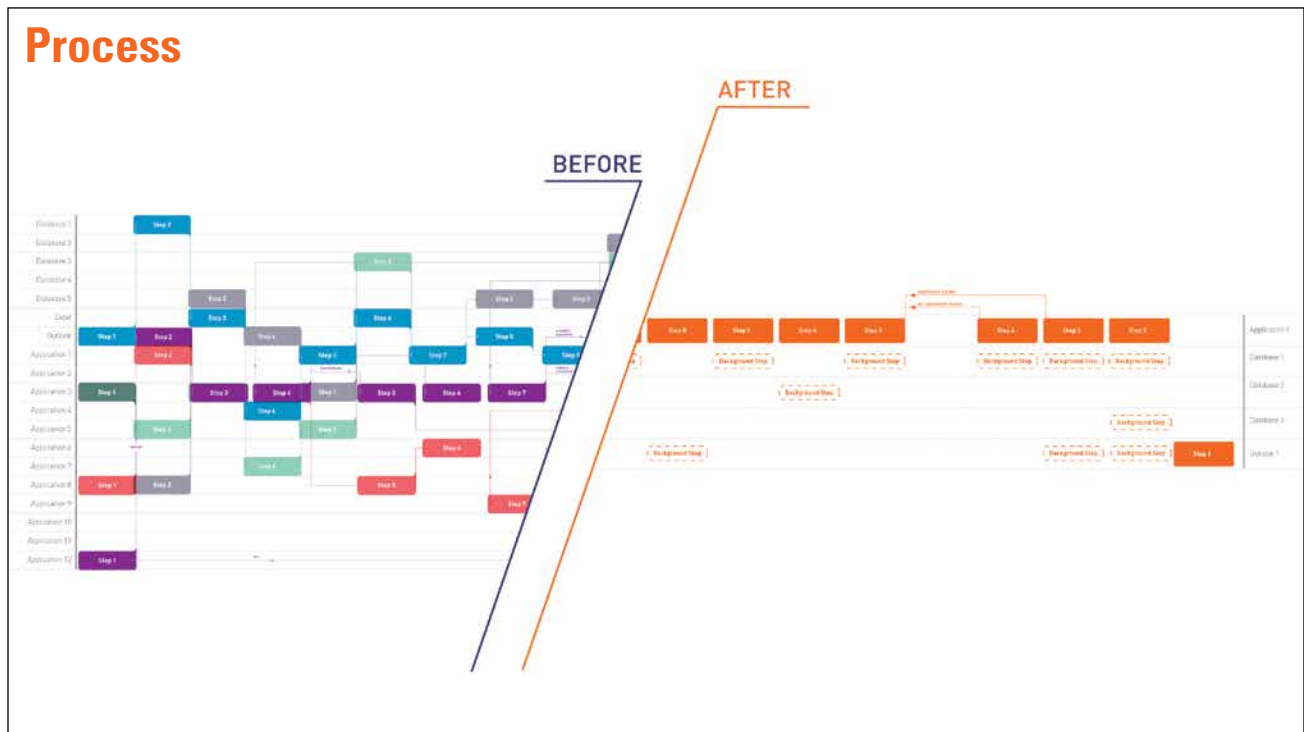


Figure 1 – Source: Electronic Ink; pictorial view of the “before” and “after” processes

the design team to create a secure, global application with a customizable user interface to accommodate the specific needs of each office. The new application provided greater consistency, accuracy, and information security across the enterprise.

The solution used a single, repeatable process that eliminated the need for 11 duplicative applications. It automatically and intelligently delivered necessary information in the right format, to the right person, at the right time. The system eliminated rogue application data, and it reduced maintenance and training, databases and server requirements, and workflow steps by 66% (See Figure 1).

All of these achievements were the result of a deep appreciation and respect for the knowledge workers, their individual roles, and their contribution towards a grander solution.

Taking into Account Human Behavior

The third element of a successful change initiative for the imple-

mentation of a RIM program is to understand human behavior. Do not design or invest in the process without understanding the culture and human behavior of those it will affect.

For example, knowledge workers may circumvent a process because it causes redundancies and bottlenecks that frustrate them. Even though their “workarounds” might waste time and resources, negatively affect customer service, and increase risk, they continue the workarounds because they naturally want to get their work done in the ways that suit them best. Without understanding this natural human instinct, an organization may continue to design unrealistic processes.

A clear, unbiased view of the people who will use a system or process is critical. Many companies now realize that this key skillset has been missing and are looking for ways to develop it or are getting it by partnering with groups that specialize in human behaviors and user experience. By leveraging this highly specialized

skill and integrating it with process improvements, organizations can realize tremendous results.

Concluding with a Successful Change

Although the word “change” has a negative connotation for many people, it is possible to implement change positively. It begins with ensuring that power employees realize the need for and benefits of the change. It progresses by including knowledge workers in discussions about the change, listening “between their words” to understand their perspective, and demonstrating that their concerns are heard and considered. And, it concludes successfully with a well-designed solution that addresses their concerns and takes into consideration the natural human behavior of those who will be affected by it.

Melissa G. Dederer, IGP, CRM, can be contacted at mgdederer@yahoo.com. Aaron Swan can be contacted at absswanii@gmail.com. See their bios on page 47.

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.

50, 25, 10 Years Looking Back...



July 1967

Twin City Chapter Conference,
April 1967.

Records Management Quarterly Association News

- ARMA chapters have been formed in Pittsburgh and Orlando (Central Florida).
- ARMA exhibited at the National Microfilm Association Conference in Orlando. The booth was staffed by ARMA President Eunice Thompson, as well as Bill Benedon, Bruce Mowry, and Louise Merritt of the Greater Los Angeles chapter and Bruce Carswell from New Jersey.

Articles

- "Microfilm as a Management Tool," by Richard E. Wolff
- "Microfilm at North American Aviation – LAD," by Mark Keith
- "Microfilm in an Uncertain World," by Genealogical Society of the Church of Jesus Christ of Latter-day Saints
- "The Computer Programmer – A Helpmate to the Records Manager," by Phyllis Lorek
- "Paperwork: A Twentieth Century Dilemma," by Bruce C. Harding
- "People and Records," by Dr. Irene Place
- Special features in this issue:
 - ARMA's 12th Annual Conference program for Oct. 24-27 at the Roosevelt Hotel in New York. The registration fee for the entire conference, including luncheons and banquet, is \$90 for members and \$100 for non-members (\$10 of which goes to the ARMA membership fee)

– Records Management Glossary from the "first of its kind" ARMA correspondence course developed by William Benedon. (See excerpt on page 42.)

- Charles Macbeth reviewed the following books: *The Effective Executive* by Peter F. Drucker, *The Business Executive in a Changing World* by William N. Mitchell, *Technical Information Center Administration* edited by Arthur W. Elias, and *Management Uses of the Computer* by Irving I. Solomon and Laurence O. Weingart.

Advertising

The first advertisers to appear in *RMQ* were:

- Kodak – "What's new in microforms? Come to Kodak."
- Remington Rand Office Systems (Division of Sperry Rand Corporation) – "Now... a one-stop source for all your Records Retrieval Micro-System needs!"



July 1992

John T. Phillips (1992) also wrote
an article for this issue of *RMQ*.

Records Management Quarterly Association News

- The president of ARMA International is Patricia Dixon, CRM.
- Others newly elected officers to the ARMA Board of Directors are James Allin Spokes, president-elect, and Michael P. Flanagan, secretary/treasurer.

Articles

- "A New Look at Information Systems and Records Management," by Guy H. Thomas and Dr. Mark Langemo, CRM
- "The Value of Enhanced Service in Cost Justification," by Ron Lacharité
- "The Use of Transportation Methods to Achieve Efficiencies in Data Placement," by Robert H. Fireworker,

Ph.D, and Patrick Geier

- “An Automated Solution to the Superfund Documentation Problem,” by Sandra J. York, CRM
- “A PR Plan for Records Managers,” by Juanita M. Skillman, CRM
- Kenneth V. Hayes reviewed *Personal Computer Systems for Automated Document Storage and Retrieval* by William Saffady, *Desktop Image Scanners and Scanning* by Fred U. Wetzler, and *All About Micrographics* by Don Avedon and Rodd Exelbert.

Advertising

- Acorn Information Systems – “You LIE Like A Dog?! If You Think We Are Lying When We Say **RETRIEVER™** Is A FULL FEATURED Personal Computer Records Management System, And Sells For Only **\$595...** Then Order The Demonstration System For Only \$10 With The Above Coupon, And We Will Prove... **RETRIEVER's™** Bark Is As Strong As Its Bite!”
- Ames Color-File – “SQUEEZED FOR FILING SPACE?”
- Association of Commercial Records Centers – “How to get your records at midnight.”
- Assured Information Systems, Inc. – “Records Management Software”
- Automated Records Management Systems – “Our clients know a lot about records management.”
- Borroughs, a Lear Siegler Company – “Record Holders”
- CASS – “SOFTWARE To Do: · BOX TRACKING · FILE TRACKING · DRAWING MANAGEMENT”
- Chase Technologies, Inc. – FAST-PACED SOLUTIONS FOR A FAST-PACED WORLD: CHASE TECHNOLOGIES, INC.
- Commonwealth Films Inc. – “Buried Alive: The Critically Acclaimed Document Retention/Records Management Video.”
- DSC Data Storage Centers – “OFFSITE STORAGE WITH ONSITE CONTROL”
- Engineered Data Products – “The Filing Solution”
- GBS Filing Systems (formerly VRE Inc.) – “ASK OUR ORGANIZATION TO TAKE OVER YOUR OFFICE”
- Information Requirements Clearinghouse – “Protect Your Organization... Comply with the Laws Affecting Your Records!”
- InfoTRAX – Increase Efficiency, Accuracy, and Productivity with InfoTRAX – The Records Management System for the 90s”
- Iron Mountain – THE IRON MOUNTAIN SYSTEM: YOUR RECORDS MANAGEMENT SOLUTION
- Olsten Records Management Services – “Convert it. Maintain it. Destroy it.”

- Records Improvement Institute – “IN-HOUSE WORKSHOPS”
- Redweld – “Redweld Recycled Products...State Your Case.”
- TAB Products Co. – “Barcodes to control and manage your sensitive documents”
- Triadd Software Corporation – “ALL RECORDS MANAGEMENT SOFTWARE WAS NOT CREATED EQUAL”



Access Sciences has been a long-time supporter.

April 2007

The Information Management Journal

Association News

- The association is promoting the “Risk Profiler Self-Assessment” and the DVD training program “Keeping Good Company.”
- ARMA International’s Standards and Best Practices Program has published *The Digital Records Conversion Process: Program Planning, Requirements, Procedures* (ANSI/ARMA 16-2007) and *Guideline for Evaluating Offsite Records Storage Facilities*.

Articles

- “Blogs, Mashups, and Wikis – Oh, My!,” by Bruce W. Dearstyne, Ph.D.
- “Does Your RIM Program Need a Strategic Alignment?,” by Alan A. Andolsen, CMC, CRM
- “Eight Tips for Working with a Consultant,” by Julie Gable, CRM, CDIA, FAI
- “RIM Marketing Made Simple,” by Laurie Carpenter, CRM
- “Evidence Management Solutions for Mitigating E-Records Risks,” by Rob Peglar

- *Archiving Websites: A Practical Guide for Information Management Professionals* was reviewed by Anselm Huelsbergen, CA

Advertising

- Access Sciences – “Data Warehousing. Global Information Strategy. Compliance Knowledge Management, Records Management, Audit and Legal Support. Document Management. Access Sciences...Connecting the Dots”
- AIIM – “ready. aim. learn. Learn how to implement electronic records management (ERM).”
- Allegheny Paper Shredders – “SelecShred Adjustable Screen. Double your security at the touch of a button!”
- Bankers Box – “IS YOUR STORAGE ROOM SHRINKING?”
- BELFOR Property Restoration – “We listen. Clean and simple.”
- DACS – “THE PROVEN SOLUTION PUNCHDECK Open Area Corrugated Rack Deck”
- Dahle – “Save Money. Shred It Yourself!”
- FileTrail – “Stranded by your RIM vendor? Get on board with FileTrail and never be left behind again.”
- Fujitsu – “Fujitsu scanners. You’ll see productivity everywhere you look.”
- Iron Mountain – “Sally files it. Jack prints it. Jen downloads it... Fortunately, you can trust one company to protect it.”
- Leggett & Platt Store Fixtures Group – “Our records speak volumes about the experience and resources we bring to every project.”
- MBM Corporation – “Before a discarded document comes back to bit you...Shred it at the Source.”
- OmniRIM – “Take Control of Your Records Management.”
- O’Neil Software – “Scan. Store, Manage. Deliver.”
- Paige Company, The – “Ordinary boxes hold stuff. Ours are built to hold your future.”
- Recall – “THEY SAY, ‘Nobody’s Perfect.’ WE SAY, ‘How Hard Are They Trying?’”
- Smead Manufacturing Company – “If only everything worked together as well as our paper and electronic records management systems.”
- SNIA – “Does your information put you at risk? Protect yourself at Enterprise Information World.”
- Tower Software – “Enterprise Content Management. Knowledge...where it needs to be.”
- Xerox – “ONE TOUCH. Put information you need right at your finger tips for under \$500.”
- Zasio – Point. Click. Save. “When it comes to managing your electronic records, you’d be happy if *Point-Click-Save* were all it took. With Zasio, it is!” **END**

Records Management Glossary

July 1967

ARMA’s first glossary, which was part of its first records management correspondence course, included terms that are no longer familiar to most records management professionals. Even a few of the subject areas represented by the terms (and noted in parentheses after each term) may be unfamiliar:

CFM – Correspondence and Files Management; **FM** – Forms Management; **GRM** – General Records Management; **M** – Microfilm Systems; **RC** – Records Center Operations; **RM** – Reports Management; **RP** – Records Protection; and **RS** – Retention Scheduling.

How many of these terms do you know?

Can’t Finds: (RC-CFM): Materials which have been searched but not located.

Card-Tabulating (RS-FM): Heavy, stiff paper of uniform size and shape, adapted for being punched in an intelligent array of holes. The punched holes are sensed electrically by wire brushes, mechanically by metal feeders or by electronic circuitry.

Cushion Sheet (FM): A plastic sheet placed between the stencil and backing sheet when preparing a stencil master on a typewriter. The cushion sheet insures a clean, sharp copy.

Duo (M): Recording of images on only one-half of the film width during one passage of the film. Film is then turned end-for-end and rerun to utilize the second half of the film. The principle is both useful and economical when filming small documents at high degrees of reduction.

Head-to-Foot (FM): Also called “tumble-turn” and indicates printing the reverse side of a sheet upside down so that it can be read by turning the sheet over from top to bottom instead of turning it as you would the pages of a book.

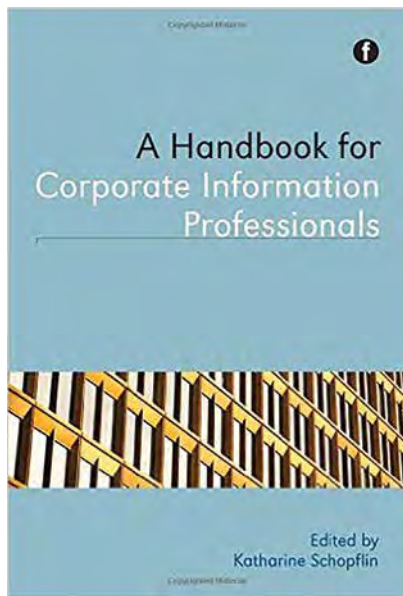
Pen Rule (FM): A method of printing lines only on columnar formats. The pen rule machine makes use of “pens,” which come in contact with the stock traveling beneath them in a continuous web.

Riffle (CFM): To thumb rapidly through the edges of a stack of papers to loosen them for easy handling.

Unitized Film (M): Microfilm mounted in some “unit” fashion; usually film mounted in a film jacket, aperture card, or film card – frames of microfilm instead of an entire role.

A Primer for Corporate Librarianship and Information Management

Melanie Sucha



A *Handbook for Corporate Information Professionals* is a concise, but thorough, compilation of contemporary topics in corporate librarianship. It covers practice areas such as corporate intranets, marketing, taxonomies, knowledge management, market analysis, electronic licensing, and end-user training.

Aimed at Corporate Librarians

While the broad term “information professional” is used in the title and by the various authors throughout the text, the content is presented from the corporate librarianship standpoint – as opposed to the standpoint of other information management (IM) domains, such as records management.

The primary audience becomes readily apparent in Katharine Schopflin’s introduction, which is an articulate description on the history of corporate librarianship and discussion of the discipline today. Many of the

topics in the book pertain to corporate library processes – that is, the management and dissemination of acquired published resources to support the business.

Linda-Jean Schneider and Simon Barron’s chapter, “The hybrid librarian-IT expert,” is focused solely on the librarian perspective. This chapter takes a traditionalist view of both the librarianship and IT disciplines, perhaps unfairly criticizing IT departments as being overly imposing, and it lacks discussion on more contemporary topics, such as the need for information governance and the skills that both IT and IM professionals have to offer in the governance domain.

Anneli Sarkanen and Katy Stoddard’s chapter, “Training end-users in the workplace,” is focused on the search and usage of library resources, without addressing use of internal document management systems or line-of-business information technologies.

This chapter demonstrates some outdated views, painting vendors simply as salespeople and discouraging vendor collaboration for training assistance – a point that runs contradictory to Tina Reynolds, Schneider, and Fiona Fogden’s more progressive arguments in favor of a collaborative approach with vendors in their chapter, “Working with suppliers and licensing for e-libraries.”

A Focus on Growth, Exploration

Other chapters are focused on growing the corporate librarian’s skill set to adopt broader IM duties relating to managing the organization’s internal information assets.

James Mullan’s chapter, “Manag-

A Handbook for Corporate Information Professionals

Editor: Katharine Schopflin

Publisher: Facet Publishing

Publication Date: 2015

Length: 184 pages

Price: \$125 (No. America); £59.95

ISBN: 978-1-85604-968-9

Source: www.alastore.ala.org (No. America); www.facetpublishing.co.uk

ing the corporate intranet,” offers solid strategic advice for content management and governance of an intranet platform, as well as covers best practices and hot topics for those new to using intranets and related social media features.

Danny Budzak’s chapter, “Practical knowledge management,” offers an introductory level overview of knowledge management, followed by practical advice on consulting with business clients to facilitate knowledge capture.

Helen Lippell’s chapter, “Building a corporate taxonomy,” gives advice on critical steps in this activity, such as running stakeholder workshops and aligning to end-user language.

These chapters are excellent summaries for librarians exploring growth in and beyond their roles or for information studies students exploring different career opportunities.

Uneven Writing Quality

While the compilation covers a number of current and relevant topics for corporate librarians, the quality of the writing varies throughout. Most chapters are very clear and easy to ab-

sorb. For example, Shaunna Mireau's chapter, "Internal and external marketing by information professionals," gives very thorough coverage of the topic and includes a mix of theoretic explanation of metrics and service delivery processes, balanced with illustrative anecdotes.

Other chapters are not so well-written. Phillip Weinberg's "Successful management of insight, intelligence and information functions in a global organization" contains many name-dropping references to other authors and field experts without explanation as to who these people are and what their views comprise.

Andrew Grave's chapter, "Successfully managing your team through

change and transition," has a vague title; the content is not so much a change management overview so much as guidance pertaining to organizational layoffs. Some of the advice ignores the need to understand unique corporate culture, and this could have negative outcomes in execution. Taking his blanket advice to leverage human resources teams but to use caution when approaching managers would certainly have varying results depending on the organization's unique culture.

Some Usefulness for All IM Pros

Since this text is aimed at one type of information professional, it may be challenging for those with

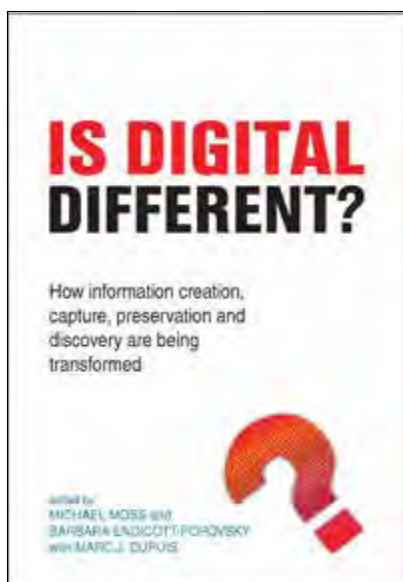
training and strengths in other IM backgrounds (e.g., records managers, content analysts) to leverage this material in a manner meaningful to their roles. However, this book does provide a vast breadth of topical coverage, so it could certainly be used by anyone to review an area of interest on a chapter-by-chapter basis.

With well-written and easily consumable chapters, it is also a quality resource text for its primary audience, offering many insights and up-to-date information on performing information and library services in the corporate environment. **END**

Melanie Sucha can be contacted at msucha@suncor.com. See her bio on page 47.

How the Hybrid Information Environment Is Transforming Libraries, History, Scholarship

Mary Broughall



Is *Digital Different?*, edited by Michael Moss and Barbara Endicott-Popovsky, is a collection of essays that brings together global experts discoursing about the impact of digital

technology on information services. Focusing on the issues surrounding the transition from an analog to a digital environment, contributors examine whether analog practices and procedures are still valid and if they shape or distort those in the digital realm.

One of the co-editors opens the book with a brief overview entitled "What is the same and what is different," which is a fitting summary of where the compilation starts and where it's going. Despite the title, the assumption is that digital *is* different and the various authors take us on a tour of "How information creation, capture, preservation and discovery are being transformed," a very apt subtitle to the manuscript.

Finding Stuff

Chapter 2, "Finding stuff," explores the ways in which we now search for

Is Digital Different? How information creation, capture, preservation and discovery are being transformed

Editor: Michael Moss and Barbara Endicott-Popovsky, with Marc J. Dupuis

Publisher: Facet Publishing

Publication Date: 2015

Length: 360 pages

Price: \$95 (No. America) £49.95

ISBN: 978-1-856-04854-5

Source: www.alastore.ala.org (No. America); www.facetpublishing.co.uk

"stuff" (yes, it is different) and how the scattered nature of the now and future "stuff" finding is consumer driven. It also marks a change, they argue, in

how “stuff” is consumed.

Chapter 6, “Finding archived records in a digital age,” is a synopsis of the method that the UK National Archives in London employs in addressing the statement that “Preservation and findability truly go hand in hand – what real value does an archival collection have if it cannot be effectively used and interpreted?” They delve into their rich history of the problems and solutions to finding things, all the while keeping in mind the “...ability to find/understand/access the archive are inexorably intertwined...”

... one of the problems we face... going forward is that everything is networked.

Interacting with People

Chapter 4, “Crowdsourcing,” is straightforward conversation about the power of the people. Anyone who has seen or heard of the uses (and abuses!) of sites like Wikipedia and GoFundMe will be familiar with the topic. The author comments on breaking down barriers, and this dovetails nicely with the Chapter 2 assertions about the consumer-driven consumption of information. She concludes that while it may not be the answer to such things as staff shortages, it can be very useful in surprising ways, such as engaging consumers in a way that they feel like they have a voice.

Chapter 5, “Pathways to integrating technical, legal and economic considerations in the design, development and deployment of trusted IM systems,” is by far the longest chapter. The authors posit that a single condition, the lack of agreement by stakeholders, is the source of most of the challenges within networked systems. They go on to argue that “...focus on technology alone does not adequately address the system operational variables that arise from human behaviours engaged in by IM system stakeholders.” The ensuing discussion addresses the complexity of the issues

and predicts that standardized tools and rules will emerge to govern the real-time feedback mechanisms that govern interaction decisions.

Untangling the Web

Chapter 3, “RDF, the Semantic Web, Jordan, Jordan, and Jordan,” dissects the novelties of the emerging semantic web in the context of its continuities with the old textual web. The author takes a refreshing approach to the discussion by starting with a definition of the semantic web, then breaking down the definition

phrase by phrase to show how this next step is the logical progression as well as why it’s important. This tactic is commendably educational, especially if you are not familiar with the concept of the semantic web.

Chapter 8, “Rights and commons: navigating the boundary between public and private knowledge spaces,” points out that one of the problems we face now and going forward is that everything is networked. The trust implicit in the act of accessing information not in your custody is at the heart of this essay. The Australian authors present three informative case studies that “...explore the new public-private frontier...” and conclude with a proposal to “...move away from ‘restriction’ being the guiding principle, to the recognition and codification of obligations and responsibilities that a user should sign up to before getting access to archival material.”

Chapter 7, “Security: managing online risk,” written by a co-editor, bravely takes on the topic of electronic security. It employs the most scholarly and technical approach of all of the essays, drawing on cognitive psychology, systems dynamics, and criminal justice. The use of research, including the attendant mathematical models

and formulas, makes this particular essay a bit formidable. However, if this is a topic of interest to you, the discussions are valuable, lucid, and contain plenty of references and notes. The author concludes “...with an admonition about how we should think of ourselves and our activities online in order to stay reasonably safe.”

Wrapping It Up

Chapter 9, “From the Library of Alexandria to the Google Campus: has the digital changed the way we do research?,” is a lovely concluding article. Whereas the opening chapter assured us this new digital age is different, the ending chapter assures us this is a hybrid environment that is built on the printed page – that it doesn’t throw out everything that has come before. We are at the dawn of a golden age, they assure us, with our new-found abilities to transform libraries, history, and scholarship.

Embracing Diversity

The fun thing about any anthology is the diversity of voices and perceptions. The global perspective (this book is published by a UK publisher) reflects the increasingly universal considerations we as information management professionals face.

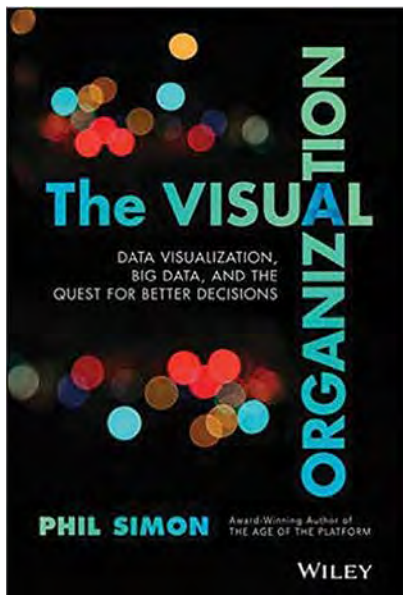
The publisher describes the targeted readership as “...students, particularly those on information studies programs, and academics, researchers and archivists globally.” Given that we are all students in some form or another, this book has something to offer everyone. The fact that each chapter does not build on the one before means you can read these in any order, and even NOT read chapters if you choose. However, they all expand our understanding of our progressively intertwined profession. **END**

Mary Broughall can be contacted at mbroughall@tristategt.org. See her bio on page 47.

Visualize It!

The Key to Driving Better Business Decisions

Robert Bailey, Ph.D., CRM



The author of *The Visual Organization*, Phil Simon, indicates that it is not a book about how to do data visualization – or dataviz, as he calls it. Rather, it’s a book about becoming a *visual organization*, one that is “composed of intelligent people who recognize the power of data” and who “routinely uses contemporary, powerful, and interactive dataviz tools to ask better questions and ultimately make better business decisions.”

These interactive and robust tools allow an organization to analyze its data, records, and information, as well as their relationships, to discover trends, diagnose technical issues, and unearth valuable insights about its customers and services.

According to Simon, because every organization has data, all can benefit from data visualization, including to:

- Understand past events and why they happened
- Monitor current activities

- Generate insights and make more informed organizational decisions
- Discover and identify nuanced issues and ask better questions about existing processes

Profiles Visual Organizations

Simon writes that too many organizations “rely on old standbys [like] bar charts, simple graphs and the ubiquitous Excel spreadsheet. And their business decisions suffer as a result.”

He explains clearly how visualization tools and strategies are being used successfully in organizations every day, featuring profiles of some of the organizations who get it – like Netflix, Autodesk, and eBay. For example, Netflix’s data-centric mindset is captured in its three-part credo:

1. Data should be accessible, easy to discover and easy to process for everyone.
2. The longer you take to find the data, the less valuable it becomes.
3. Whether a dataset is large or small, being able to visualize it makes it easier to explain.

Parallels with RM

Netflix’s credo is not much different from any good records manager’s view. The important additional element of Netflix’s formidable data capabilities is data visualization.

Simon also stresses *metadata*, or data about data, which records managers also recognize as critical to what I call the five rights: getting the right information to the right person at the right time at the right place in the right format

Certainly data visualization goes well beyond everyday recordkeep-

The Visual Organization: Data Visualization, Big Data, and the Quest for Better Decisions

Author: Phil Simon

Publisher: Wiley

Publication Date: 2014

Length: 240 pages

Price: \$50

ISBN: 978-1-118-79438-8

Source: www.wiley.com

ing, but the commonality between the two is the purpose they both also share with data mining, business intelligence, analytics, and enterprise reporting: to lead organizations to a better understanding of their information assets and drive more informed business decisions.

Applies to All

This is a book that every records manager should read. Data visualization is now mainstream, and records managers need to understand its best practice and how it applies to their roles. It will certainly help them illustrate to upper management the bridges between data, records, and the organization’s decision-making needs. In fact, it applies to all employees, as they also can use data visualization to improve their work.

As the volume of electronic records continues to grow, the challenge will, too, but as this book makes apparent, the types of tools available to handle this challenge will also continue to improve. **END**

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



BAILEY



COREY



DERER



FRANKS



PHILLIPS



SNYDER



SUCHA



SWAN

Integrated ECM Solutions: Where Records Managers, Knowledge Workers Converge Page 18

Patricia Franks, Ph.D., IGP, CRM, CA, FAI, coordinates the Master of Archives and Records Administration program in the iSchool at San José State University. She is the author of *Records and Information Management*, co-editor of the *Encyclopedia of Archival Science*, and team lead of *Implications of Web-based Collaborative Technologies in Records Management* (ANSI/ARMA 19-2011) and *Using Social Media in Organizations* (ARMA TR21-2012). She is also a member of the InterPARES Trust research team. Franks can be contacted at patricia.franks@sjsu.edu.

Five Steps In-house Counsel Should Take to Mitigate Information Risk Page 24

H. Kirke Snyder, J.D., has more than 25 years of consulting experience with law firms, corporate law departments, and court administrators. He is an expert in records retention, information management, and e-discovery issues and an adjunct professor of law and ethics at Regis University School for Professional Studies in Denver, Colorado. Snyder can be contacted at kirkesnyder@gmail.com.

Minimizing the Use of Trigger Events to Increase Records Retention Compliance Page 29

Tom Corey, J.D., CRM, is an attorney and Certified Records Manager focusing in the area of records and information management for Consilio LLC. This includes developing records retention schedules that comply with domestic and international requirements. Corey received his juris doctor degree from the Charlotte School of Law, is licensed to practice law in North Carolina, and is an active member in the local bar association and the American Bar Association's Administrative Law and International Law Section. He can be contacted at tcorey@consilio.com.

Software Updates May Be Compromising Your IG Page 32

John T. Phillips, CRM, CDIA, FAI, has made a major difference in the ability of individuals to remain knowledgeable about changing information management methodologies and technologies for many years. He is a consultant with Information Technology Decisions, author, and educator, and his work illustrates how information management professionals can grow as their professional activities increasingly include electronic records. A Certified Records Manager, Certified

Document Imaging Architect, and Fellow of ARMA International, Phillips can be contacted at john@infotechdecisions.com.

3 Keys to Managing Change for a Successful RIM Program Implementation Page 36

Melissa G. Dederer, IGP, CRM, is a records and information governance consultant with more than 20 years of experience in records and information management, project management, and automation experience and is a former member of ARMA International's Board of Directors. A certified Information Governance Professional and Certified Records Manager, Dederer can be contacted at mgdederer@yahoo.com.

Aaron Swan is vice president of client strategy at Electronic Ink, a research and design consultancy located in Philadelphia. He prides himself on being a creative self-starter with an entrepreneurial spirit. Swan has advised companies on the value of planning strategic initiatives and the impact of launching initiatives that require enormous investments. He can be contacted at absswanii@gmail.com.

A Primer for Corporate Librarianship and Information Management Page 43

Melanie Sucha is team lead, Information Management Policies and Standards, at Suncor Energy Inc. She holds a master's degree in library and information sciences and teaches information management in the Faculty of Information and Media Studies at the University of Western Ontario. She can be contacted at msucha@suncor.com.

How the Hybrid Information Environment Is Transforming Libraries, History, Scholarship Page 44

Mary Broughall is a records specialist for Tri-State Generation & Transmission Association Inc. Previously, she did Records and Freedom of Information Act work with the U.S. Department of Energy. She can be contacted at mbroughall@tristategt.org.

Visualize It! The Key to Driving Better Business Decisions Page 46

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.



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 Jennifer about making a splash.



Jennifer Millett
Sales Account Manager
+1 888.279.7378
+1 913.217.6022
Fax: +1 913.341.6823
jennifer.millett@armaintl.org

ADINDEX CONTACT INFORMATION

IBC **Baypath**
graduate.baypath.edu

BC **NAID**
<http://directory.naidonline.org>

3 **Institute of Certified Records Managers**
518.694.5362 – www.ICRM.org

IFC, 39 **Next Level**
www.arma.org/nextlevel



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!

careers.arma.org

THIS IS THE AGE OF **BIG DATA,** OF **ANALYTICS** AND **ALGORITHMS.**

BUT ALSO
CYBER CRIME.

[BOT NETS.
IDENTITY THEFT.
DATA BREACHES.]

THIS IS THE
NEW NORMAL.

STAY AHEAD OF THE CURVE,
MEET THE THREAT, AND
BE READY TO DO BUSINESS.

IN A CONSTANTLY
CHANGING WORLD.

**WE'LL GET
YOU THERE.**

MS in
APPLIED DATA SCIENCE

MS in
**CYBERSECURITY
MANAGEMENT**

MS in
**COMMUNICATIONS
& INFORMATION**

- Online or on-campus options
- Award-winning faculty
- Degree combinations & graduate certificates
- Financial aid available
- No GMAT or GRE required

Classes start in October
Apply Today!

GRADUATE.BAYPATH.EDU

 **BAY PATH**
UNIVERSITY
FOR A CONSTANTLY CHANGING WORLD



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>