

INFORMATION MANAGEMENT

AN ARMA INTERNATIONAL PUBLICATION

JULY/AUGUST 2013

**Accelerating out
of the Recession:
New Approaches to
Executing RIM
Program Strategies**

Page 27

**Using
Data Profiling
to Mitigate
7 'Red Flag'
Information Risks**

Page 34

**CLEARING THE HURDLES OF
INTERNATIONAL
TECHNOLOGY IMPLEMENTATIONS**

Page 22





THE OFFICIAL SPONSOR OF INFORMATION GOVERNANCE



IGaaS



RIM Manager (Records Manager)
Help! @RSDig We have 2 much
information to manage



RSDig (RSD InfoGov)
Are u SURE u aren't over-retaining
information?



LegalMgr (General Counsel)
I hope not, I have to reduce business
#risk and #eDiscovery costs



RSDig (RSD InfoGov)
Have u considered implementing #IG
(information governance)?



RIM Manager (Records Manager)
What is #IG?



RSDig (RSD InfoGov)
#IG enforces desirable behavior in the
creation, use, archiving, and deletion
of ALL corporate information



IT Manager (VP of IT Infrastructure)
Hey, but I have way too many #ECM
and #RIM systems to manage. And
what about content in the #Cloud and
on #SharedDrives?



RSDig (RSD InfoGov)
Use RSD GLASS 2 ensure policy is
enforced across information silos and
regulatory jurisdictions



RIM Manager (Records Manager)
Finally!! +1 RT @RSDig: Use RSD
GLASS 2 ensure policy is enforced
across information silos and
regulatory jurisdictions



RSDig (RSD InfoGov)
This is why we are the official sponsor
of information governance :-)

Trending topics:

#InformationGovernance
#IGaaS™
#CentralizedPolicy
#PolicyEnforcement
#eDiscoveryReadiness
#RepositoryAgnostic
#MultipleJurisdiction
#LifecycleManagement
#RecordsManagementIsNotEnough

THE OFFICIAL SPONSOR



of Information Governance

For more information,
please visit www.rsd.com
or scan the QR code.



INFORMATION MANAGEMENT

JULY/AUGUST 2013 **VOLUME 47 NUMBER 4**

- DEPARTMENTS** 4 **IN FOCUS** A Message from the Editor
6 **UP FRONT** News, Trends & Analysis



- FEATURES** 22 **Clearing the Hurdles of International Technology Implementations**
John T. Phillips, CRM, CDIA, FAI
27 **Accelerating out of the Recession: New Approaches to Executing RIM Program Strategies**
Bruce W. Dearstyne, Ph.D.
34 **Using Data Profiling to Mitigate 7 'Red Flag' Information Risks**
Jim McGann

- SPOTLIGHTS** 38 **GENERALLY ACCEPTED RECORDKEEPING PRINCIPLES® SERIES**
The Principles Assessment as a Collaborative Tool
Julie Gable, CRM, CDIA, FAI
42 **RIM FUNDAMENTALS SERIES**
A 5-Step Strategy for Harnessing Global Information Growth
Brian Nowak
45 **IN REVIEW** Addressing Security Concerns: The Expanding Role of Information Governance
Andrew Altepeter

- CREDITS** 47 **AUTHOR INFO**
48 **ADVERTISING INDEX**



INFORMATION MANAGEMENT

AN ARMA INTERNATIONAL PUBLICATION

Publisher Marilyn Bier

Editor in Chief Vicki Wiler

Contributing Editor Cyndy Launchbaugh

Art Director Brett Dietrich

Advertising Sales Manager Elizabeth Zlitch

Editorial Board Barbara Benson, Director, Records Management Services, University of Washington • Alexandra Bradley, CRM, President, Harwood Information Associates Ltd. • Marti Fischer, CRM, FAI, Corporate Records Consultant, Wells Fargo Bank • Paula Harris, CRM, Director, Global Records Management, Georgia Pacific • John Montaña, J.D., FAI, General Counsel, Montaña and Associates • Preston Shimer, FAI, Administrator, ARMA International Educational Foundation

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 membership in ARMA International. Non-member individual and institutional subscriptions are \$140/year (plus \$25 shipping to destinations outside the United States and Canada).

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

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

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

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

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

© 2013 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.

GET MORE ONLINE

WWW.ARMA.ORG
INFORMATION
MANAGEMENT

7.0 LIABILITY AND WARRANTY

7.1 Acceptance/Limit of Liability. Contractor shall be responsible for financial damages and loss of any materials deposited in bins or otherwise delivered to it for secure destruction due to accident, negligence or willful misconduct up to \$1,000,000. For purposes of this agreement, data breach notification expenses incurred by Customer due to Contractor's actions, including accident, negligence or willful misconduct, shall be considered recoverable damages.

7.2 Ownership Warranty. Customer to deliver for confidential data

legal custodian or otherwise has the right
Customer provides Contractor hereunder.

Service Provider Contract v. 8762

Did we
verify they
have the
proper
coverage?

Page 2

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

Unfortunately, that is not always true.

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

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

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



**Downstream[®]
Data Coverage**

www.downstreamdata.com

Mitigating the Risks of Explosive, Global Information Growth

Although governing the explosive growth of information is a challenge all organizations face, that challenge is multiplied exponentially for those implementing information technologies for operations in multiple countries.

In our cover feature, John Phillips, CRM, CDIA, FAI, advises readers about how to address infrastructure limitations and the regulatory, legal, social, and cultural boundaries and norms of other countries that could be impediments to successfully implementing information technologies that transcend geopolitical borders.

Brian Nowak's international organization struggled with many of these same issues. Despite the wide variations in the level of records management sophistication in his organization's worldwide locations, its global records management team was able to develop line of business liaisons and transition tactical responsibilities to them. Read about how the team followed "A 5-Step Strategy for Harnessing Global Information Growth," to make this transition and become more strategic.

Bruce Dearstyne, Ph.D., picks up on the theme of strategic leadership in his feature, "Accelerating Out of the Recession: New Approaches to Executing RIM Program Strategies." Dearstyne writes that despite the challenges and risks inherent in our "disruptive, digital age," the future is

promising for records and information management leaders who are willing to try non-traditional approaches to traditional leadership strategies.

As the major characteristic of our "disruptive, digital age," explosive information growth increases the costs and risks for organizations that are often hard pressed to even identify what information they have and where it is. In "Using Data Profiling to Mitigate 7 'Red Flag' Information Risks," author Jim McGann describes how these organizations can use data profiling technology to create a data map that will enable them to actively enforce and audit compliance with their information governance policies, which are critical to reducing costs and risks.

With the same goal of helping organizations reduce costs and risks, consultant John Isaza, Esq., FAI, uses "The Principles Assessment as a Collaborative Tool." Author Julie Gable, CRM, CDIA, FAI, interviewed Isaza to discover and write about his techniques and tips for using the Principles Assessment tool to audit and assess compliance with information governance policies and procedures or to formulate new programs.

Reducing information risks is the primary theme of Robert Smallwood's *Safeguarding Critical E-Documents: Implementing a Program for Securing Confidential Information Assets*, which is re-



viewed in this issue by Andrew Altepeter. The book introduces basic information governance principles; outlines the major security problems and risks organizations face; describes countermeasures that can be taken; introduces technologies that can help protect information assets; and provides strategies for obtaining executive sponsorship, managing projects, and selecting vendors.

"Smallwood's book gives readers a solid foundation for making informed governance decisions and presenting them in a way that upper management will find appealing," Altepeter writes.

What information challenges is your organization facing? We'd like to hear about them and develop articles that will help you conquer them. E-mail editor@armaintl.org to tell us how we can help. **END**

Vicki Wiler
Editor in Chief

People.
Communication.
Technology.

Make data discovery projects happen.

We know information management and why it matters.
From forensic data collection to electronic and paper discovery
and beyond, Xact Data Discovery manages the entire process —
giving you one point of contact. What could be easier?

Privately owned and supporting clients nationwide,
with unmatched service for more than twenty years.



XACT DATA DISCOVERY

Because you need to know

(877) 545-XACT

www.xactdatadiscovery.com



MOBILE DEVICES

Do Tablets Have a Future in Business?

BlackBerry CEO Thorstein Heins predicts that tablets will not prove to be an effective business tool.

"In five years I don't think there'll be a reason to have a tablet anymore; maybe a big screen in your workspace, but not a tablet as such. Tablets themselves are not a good business model," Heins said in a recent interview reported by *Engage.com*.

Some attribute Heins' somewhat controversial remarks to BlackBerry's less-than-stellar experience with PlayBook, its version of a tablet. The growth in the use of tablets in the consumer market has clearly seeped into the business market, a trend that some experts believe will continue with the changing demographics of the workforce.

Gartner Inc. predicts that business purchases of tablets will more than triple from 13 million units sold in 2012 to 43 million by 2016. If Gartner is correct, this would, of course, increase the pressure on enterprises to support tablets as business tools.

Yankee Group has expressed a more moderate position. Its research shows a slowing of growth in 2012 and predicts that tablet use in enterprises will flatten in 2013. Yankee Group researchers estimate that 30% of employees will use tablets at work and about 80% of those devices will be employee-owned. Laptops will continue to be the preferred computing method, supported by smartphones for communication. However, the research company does expect tablets to become increasingly popular in retail and other customer-facing positions.

EHR

Pentagon Reassigns EHR Project

It's never good news when the boss takes over your project. Just ask the Pentagon's Military Health System (MHS), which had been tasked with developing a single integrated health records system (iEHR) for the military, in conjunction with the Veterans Affairs Department.

Nextgov reported in April that after having spent \$1 billion on

building a new system, MHS announced it wanted to take a different course. J. Michael Gilmore, the Pentagon's director of operational test and evaluation, wrote a memo to Deputy Secretary of Defense Ashton Carter stating that MHS preferred to buy commercial health IT software rather than develop systems that are based on open standards as mandated by President Obama in 2009. He added that the department was preparing to distribute a request for proposals.

That's when the boss stepped in.

"I don't think we knew what the hell we were doing," Secretary of Defense Chuck Hagel told a House Appropriations Committee Defense panel in April. That's why Hagel stepped in and took



"personal responsibility" for the iEHR project. According to *Nextgov*, he "deferred" the request for proposals and quietly reassigned the project to Frank Kendall, undersecretary of defense for acquisition, technology, and logistics.

The proposals, which never got past the request-for-information phase, will be in Kendall's hands as Hagel works on the overall plan for iEHR. The plan was expected in June.

E-DISCOVERY

Judges on E-Discovery: Keep It in Perspective

At a recent panel discussion on e-discovery, three influential judges agreed that lawyers must take the lead on decisions of proportionality rather than rely on the judges, who are less familiar with the details of the cases.

The panel, titled "Judges Meet the General Counsel Department," was held at a consortium on litigation, information law, and e-discovery. It focused on the proposed additions to the U.S. Federal Rules of Civil Procedure (FRCP) that concern e-discovery's scope, limitations, and need for cooperation.

According to *Law Technology News*, U.S. District Court Judge Shira Scheindlin was joined by Magistrate Judge James Francis IV who, like Scheindlin, is from the Second District of New York, and Circuit Judge Peter Flynn from the Circuit Court of Cook County in Illinois.

"How am I supposed to conduct proportionality (hearings) – especially right up front?" Scheindlin asked. "It's very difficult to know how to vet things when I know little about the case and have so little time."

Flynn agreed: "Why would anybody ask the judge – who knows the least about the case – to make the decisions?"

Flynn also cautioned against "discovery paranoia – the urge to turn over the next rock, no matter the consequences. Proportionality is an attempt to get people to think about the [possible] costs of turning over the next rock."

The judges also said preservation should be viewed from a business perspective, not as a risk management tool for litigation.

"If you make preservation decisions based on what might be needed in litigation, you are going

to save everything, and that's not good for business," Flynn stated.

Francis added that preservation should be just one of the many risk determinations that lawyers make throughout the litigation process.

Scheindlin said the courts may be "moving to staying e-discovery pending a motion to dismiss," thus weeding out cases that cannot proceed.

The advisory committee to the Judicial Conference of the United States proposed significant changes to the FRCP in January. Those changes included limiting the number of production requests and depositions, as well as the amount of time spent on depositions. The committee also proposed

tightening the scope of discovery from any information "reasonably calculated to lead to the discovery of admissible evidence," to relevant, non-privileged information that is proportional to the reasonable needs of the case.

Defense attorneys fear limiting discovery will put their clients at a disadvantage. The judges, however, again contend that the key lies with the attorneys talking to each other up front.



E-DISCOVERY

ISO Moves Forward on E-Discovery Standard

A technical committee of the International Organization for Standardization (ISO) has approved moving ahead with a standard for e-discovery, as reported last month in *Law Technology News*. The official title for the standard is ISO/IEC 27050: *Information Technology – Security Techniques – Electronic Discovery*.

Once completed, the new guidance standard will provide an overview of e-discovery and electronically stored information, define terminology, and address the technological and process challenges associated with e-discovery. This will be the first release in what's expected to become a multipart standard that provides requirements as well as guidance.

The new standard will reportedly incorporate elements from the U.S. Seventh Circuit Electronic Discovery Pilot Program, The Sedona Conference®, various state-sponsored best practice guidelines, and contributions from other experts in the field. It is not intended to supersede or contradict local laws and regulations.

Several countries' ISO delegations support the project, including the United States, United Kingdom, China, Mexico, Belgium, Singapore, Norway, Mexico, South Africa, Italy, and the Republic of Korea. Comments and contributions on the working draft will be due by mid-September and processed at the technical committee's meeting in October.

EHR

HHS Puts EHR Vendors on Notice

The U.S. Department of Health and Human Services (HHS) is taking its role seriously when it comes to certifying – or decertifying – electronic health records (EHR) systems. It recently revoked the certification of two systems developed by EHRMagic Inc. after a six-month investigation that stemmed from an anonymous complaint.

An agency spokesperson told Thomson Reuters the certifications were pulled because EHRMagic-Ambulatory and EHRMagic-Inpatient did not meet the “meaningful use” standards. The standards were defined by the Centers for Medicare & Medicaid Services Incentive Programs that govern the use of EHRs and establish the criteria that eligible providers and hospitals must meet to earn incentive payments. The standards are intended to help ensure access to complete and ac-



curate information, which in turn will empower patients to take a more active role in their health management.

There are about 1,800 certified EHR software products available. To qualify for the incentives, healthcare providers must use a certified program and be able to show that the software fulfills the meaningful use requirement.

Henry Ward, an intellectual property and information technology lawyer, told Thomson Reuters that HHS’ decision to revoke the certification of the two products “doesn’t do a lot in terms of telling the software companies and providers what constitutes meaningful use. [However,] it does provide some context on what doesn’t constitute meaningful use.” More important, he said, it puts providers and software companies “on notice that the concept of meaningful use has teeth in it.”

There are three levels of meaningful use criteria. Stage one (2011-2012) focuses on data capture and sharing; stage two (2014) on advanced clinical processes; and stage three (2016) on improved outcomes. Final rules for the second phase have met some push-back from the industry, which is calling for more time for stage one to ensure systems are working as well as possible and to give more time to ensure integration.

PRIVACY

UK Report: Health Care Too Protective of Patient Data

A landmark report on patient information in health and social care in the United Kingdom has raised serious concerns about the balance between protecting the confidentiality of patient data and sharing to improve care, according to *The Guardian*.

“Our conclusion is that the balance isn’t right,” wrote Dame Fiona Caldicott, who authored the report. “People have become over-concerned about protecting confidentiality.”

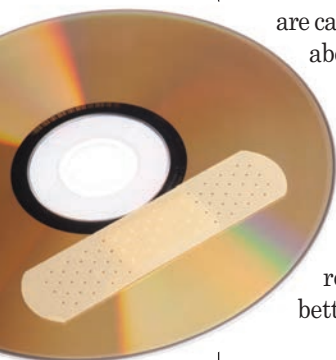
The UK’s former health secretary commissioned Caldicott, a highly respected psychiatrist and psychotherapist, to examine the issue in 2012 following a report from the National Health Service (NHS) Future Forum that identified information governance as an impediment to sharing information, even if sharing would be in the patient’s best interest.

Caldicott contends that much of the problem can be attributed to a lack of public education. “While there are professionals who are familiar with the issue of confidentiality, data sharing, and the various systems in place at the moment, we are not sure that the public is given sufficient information,” she wrote.

“So I think one of the things is how we can help the public – and of course that is a very varied group of people: some are patients, some are carers, some are healthy but interested, and so on – to know more about what is going on in the new health and social care system.”

Caldicott and her team found many instances where IT systems are not linked within hospitals; even fewer are linked between hospitals and other parts of the NHS.

“I think that most NHS patients would be astonished to know that their information doesn’t flow around the system,” said Health Secretary Jeremy Hunt. He thinks that Caldicott’s report provides “the intellectual framework” for approaching better information sharing.



“ With all the complexities of active/inactive records, on-site/off-site storage, and physical/electronic media—**is there an easy way** to keep track of it all in one system? ”

Yes! Zasio has the solution.



ZASIO

RECORDS & DOCUMENT MANAGEMENT EXPERTS

Zasio's powerful suite of intuitive records management software lets you effectively manage both your physical and electronic records, regardless of where they are located—on-site and/or off-site. Whatever the size of your organization or the scope of your records management needs, Zasio has the solution.

To choose the right solution for you, visit our website and download the Versatile™ Selector Guide!

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

800 513 1000, Opt. 1
www.zasio.com

CYBERSECURITY

Privacy vs. Security: A Balancing Act

It's back to the drawing board for the U.S. Congress in its effort to draft cybersecurity legislation that doesn't sacrifice individuals' privacy. Had the most recent bill passed, it was headed for a veto by the White House.

"The president has been clear that the United States urgently needs to modernize our laws and practices relating to cyber security, both for national security and the security of our country's business — but that shouldn't come at the expense of privacy," wrote U.S. Chief Technology Officer Todd Park and Cyber Security Coordinator Michael Daniel, special assistant to the president, in response to an e-petition opposing passage of the Cyber Intelligence Sharing and Protection Act (CISPA).

Balancing privacy and security also emerged as an issue following the bombing at the Boston Marathon in April. The debate centers on the question of whether the bombing could have been prevented if the government and law

enforcement could tighten its surveillance measures.

So where should the line be drawn? That's a question that undoubtedly will be argued for some time to come. It is also a global concern. The same debate is taking place in New Zealand, for example.

The New Zealand Herald recently reported that Roy Morgan Research "sounded alarm bells that the government's response to the growing cyber-security threat may undermine liberties." New Zealanders have become increasingly aware of the challenges of balancing security and privacy as a result of the increased use of new technologies over the past couple of years.

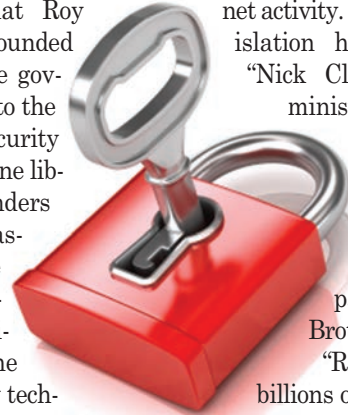
"And with the debate raging over proposed legislation to allow spy agencies and the police to conduct cyber surveillance on New Zealand citizens, these are more relevant than ever," said Pip Elliott, chief executive of Roy Morgan Research. She added that the number of citizens who said they were worried about the invasion of their

privacy through new technology has increased from 54% to 62% over the past decade; it raised two percentage points in the last two years.

In the United Kingdom, the government recently abandoned its efforts to introduce legislation that would have given security services sweeping powers to monitor Internet activity. Opponents of the legislation heralded the move: "Nick Clegg [deputy prime minister] has made the right decision for our economy, for Internet security, and for our freedom," blogged the campaign group Big Brother Watch.

"Rather than spending billions on another Whitehall IT disaster that tramples over our civil liberties and privacy on an unprecedented scale, we should focus on ensuring the police have the skills and training to make use of the huge volume of data that is available."

Discussions over the plan have continued. "The reality is that the technology changes fast and that issue has not gone away," Downing Street told the *Financial Times*.



INFORMATION SECURITY

EU Delays Vote on Data Protection Again

The civil liberties committee of the European Parliament met in early May to discuss the latest draft of Europe's Data Protection Regulation, expecting to vote at that time. Instead, after German Member of Parliament Jan Philipp Albrecht observed that more discussions were needed before the draft was indeed final, the committee decided to delay the vote until the end of May.

PC Advisor reported that Albrecht, who is responsible for shepherding the legislation through to the final vote, said he believes that compromises can be adopted with a broad consensus and be ready for the vote before the summer recess in July.

The goal is to create one regulation that replaces 27 national data protection and privacy laws. More than 4,000 changes to the draft text had been put forward in Parliament. In the end, though, the commission predicts the revised regulation will save industry €2.3 billion (\$3 billion U.S.) annually.



CYBERSECURITY

U.S. and UK Universities: Welcome to Cybersecurity 401



The best way to beat a hacker is to be a hacker. Seniors at the Polytechnic Institute of New York (UNY-Poly) are learning how to be “white-hat” hackers, experts with hands-on experience to help businesses and government agencies protect their data from cyber attacks.

“It’s the new espionage,” Evan Jensen, a senior at UNY-Poly, told Associated Press’s Jake Pearson. “Spies operate from behind keyboards now.” Jensen is one of the leaders of the university’s “Hack Night” events where a group of students meet weekly to hone their hacking skills.

Of course they aren’t really hacking; that would be illegal. But professors and industry experts collaborate to create exercises that emulate real-world hacking scenarios. Dan Guido, a cybersecurity expert and UNY-Poly’s very own “hacker in residence,” uses China’s 2011 attack on Google e-mail accounts – many of the details of which have been made public – as a case study. The students have to map out, step by step, how the hackers accessed a desktop computer and broke into the company’s network.

While Georgia Tech, Purdue, and Carnegie Mellon are well known for their cybersecurity programs, some experts consider UNY-Poly to be among the best programs because of the hands-on, mission-

critical, cybersecurity skills the students are gaining, writes Pearson. Not surprisingly, these students’ job prospects are extremely good. A 2012 report conducted by the SANS Institute, a cybersecurity training organization, stated that the Department of Homeland Security alone needs 600 cybersecurity experts, preferably with real-world training.

Across the pond, two universities will also offer graduate studies in cybersecurity this fall in support of the UK’s national cybersecurity program. The government’s National Security Strategy classifies the cyber attack on the same tier-one level as terrorism. The programs are being developed by Oxford University and the University of London’s Royal Holloway, thanks to a total of £7.5 mil-

lion (approximately \$86 million U.S.) in funding from the UK’s Department for Business, Innovation, and Skills and the Engineering and Physical Sciences Research Council.

The BBC reported that the Oxford program will study security issues related to big data as well as “cyber-physical security,” “the idea that cyber security and physical security need to be addressed together rather than separately.” It will also research computer verification systems. Royal Holloway’s program will work with about 30 businesses and organizations in the security field.

According to Keith Martin, director of Royal Holloway’s Information Security Group, this “represents a significantly different approach to research training.”

INFORMATION SECURITY

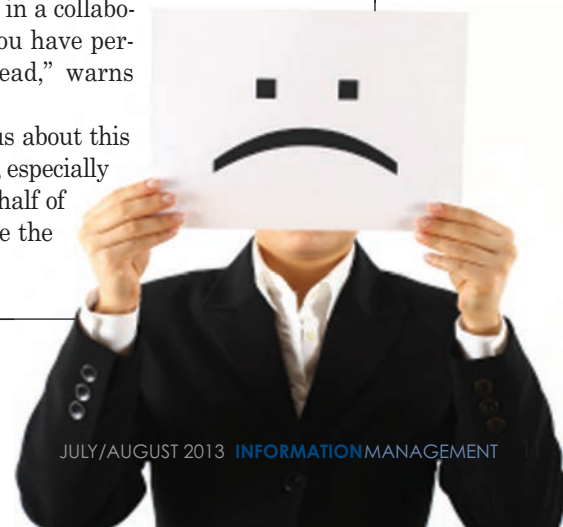
Beware the Enemy Within

A recent study of UK organizations revealed that 83% experienced a data security issue last year. The majority (58%) of those incidents came from within the extended enterprise and may have involved employees, ex-employees, or trusted partners.

The study, “The Enemy Within,” was conducted by Clearswift, a cyber-protection software company. The survey focused on the internal threats affecting UK organizations, a contrast to most studies that have zeroed in on external threats. Most internal threats are malicious attempts or stem from poor business processes or human error. Clearswift maintains they are due largely to a lack of awareness of security policy as well as the increasing use of personal devices for work purposes.

“Combine this with the increased uptake of cloud-based tools and reliance on the extended enterprise in a collaborative working environment and you have perfect security storm conditions ahead,” warns Clearswift.

Organizations need to get serious about this internal threat, the report concluded, especially because the survey discovered that half of local government bodies do not have the resources to deal with the problem.



ARCHIVES

UK Libraries
Build Digital
Archive

Six legal deposit libraries in the United Kingdom have begun building an archive of digital content. Regulations were passed in April that allow the libraries to collect and archive such digital content as websites, blogs, electronic journals, and other digital publications. Specifically, the legal deposit regulations give the six libraries the right to receive a copy of every UK electronic publication, “starting with freely accessible websites on the .uk domain, estimated at 4.8 million websites,” reported *FutureGov* magazine.

The libraries will employ web-crawling software to store

snapshots of 200-500 websites that have been identified as being important for research. These sites will be harvested on a monthly or weekly basis, while others will be captured once a year. Publishers will also be able to submit their material for deposit using a secure deposit portal. According to *FutureGov*, a pilot process has been developed to collect e-books in the ePub format.

The six deposit libraries include the British Library, the National Library of Scotland, the Bodleian Libraries at Oxford University, and the Cambridge University Library. The content will be available to researchers online and onsite via reading rooms at each library. Results of the first year’s collection efforts are scheduled to be available to researchers by year end.

“Legal deposit arrangements remain vitally important,” said UK Culture Minister Ed Vaizey. “Preserving and maintaining a record of everything published provides a priceless resource for the researchers of today and the future. So it’s right that these long-standing arrangements have now been brought up to date for the 21st Century, covering the UK’s digital publications for the first time.”

FACTOID: Legal deposit regulations for print publications have been in place in the United Kingdom since 1662.



CYBERSECURITY

South Africa
Institutes
Australian iCode

South Africa recently became the second country to implement network-level protection for end users. The Internet Service Providers’ Association (ISPA), South Africa’s Internet industry body, developed the voluntary code of practice, iCode, in conjunction with Australia’s Internet industry, which pioneered the approach in 2010.

According to ISPA, the code was designed primarily to protect the privacy of end users, not violate it. “The network-level scanning that allows ISPs to detect signs of infected machines does not in any way involve looking at what users are doing online.”

The code consists of four main elements: a notification/management system; a standardized information resource; a comprehensive resource for ISPs to access the latest threat information; and a mechanism for reporting back to national security agencies in cases of extreme threat.

“By providing plain-English communication about cyber threats, as the iCode requires, ISPs will help inform the public. They will also help customers who are frequently infected to develop simple and effective safety strategies,” the ISPA says.

ISPs that have adopted the code will display a “trust mark” on their websites and other materials.



TOTAL RECALL™

— PHYSICAL RECORDS — MANAGEMENT SOFTWARE

Manage and Protect Your Information

- Manage Onsite and Offsite Records
- Retention and Hold Management
- Organization-Wide Charge-Backs
- SCAN ON DEMAND™
and High-Speed Digital Imaging
- RIM Consulting Services

DHS **WORLDWIDE**™
SOFTWARE SOLUTIONS

Call 1-800-377-8406 • www.dhsworldwide.com

INFORMATION SECURITY

How Well Prepared Are You for a Data Breach?

According to a recent study by the Ponemon Institute and Experian Data Breach Resolution, 52% of U.S. companies have experienced more than one data breach in the past two years.

If your company is like the overwhelming majority of those that responded to the study, there's a great deal you can do to be better prepared for a data breach. For example, do you require employees' mobile devices (including smartphones and tablets) to be tested for security purposes before connecting to the company's systems? The Ponemon study found that although 78% of companies allowed employees to bring their own devices to work, one-third don't require they be tested; another 28% are not sure if they have such a requirement.

Nearly half (44%) of the respondents said their organization effectively authenticates and otherwise ensures appropriate access to their information systems. Only 43% said their organization promptly changes network access rights when an employee leaves the company. This becomes even more alarming when only one-third of companies are actively monitoring for unusual traffic and other risk indicators.

Following a breach, most organizations could improve how well they communicate the incident to their customers. Just 30% of companies actually train their customer service representatives on how to answer questions about a breach.

"Based on the findings of this research, many organizations are losing opportunities to reduce the risk of negative opinion and loss of customer trust by not focusing on communications with victims," the survey report concluded.

Clearly there is a lot of room for improvement in the majority of U.S. companies. A good place to start, according to *Corporate Counsel*, is by addressing many of the gaps highlighted here.

Cyber-liability insurance may be advisable as well, especially for smaller companies. Symantec reported in April that cyber attacks on businesses with fewer than 250 employees increased 31% in 2012 following an 18% increase in 2011. This is testament to the reality that small businesses typically don't have adequate security infrastructure for protecting financial information, intellectual property, or customer data.

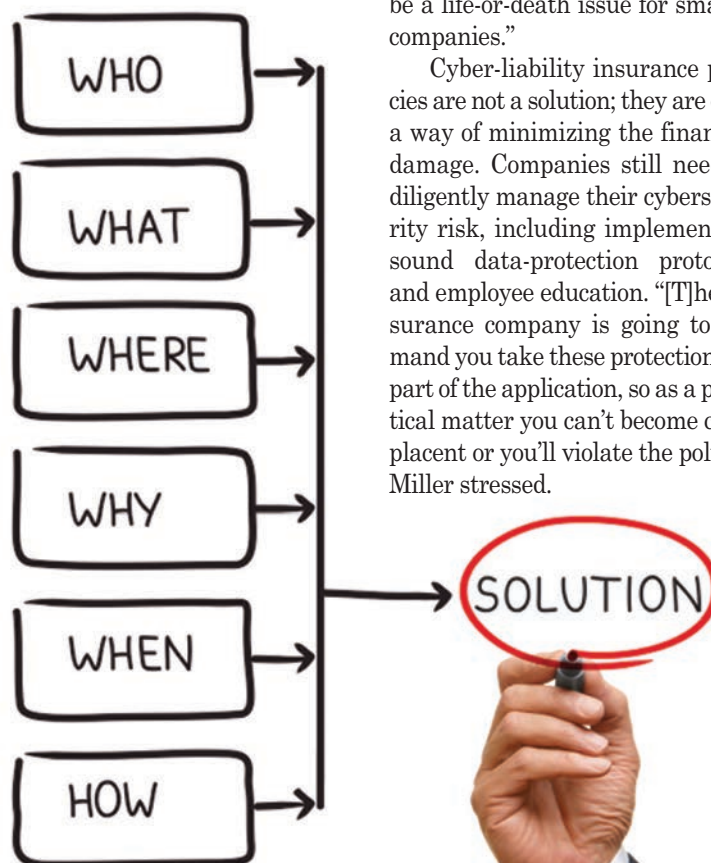
An article in *CFO* magazine reported that small businesses in high-risk industries, such as high technology, financial services, and health care, are "taking out insurance policies to bolster their protection from the potentially crippling

costs that can accompany data breaches and other cyber attacks."

Larger organizations tend to have a risk manager and a strong IT department to help reduce the risk and liability. Smaller companies, on the other hand, may only have a chief financial officer or chief operating officer that doubles as a risk manager.

According to Ethan Miller, an attorney at Hogan Lovells, cyber-liability insurance policies usually cover costs incurred by first-party claims, such as the loss of trade secrets and intellectual property. They also cover damages a company pays when involved in a third-party claim. Miller told *CFO* that most policies also include business-interruption coverage in case of a denial-of-service attack whereby the insurance company would provide payment reimbursement for expenses related to such an attack. Such costs, he said, "can sometimes be a life-or-death issue for smaller companies."

Cyber-liability insurance policies are not a solution; they are only a way of minimizing the financial damage. Companies still need to diligently manage their cybersecurity risk, including implementing sound data-protection protocols and employee education. "[T]he insurance company is going to demand you take these protections as part of the application, so as a practical matter you can't become complacent or you'll violate the policy," Miller stressed.



PII

Millennials: Online Privacy Is Dead

A new study by the University of Southern California (USC) suggests the Millennial generation (ages 18 to 34) has a concept of privacy different from that of their parents and grandparents.

Millennials are more willing to allow companies to track them or access their personally identifiable information (PII) if they receive some benefit, such as coupons. Indeed, 51% of Millennials said they would share PII with companies as long as they got something in return; 40% of those older than 35 felt the same way. The younger respondents are also more open to targeted advertising and, not surprisingly, are more active on social media than their elders.

"It's not that they don't care about [online privacy] – rather they perceive social media as an exchange or an economy of ideas, where sharing involves participating in smart ways," said Elaine Coleman, managing director of media and emerging technologies for Bovitz, the research firm that conducted the survey with USC.



INFORMATION TECHNOLOGY

Britain's MI5 Scratches New Digital RM System

MI5, Britain's top intelligence agency, abandoned its multi-million dollar IT project that would have integrated intelligence data and analysis across all the government departments that feed into the agency. The project goal was to make the agency better equipped to deal with new global security threats.

The new system would have pulled together intelligence gathering and searches of paper archives using the latest digital technology by the beginning of the 2012 Olympics in London. Despite the adding of IT experts and the hiring of a team of expensive consultants, the project floundered, leaving the agency with its outdated system. *The Inquirer* reported that earlier this year the project was re-evaluated and the decision made "to admit failure and restart with a new generation of IT specialists," a decision that is estimated to result in losses of £90 million (more than \$1 billion U.S.).

Before leaving his position, Sir Jonathan Evans, MI5's former director general, reportedly told the Commons Intelligence and Security Committee that the project's delay was acceptable as the system was not urgently needed.



SharePoint®
Governance
is a
good thing.



Governance over
metadata values
enables consistency
when content is
created, uploaded,
and managed
throughout its life
in SharePoint®.

AccessSciences.com/
SharePoint

 **Access Sciences**
www.accesssciences.com



CYBERSECURITY

U.S. Navy Is Serious About Cybersecurity

Despite budget cuts and the sequester and other funding obstacles, the U.S. Defense Department's cyber program has continued unabated, according to Admiral Jonathan Greenert, the chief of naval operations, who spoke to Reuters.

"The level of investment that we put into cyber in the department is as protected or as focused as it would be in strategic nuclear," Greenert said. "It's right up there in the one-two area above all other programs."

The effort makes sense, considering how heavily the U.S. Navy depends on computer networks and satellites to coordinate personnel, ships, and planes.

"Many people who look at the future of warfare say it's bound to start in cyber. The first thing you'd want to do is shut down their sensors, interrupt their power grid, confuse them...and presumably guard against that kind of thing and recognize it if it's starting," he added.

Greenert's comments came

shortly after the Pentagon filed its report with Congress that accuses China of trying to break into U.S. defense computer networks. In addition to China, Greenert said Iran has a "deliberate and emerging" cyber capability, Russia is "very advanced," and North Korea is in the "development stage."

As part of its contingency planning in case of a serious cyber or physical attack on military and intelligence satellites, the Navy is looking at using high-frequency relays employed during the Cold War. The energy blasted from ships by radar and satellite is like a beacon, the admiral explained. Reducing the electronic signature is a key part of the Navy's cyber strategy.

Using radar in targeted patterns, changing frequencies, and shorter pulses are also part of the plan, along with shutting down the systems quickly when in "mission control mode."

"It's like quitting smoking," Greenert said. "You've got to learn to get off this addiction to constant information to and from. Going off the grid can be a good thing."

PII

Australian Privacy Commissioner: Get Ready Now

Australian businesses and government agencies need to get serious about privacy, warned the nation's privacy commissioner and attorney general.

A recent survey conducted by McAfee revealed that 59% of the employees responsible for managing customers' personally identifiable information (PII) were unaware or unsure of the changes

contained in the Australian Privacy Act. The new regulations, which become effective next March, levy large fines – \$340,000 for individuals and \$1.7 million for corporations – if consumer PII is not adequately protected.

The privacy commissioner and attorney general have warned businesses that they need to prepare now for the impending changes, reported *ZDNet*.

Honorary Associate Professor Terry Beed, from the University of Sydney Business School, asserts that a lot of consumer information is being gathered by researchers in a way that doesn't meet the code that governs data collection. Market research tools are readily available to individuals or firms who have no background in market and social research and therefore may not use the data correctly or ethically.

"The ground is changing under our feet," said Beed. "There has been an explosion in the amount of personal data being gathered in the digital environment, and it has revolutionized the way we go about marketing goods and services."



INFORMATION TECHNOLOGY

Data Management New Top IT Concern for Accounting Pros

According to a recent study, managing and retaining data rose to the top of the list of IT concerns for accounting professionals in the United States and Canada. Second on the list for both countries is securing the IT environment, which had been the primary concern cited for the previous nine years.

These were the key findings of the 2013 North America Top Technology Initiatives Survey conducted by the American Institute of Certified Public Accountants (AICPA) and the Charter Professional Accountants of Canada (CPA Canada). Nearly 2,000 accounting professionals participated in the survey, which was designed to “dive further into the core concerns and priorities” that AICPA members have regarding IT. This was the first year the survey was conducted jointly in the United States and Canada.

“While survey respondents see data as a key differentiator for businesses, they are less confident in their organizations’ ability to successfully address several underlying technology priorities than they were a year ago,” according to AICPA’s press release announcing the results of the study. Last year, the majority of U.S. respondents reported they were successfully meeting goals in eight of 10 top initiatives; this year, it was only two initiatives – data management and security.

“The good news is that accounting professionals in both the United States and Canada feel comfortable in handling what they view as their two top priorities for [2013] – data management and IT security,” said Jeannette Koger, director of member specialization and credentialing for the AICPA.

Ranking of Top Technology Initiatives, U.S. and Canada

(Percentage shown is respondents’ confidence level for successfully addressing this priority)

United States	Canada
1. Managing and Retaining Data (55%)	1. Managing and Retaining Data (57%)
2. Securing the IT Environment (51%)	2. Securing the IT Environment (56%)
3. Managing IT Risks and Compliance (47%)	3. Enabling Decision Support and Analytics (33%)
4. Ensuring Privacy (45%)	4. Managing IT Risks and Compliance (57%)
5. Managing System Implementation (44%)	5. Governing and Managing IT Investment and Spending (38%)
6. Preventing and Responding to Computer Fraud (44%)	6. Ensuring Privacy (53%)
7. Enabling Decision Support and Analytics (37%)	7. Managing System Implementation (47%)
8. Governing and Managing IT Investment and Spending (38%)	8. Leveraging Emerging Technologies (22%)
9. Leveraging Emerging Technologies (27%)	9. Preventing and Responding to Computer Fraud (47%)
10. Managing Vendors and Service Providers (47%)	10. Managing Vendors and Service Providers (42%)

Source: AICPA and CPA Canada’s “2013 Top Technology Initiatives Survey”

SharePoint®
can work
right, right
Out-of-the-Box.



Knowledgeable
implementation of
SharePoint®
out-of-the-box
functionality will
save your company
money, promote
supportability, and
lead to more timely
implementation.

AccessSciences.com/
SharePoint

 **Access Sciences**
www.accesssciences.com

PRIVACY

Apple's Privacy Headache Intensifies

Apple is taking heat for its privacy policy in both Germany and the United States. On April 30, a Berlin court ruled that Apple's privacy policy violates Germany's privacy law. Apple must either change its policy or appeal the decision.

In 2011, the Federation of German Consumer Organisations (VZVB) accused Apple of "unfair contractual clauses" in its privacy policy, according to *PCWorld.com*. The company eventually changed five of the 15 clauses that were cited by VZVB, but the federation was not satisfied. In 2012, VZVB filed a lawsuit against the software giant. In response, Apple committed to changing two additional clauses, but the VZVB contended the policy still violated German law. The court agreed.

Apple's German privacy policy, which is similar to the U.S. policy, gives the company broad and unspecified use of customers' private

information. It also allows Apple to use the personal information for the issuance of gift cards. German law, however, requires that a company advise customers of exactly what personal information would be used and for what purposes.

As of press time, Apple had not commented on whether it would appeal the decision or change its policy accordingly.

Meanwhile, in the United States, privacy watchdog group Electronic Frontier Foundation (EFF) blasted the technology giant for its lack of transparency with its privacy policies. According to the EFF, Apple could be freely giving up user information to the government. Apple was one of four companies the EFF cited for its lack of transparency; the others were AT&T, Verizon, and MySpace.

EFF cited the four after evaluating 18 companies on six criteria:

- Whether a warrant was required for content of communications

- Whether the firm tells users about government data requests
- The availability of published transparency reports
- Published law enforcement guidelines
- A public record of fighting for user privacy rights in the courts
- Whether the firm supports efforts in Congress to protect privacy rights

The news for Apple wasn't all bad, though. EFF recognized it and AT&T for being members of the Digital Due Process coalition, a group that advocates for user privacy issues in Congress. Only Twitter and *Sonic.net* received gold stars for all six criteria.

END



Who has your back?

	Requires a warrant for content	Tells users about gov't data requests	Publishes transparency reports	Publishes law enforcement guidelines	Fights for users' privacy rights in courts	Fights for users' privacy rights in Congress
Amazon	★	★	★	★	★	★
Apple	★	★	★	★	★	★
AT&T	★	★	★	★	★	★
Comcast	★	★	★	★	★	★
Dropbox	★	★	★	★	★	★
Facebook	★	★	★	★	★	★
FourSquare	★	★	★	★	★	★
Google	★	★	★	★	★	★
LinkedIn	★	★	★	★	★	★
Microsoft	★	★	★	★	★	★
MySpace	★	★	★	★	★	★
Sonic.net	★	★	★	★	★	★
SpiderOak	★	★	★	★	★	★
Twitter	★	★	★	★	★	★
Tumblr	★	★	★	★	★	★
Verizon	★	★	★	★	★	★
WordPress	★	★	★	★	★	★
Yahoo!	★	★	★	★	★	★

Source: Electronic Frontier Foundation "Who Has Your Back?" reports: 2011, 2012

"All I did was suggest we NAID the old records."

See what
happened at
www.naid-em.com.



NAID, the NAID logo, and the NAID Certification logo are registered trademarks of the National Association for Information Destruction.





LIVE!
CONFERENCE
& EXPO

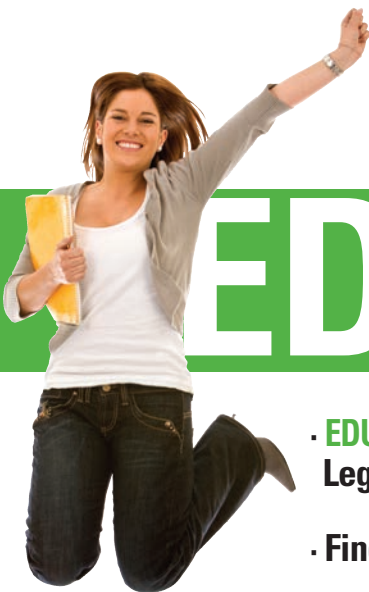
THE PREMIER EVENT IN INFORMATION
GOVERNANCE BROUGHT TO YOU BIGGER,
BETTER, AND MORE **COLORFUL!**

MOTIVATE!

- Catch **FRANK ABAGNALE** at the Opening General Session
- **TECHNOLOGY IN THE SPOTLIGHT** will focus on business security for information governance professionals
- **NEW!** Featured Track Sessions
- **NEW!** Lunch with the Experts



EDUCATE!



- **EDUCATION TRACKS** for Technology Solutions, Business Value, and Legal and Compliance
- Find your **SKILL LEVEL** to tailor the conference experience YOU need
- A Town Hall Meeting with **THE SEDONA CONFERENCE®**
- Take advantage of **PRE-CONFERENCE SESSIONS**

ARMA LIVE! Conference & Expo 2013 offers inspiring speakers to **MOTIVATE**, the best in the business to **EDUCATE**, and cutting-edge best practices and technology tools to **STIMULATE** your quest for career growth. Here are a few highlights for you to look forward to:

STIMULATE!

- See the industry's **EMERGING TECHNOLOGIES** at the ARMA Expo
- Cheer on colleagues at the **AWARDS LUNCHEON**
- The 2013 **WELCOME PARTY** is a Venetian masquerade
- **PUB CRAWL** cocktail reception on the Expo Hall Floor
- A perennial favorite, the **CANADIAN PARTY**



WE'RE WHEELIN' AND DEALIN' UNTIL SEPTEMBER 16!

SAVE \$100

with the Early Bird Discount!

Register by Sept. 16
Member Non-Member

FULL CONFERENCE REGISTRATION ~~\$1,199~~ **\$1,099** ~~\$1,449~~ **\$1,349**

Want to save even more? See how when you register at www.arma.org/conference.

VIVA! ARMALAS VEGAS2013
Conference & Expo, October 28-30
The Venetian Congress Center
Register today! www.arma.org/conference



CLEARING THE HURDLES OF INTERNATIONAL TECHNOLOGY IMPLEMENTATIONS

Making an action plan that addresses the infrastructure limitations and the regulatory, legal, social, and cultural boundaries and norms of the countries where an enterprise wishes to expand is critical to successfully implementing information technologies globally.

John T. Phillips, CRM, CDIA, FAI

Implementing technology-based information management (IM) systems can be a nightmare. Yet, candid vendors of IM systems will be very clear that how the technology is implemented is at least as important to its success as the product's capabilities; complete access to all of the product's features is required for the organization to fully realize its benefits.

Technical issues are to be expected; implementing a new technology may require operating systems upgrades, software integrations, accurate data migrations, and more modern hardware or networking infrastructures.

Well-known human factors to be attended to include training for the application interface, planning for the system rollout, and gaining buy-in for organizational adoption of the technology.

All of these issues must be thoroughly addressed to get maximum return on investment from any system implementation. And, extending an implementation to international business environments will compound these challenges.

... implementing a new technology may require operating systems upgrades, software integrations, accurate data migrations, and more modern hardware or networking infrastructures.

Technology Infrastructure Issues

Implementing “global technology” – any information processing and storage technology that can reach across geopolitical boundaries – throughout an international enterprise can make both the goals and the impediments to achieving those goals vastly more complex.

Determining Network Readiness

International network readiness is critical to information technology implementation and varies drastically among regions and jurisdictions.

In many geographic locations, there is an absence of networking infrastructure, supportive technology vendors, or trained personnel. Organizations must determine whether it is best to send trained individuals to sites where servers and applications will be located or to train local individuals in IT systems maintenance.

The correct decision may depend on whether there are trained and educated individuals in that location already who can receive additional training to become system administrators. How these questions are answered can have a major impact on system performance.

Unfortunately, the implementation of these technologies is very inconsistent around the globe. For instance, India is a good example of a country where records are valued, but it is swamped in managing paper records, due in part to a lack of technology infrastruc-

ture to support electronic records management.

As another example, the authors of *The Global Information Technology Report 2013 – Growth and Jobs in a Hyperconnected World* write that “Asia is home to some of the world’s wealthiest, most successful economies in the world and also to some of its poorest. Unsurprisingly, a similarly profound diversity characterizes Asia’s digital landscape, thus making it impossible to draw a uniform picture of the region. The most digitized and innovative nations – the Asian Tigers – on the planet are next to some of the least-connected ones. Nowhere else does the regional digital divide run as deeply as it does in Asia.”

Locating Servers/Data

If an international enterprise wants to share data among employees in U.S., European, and Asia/Pacific countries, it may be a challenge to decide where it locates the servers, software, and data.

Most businesses are not comfortable with public dis-

cussion of these issues in great detail. However, in “off the record” talks, some admit they often segment data in database applications so that specific data will be stored in a distributed manner across different servers to allow compliance with the laws and regulations governing the origin of that data.

The unfortunate consequence of that approach is that some data may not be seen in the results of queries initiated from locations that do not share a mutually agreed-upon understanding of the compliance regulations of the country where the data is stored.

More common is that many enterprises separate both data and applications so there are fewer technical complexities. It is easier to generate reports that are country-specific based on the origin of the data in the reports and then subject the reports themselves to compliance scrutiny. Thus, U.S., European Union (EU), China, India, and Middle Eastern business locations may have different servers, applications, and databases.

In addition, operating systems and applications often are implemented in different languages. The very definition of a record, a document, and data can vary among cultures, as can the concepts of responsible recordkeeping. It can be easier to avoid too many interpretations of language and culture across political and regional influences by having data stored in a particular country according to its customs, linguistic nuances, and laws.

Using the Cloud

There is much discussion today about processing and storing information in “the cloud.” For instance, using Gmail, Google Docs, or similar services typically means configuring an application and data storage space on a remote disk drive accessible over an Internet connection that appears as an extension of a local computer.

According to the Google website’s “Google Apps for Business,” “Google Apps is a cloud-based productivity suite that helps you and your team to connect and get work done from anywhere on any device.” Note that it says “anywhere.” Although users are expected to conform to local security policies and electronic records retention rules for their work environments, it may be difficult to implement those policies and practice those procedures in cloud environments where the organization has little control over data storage and access.

... it may be difficult to implement ... policies and ... procedures in cloud environments where the organization has little control over data storage and access

Dealing with Big Data

IT systems’ architectural dilemmas with storage communications or the location of servers can wreak havoc with new software technologies that support concepts like “big data.” The very essence of big data technology is to cross-search databases and derive meaning from data accumulations from many sources by using advanced search algorithms to analyze information.

In fact, big data is often used to detect trends in customers or markets and, therefore, it can be particularly focused on personally identifiable data, thus running afoul of conflicting information governance statutes.

Clear understanding of the data and the metadata used to describe big data database content is critical, as is knowing precisely where each data element is stored. Unfortunately, Internet domain extensions, such as .us, .ca, or .eu, cannot be relied upon because computers do not always recognize regional boundaries even when these domain extensions are present, and the unscrupulous can devise ways to circumvent these limitations.

Protecting Intellectual Property

The growing challenge of software piracy is a good example of the starkly different perspectives among countries about technology use. Most individuals in western, economically well-developed countries understand and generally respect the system use requirements specified in software manufacturers’ end user license agreements (EULAs), which users must accept for the software to be activated. Because these are contractually binding agreements, individuals in western nations generally pay attention to these “boundaries.” They know they can be held

financially and legally responsible for compliance.

Unfortunately, that is not the case in many other countries, where there are growing problems with software piracy and copyright violations despite occasional well-publicized prosecutions. Software piracy is an international concern, especially regarding western-created software in use in China.

Kenneth Rapoza, in his July 22, 2012, *Forbes* article “In China, Why Piracy Is Here to Stay,” wrote, “Piracy goes back to the China world view that individual rights don’t matter. The courts have never evolved to protect innovative individuals.”

Microsoft CEO Steve Ballmer was quoted in a January 21, 2011, *Network World* article as saying that “90% of Microsoft software users in China didn’t pay for it.”

So, if an organization decides to expand its scope of business where there are cultural and legal system barriers to

basic trust and accountability, it should not expect its own intellectual and corporate properties to be respected.

Similarly, where there is not a uniform set of legal and regulatory expectations for hardware, software, and networking systems operations and ownership, the organization may have difficulty protecting the data in its own servers and systems.

If an organization is planning to expend capital and resources where the technology assets may be at risk, it may be unable to convince investors, customers, and decision-making executives that an implementation will be successful.

Information Use Issues

It’s one thing to worry about the consequences of investing in hardware and software infrastructure to be used internationally by employees, but it’s another matter entirely to be concerned about how those employees create and share content within those systems.

Because countries have varying perspectives about information and records, they will have varying attitudes toward personal and business information that is stored in computers and transmitted across networks. In addition, what is permissible in some countries and cultures may be unsupported or a violation of others’ laws.

Transmitting Info Across Borders

Of particular interest is the matter of storing and transmitting data within communications systems and large databases, especially with respect to transmitting information across international political borders. Because attitudes and regulations on the use and privacy of personally

Making a Global Technologies Action Plan

When enterprises are moving business processes overseas or planning to take advantage of foreign operation sites and employees, a specific plan to address international IM technology implementation issues will be critical to the success of those initiatives. Technologies, IM policies, applicable laws, regulations, and cultural norms must be evaluated by a cross-enterprise team of information users, compliance experts, and IT professionals. Consider taking these actions:

1. Identify and technically characterize the extent and specific infrastructure of each technology to be used, such as e-mail and social media.
2. Identify the locations where data may be stored or shared among users and characterize the content.
3. Identify the applicable laws, regulations, IM standards, and cultural norms that may have an impact on records management or technology use in the countries of interest.
4. Identify records management consultants and service vendors with experience and existing services in the countries of interest.
5. Identify law firms with international legal system expertise that are familiar with relevant laws, regulatory guidelines, and cultural expectations.
6. Create a matrix of these factors.
7. Form a technology implementation team wherein individuals take responsibility for creating portions of a global technology implementation compliance plan that will address all issues.

identifiable information vary dramatically among countries, some organizations maintain separate servers and networks in an attempt to identify and manage information appropriately within specific geopolitical boundaries.

In addition, communications media, such as e-mail, text messages, and social media, enable cross-border data flows and data storage at the initiation of computer users who often have little knowledge of the end use or storage location of the information they are creating and transmitting.

When people create e-mails or text messages, they usu-

ally think about their content with respect to their own information management, governance, or security policies. Rarely do they consider the receivers' information management policies or their countries' laws or regulations – or that these messages could be re-transmitted and used internationally far beyond their original intent.

Complying with End-User Agreements

Although software EULAs do not typically contain clauses that limit the content type and nature of the information that is created or stored, acceptable use policies (AUPs) for remote computing platforms, such as those offered by Google, Facebook, and other social media vendors, often impose limits.

These AUPs do not typically garner a high level of attention and compliance by end users, who often feel they can create and share “their” information any way they want. These free and freewheeling information-creation and -sharing environments often seem to encourage personal expression and communication with few restrictions, in stark contrast to the limitations described by the AUPs.

For instance, the first three of eight restrictions in Google Cloud Platform’s AUP are:

“Customer agrees not to, and not to allow third parties (including End Users) to use the Services:

- to violate, or encourage the violation of, the legal rights of others (for example, this may include allowing End Users to infringe or misappropriate the intellectual property rights of others in violation of the Digital Millennium Copyright Act);
- to engage in, promote or encourage illegal activity;
- for any unlawful, invasive, infringing, defamatory or fraudulent purpose (for example, this may include phishing, creating a pyramid scheme or mirroring a web-site);...”

Users in various countries will have different interpretations about what “illegal activity,” and “violate, or encourage the violation of, the legal rights of others” mean. It may not be clear to them whether these terms are defined according to U.S. law (where Google’s corporate headquarters is located) or according to the laws of the country where the employees and customers reside or use these technologies.

These matters make it clear that it’s crucial to retain expert counsel who speak the language, understand the business environments and cultural norms, and can assist directly in disputes within the legal and regulatory frameworks of the countries that would be a part of the expanded enterprise.

Rolling out information technologies requires a consensus from the parties involved that these risks will be addressed during implementation so misunderstandings about the appropriate use of technology are few. Having individuals to represent an organization overseas who have “boots on the ground” can be invaluable.

Protecting Information Privacy

Posing particular dangers during international implementation of technologies are the varying cultural and geopolitical infrastructures that bear on information creation, storage, and use.

A good example is the extreme difference between European and U.S. laws on the privacy and control of personal data. U.S. citizens have little control and voice in enterprises' use and reuse of their personal data for business purposes, whereas there are strict rules in Europe on the use of personal information for commercial purposes.

The EU is subject to Data Protection Directive 95/46/EC that protects individuals with respect to the collection, processing, and storage of data. It strives to achieve a comprehensive balance between protecting personal data and allowing the free flow of information within the EU. Europeans are often concerned with how data created in the EU could eventually be transmitted to the United States and misused according to EU regulations.

That is because U.S. laws tend to regulate the use of personal information only in specific circumstances. For instance, the Privacy Act of 1974 protects information gathered on individuals working within the federal government framework, but it does not apply to the private sector. The Health Insurance Portability and Accountability Act (HIPAA) governs restrictions on health information, but it is focused primarily on medical records. And, the Gramm-Leach-Bliley Act governs how financial insti-

tutions create policies to share data about customers between those businesses.

Obviously, it can be difficult to determine how to integrate and navigate all of these overlapping or conflicting legal and regulatory mandates. So a U.S.-EU Safe Harbor Directive was developed by the U.S. Department of Commerce and the European Commission to bridge "differences and provide a streamlined and cost effective means for U.S. organizations to satisfy the (EU) Directive's 'adequacy' requirement."

If an organization is going to do business in Europe, either by creating data there or creating it in the United States and exchanging it across national boundaries, it must be able to comply with the requirements of the business environment.

Planning for Success

All of these factors have a direct impact on the manner, means, and feasible extent of implementing technologies across international enterprises. Organizations must address the types of risks described above to negotiate the implementation hurdles that can arise. Planning thoroughly to address the expanded enterprise challenges of international projects is critical to achieving success in implementing information technologies globally. **END**

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



2013-14 Records & Information Management BUYER'S GUIDE

Available online at www.arma.org

Featuring **78** of the Leading
Information Governance
Companies!



TIME TO BUY!

Looking for a Service Provider or Product?

Look no further...We have them listed, from A to Z!

Your Connection to
RIM Products and Services

BUYER'S GUIDE ONLINE!

Whether you're looking for a software solution, records center, or archiving supplies the *Records and Information Management Buyer's Guide* is the place to start.

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

www.arma.org/buyersguide

Accelerating out of the Recession:

New Approaches to Executing RIM Program Strategies

The volume, velocity, variety, and value of information assets organizations are creating and receiving provide a platform for information governance professionals to step up to a more strategic leadership role.

Bruce W. Dearstyne, Ph.D.

The recession is ending, the economy is recovering, and enterprises are bouncing back. The future looks promising – particularly for records and information management (RIM) program leaders who are willing to try nontraditional approaches to meeting the challenges posed by the current “disruptive” forces in information management.

Challenges of the Disruptive, Digital Age

In “Top 10 Technology Trends Impacting Information Infrastructure, 2013,” Gartner Inc. describes several of these disruptive forces, including big data, an expanding information infrastructure, and new strategies for assigning value or risk to information assets.

The report stresses there are big opportunities and risks going forward: “Significant innovation continues in the field of information management (IM) technologies and practices driven by the volume, velocity and variety of information, and the huge amount of value – and potential liability – locked inside all this



ungoverned and underused information.”

Additionally, the report emphasizes that “practically all information assets must be available for delivery through varied, multiple, concurrent and, in a growing number of instances, real-time channels and mobile devices.” Because of these ongoing “disruptions,” it’s more important than ever to be able to share and repurpose information for “multiple context delivery and use cases,” the report suggests.

Taking non-traditional ap-

proaches to the seven traditional strategies described below will help RIM programs adapt to, and shape, this complicated future.

that data can provide.” According to Mellon, the leader has no safety net and needs to know when to take risks, make tough decisions, ensure implementation, and assume responsibility if things go wrong. Being quicker and more fluid in making decisions will pay off. “Whereas some dither, you move to action,” she writes.

2. Build Resilience into Programs. The recession has also provided insights through experience about cushioning against and bounc-

ing back from adversity and unanticipated events. In the book *Resilience: Why Things Bounce Back*, authors Andrew Zoll and Ann Marie Healy define resilience as “the capacity of a system, enterprise, or a person to maintain its core purpose and integrity in the face of dramatically changed circumstances.”

- They proactively monitor their environments, seek out potentially disturbing information, identify potential disruptions, and look for early warning signals that the program may not be meeting stakeholder expectations.
- They build in flexibility and safeguards against disruption, such as redundant systems, full staffing levels, robust IT systems, and backup capacity for storing records.
- They promote a culture of shared purpose and values that focuses on the impact of the program and its services, and they build pride that can help sustain the program in hard times.
- They foster a culture of experimentation and innovation that predisposes people toward trying new things in hard times.
- They practice what *Resilience* calls “adhocracy,” which is characterized by “informal team roles, limited focus on standard operating procedures, deep improvisation, rapid cycles, selective decentralization, the empowerment of special teams, and a general intolerance of bureaucracy.”
- They prepare staff members for difficult times by providing training that encourages people to imagine possibilities, display inventiveness in problem solving, and develop alternatives when traditional approaches are threatened or curtailed.

When faced with adversity, they resist the temptation to hunker down or retreat. They develop plans for fighting cutbacks. If budgets are cut, they present a clear sense of priorities and a plan for reducing programs in a way that focuses on essentials, minimizes reductions to essential services, and cushions impact on staff.

3. Develop Effective Strategies. Mission and vision statements are essential, experts agree, but it can take too long to develop and refine them. In the meantime, particularly in times of fast-paced change, unforeseen opportunities may have passed, or unforeseen crises may have arrived. A.G. Lafley and Roger Martin in *Playing to Win* suggest we move faster by shortening discussions of mission and vision, reducing lengthy planning, and focusing more on strategy, “an integrated set of choices” that positions the organization to “create sustainable advantage and superior value.” This book and other recent literature describe strategy on a fast track:

Taking non-traditional approaches to the seven traditional strategies described below will help RIM programs adapt to, and shape, this complicated future.

proaches to the seven traditional strategies described below will help RIM programs adapt to, and shape, this complicated future.

1. Apply a High-Visibility, Decisive Leadership Style.

Until recently, many leadership authorities encouraged a deliberate, extensively consultative style. The leader, they proclaimed, needed to build consensus and be sure all issues were resolved, resources aligned, and stakeholders fully supportive before taking action.

Newer literature, more attuned to the fast-changing, post-recession world, advises less consultation and deliberation and more accelerated decision-making, even when the evidence is incomplete or ambiguous. In fact, the more innovative the program, the less likely it is to have incontrovertible evidence before deciding whether to change course.

“Eat the uncertainty,” advises Liz Mellon in *Inside the Leader’s Mind*, and beware of “the spurious comfort

ing back from adversity and unanticipated events. In the book *Resilience: Why Things Bounce Back*, authors Andrew Zoll and Ann Marie Healy define resilience as “the capacity of a system, enterprise, or a person to maintain its core purpose and integrity in the face of dramatically changed circumstances.”

Resilience varies from program to program, but resilient enterprises have these traits:

- They proactively monitor their environments, seek out potentially disturbing information, identify potential disruptions, and look for early warning signals that the program may not be meeting stakeholder expectations.
- They build in flexibility and safeguards against disruption, such as redundant systems, full staffing levels, robust IT systems, and backup capacity for storing records.
- They promote a culture of shared purpose and values that focuses

Keep on the Path to Success!

Subscribe to Paralegal Today!



Your subscription includes instant access to the current and previous editions online.

SUBSCRIBE OR RENEW TODAY!

PARALEGAL TODAY

The Authority for the
Paralegal Profession

As new technology and other factors affect the legal field, paralegals and other information professionals are being called on to know more and do more. To keep pace with the changes and complexities impacting the paralegal profession, it is vital for you to be highly informed of the latest developments, trends, and practices. One of the best ways to do that is by subscribing to **Paralegal Today!**

For 30 years **Paralegal Today** has been providing paralegals and legal assistants with the information they need to perform their jobs better. The ideas, techniques and insights you get from every issue will improve your skills, enhance your performance and help to make you an essential member of the staff at your firm or organization. This well-rounded, leading independent magazine brings you useful, pertinent content, including best practices, special reports, surveys, technology tips, association updates and much more to help you stay sharp and advance in your career.

Your subscription to **Paralegal Today** includes the regular quarterly issue plus easy access to previous editions online that you can read on your iPad or iPhone anytime, anywhere. You also enjoy a robust Web Site with a helpful Listserv, a job bank, and other great features.

**As a Legal Professional you save
20% off the newsstand price!**

Professional Discount Rate (USA)
1 year 4 issues \$32
(Save 20% off the newsstand price of \$39.80)

TO SUBSCRIBE, GO TO:
www.paralegaltoday.com
OR CALL TOLL FREE
1 877 202-5196

What “Lean Startups” Do Differently

Organizations that follow the “lean startup” approach take a view that differs from traditional ones. The following chart illustrates these changes. Developed by Steve Blank, it appears in “Why the Lean Start-Up Changes Everything,” *Harvard Business Review*, May 2013.

Feature	Traditional	Lean
Strategy	Business plan Implementation-driven	Business model Hypothesis-driven
New-product process	Product management Prepare offering for market following a linear, step-by-step plan	Customer development Get out of the office and test hypotheses
Engineering	Agile or waterfall development Build the product iteratively or fully specify the product before building it	Agile development Build the product iteratively and incrementally
Organization	Departments by function Hire for experience and ability to execute	Customers and agile development teams Hire for learning, nimbleness, and speed
Financial management	Accounting Income statement, balance sheet, cash flow statement	Metrics that matter Customer acquisition cost, lifetime customer value, churn, viralness
Failure	Exception Fix by firing executives	Expected Fix by iterating on ideas and pivoting away from those that don’t work
Speed	Measured Operates on complete data	Rapid Operates on good-enough data

- Develop a “winning aspiration” – a concise statement of what the program seeks to be and what “winning” or success will look like.
- Define the distinct or unique value the program offers – what it does that no one else can do, and why that is important. For RIM programs, that might be risk management, legal defensibility, cost savings, or organization of records and information for quick access.
- Define issues, but don’t get bogged down. Move quickly to define two or more mutually exclusive options that could resolve each issue. That moves the discussion to strategies and solutions rather than problems and obstacles.

- Specify the conditions for success. For each possibility, what must be true for it to be strategically sound?
- Test for feasibility, distinctiveness, and customer satisfaction on small pilot projects, if possible.
- Identify barriers and obstacles.
- Determine what management capabilities and systems are required.

4. Speed up Innovation.

Traditional project management often involves substantial projects, extensive planning, intensive management, and strict definitions of success: on time, within budget, and within project specifications. Newer approaches are more pragmatic, improvisational, iterative, and faster. Rather

than beginning with a business plan, they start with the search for a model. Quick rounds of experimentation and feedback reveal what works. The newer approaches emphasize breaking large projects into smaller ones, bringing in new ideas, experimenting, adapting, using what works, and learning quickly from unsuccessful initiatives.

Eric Ries in *The Lean Startup* emphasizes shortened development cycles, extensive customer engagement, and continual feedback in the development of new services and products. The book advances these two concepts: 1) *validated learning*, which means to try an initial idea and quickly measure it to see if it moves toward the goal of

building a sustainable program; and 2) to *pivot*, or make a “structured course correction designed to test a new fundamental hypothesis about the product [or] strategy.”

Peter Sims recommends “little bets” – discrete “concrete actions taken to discover, test, and develop ideas that are achievable and affordable.” These can result in “small wins” you can build on and extend, or “failing quickly to learn fast” from small, experimental projects. You can then use the insights to modify the idea or try something entirely different. (For additional perspectives, see the sidebar “What Lean Startups Do Differently.”)

RIM programs that are agile and adaptive need motivated and empowered staff. Leaders need to solicit ideas from employees who interact with customers every day and, therefore, are in the best position to discern emerging needs and opportunities.

Additionally, since RIM program managers cannot anticipate every eventuality, it is useful to empower staff to make on-the-spot decisions and use workarounds to meet customer needs. Hiring employees who are inclined toward innovation is an essential prerequisite. Setting clear goals and empowering people to reach them – by allowing a fair amount of leeway in how they do their work – are helpful tactics.

Teresa Amabile and Steven Kramer’s book *The Progress Principle* explains that “a sense of progress” is a key motivator. On days when workers sense they’re making headway or when they receive support that helps them overcome obstacles, their emotions tend to be positive and their drive to work even harder is high. On days when they feel they’re wasting their time, encountering roadblocks, or fighting red tape, their motivation and engagement tend to be the lowest. Amabile and Kramer advise managers to clarify goals, ensure that workers’ efforts are properly supported, use minor problems and

setbacks as learning opportunities, and provide positive feedback and recognition.

Adrian Gostick and Chester Elton in *All In* advance the idea of “a culture of belief” that includes articulating a “burning platform” core message about the urgency of the work, treating staff as colleagues and talented partners rather than employees, broadly sharing information, establishing accountability, and continuously expressing appreciation and recognition.

They advise leaders to aim to

Setting clear goals and empowering people to reach them – by allowing a fair amount of leeway in *how* they do their work – are helpful tactics.

make everyone feel *engaged* (attached to the program, willing to give extra effort), *enabled* (empowerment is the norm; initiative is valued), and *energized* (having a sense of well-being and drive).

5. Use a ‘Culture of Participation.’ Staff input is essential for fast-paced, customer-focused innovation, but Thomas Davenport and Brook Manville in *Judgment Calls* advocate going further to get the best solutions. Leaders need to make decisions in a timely way, they explain, but often this involves creating processes and systems for finding the best means of quickly gathering and processing information.

The book recommends “the power of leveraging colleagues, partners, and ‘networks of learning,’ trading away absolute power and hierarchy for more facilitative leadership that engages a broader and diverse mind for the challenges of today’s more complex business environments.” Tactics include:

- Define goals in ways that are quantifiable, where possible, and use data and analytics to make decisions.
- Identify model programs and best practices by monitoring blogs, social media, and other electronic discussion formats.
- Engage customers in more extensive and creative ways through dialog, recognizing they may find it challenging to articulate their needs in the complicated information arena, and they may need explanation of the program’s

capabilities and limitations.

- Conduct discussions of key issues that need decisions by bringing in differing viewpoints, encouraging spirited, constructive debate, and respecting dissenting opinions. Staff and customers are key participants, but involving other areas, such as IT, counsel, and media, may bring in fresh perspectives.
- Keep goals in mind, but encourage discussion of new ways of reaching them. *Judgment Calls* describes this as “following a strong compass but often in unpredictable and even nonlinear ways.”

6. Monitor and Adapt CIOs’ Strategies.

RIM programs are not alone in gearing up for the volatile post-recession, information-centric world. They can learn from others who are being buffeted by the winds of change, especially chief information officers (CIOs). There is a natural connection – some RIM programs

are in CIOs' offices, and many work with CIOs on a daily basis. Some CIO strategies are worthy of emulation, such as visibly supporting enterprise goals, demonstrating value at the CEO level where it may be under-appreciated, and cooperating with other offices in pushing their companies into new customer, product, and service areas.

CIO magazine's 2013 "State of the CIO Survey" highlights the need to align with enterprise goals, market the IT department to give the businesses a better idea of its capabilities, and position the office as a business peer that develops, not just enables, business strategy.

This entails pushing the program into new areas with new partnerships in support of evolving enterprise priorities. Gartner's "2013 CIO Agenda" notes that "IT must adapt by extending its role in the enterprise ... hunt for new digital business opportunities, and harvest value from business process changes and extended products/services." Likewise, RIM programs must hunt for new opportunities.

Stepping up to the Challenge

RIM programs are well positioned to capitalize on the growing importance of digital information in business, education, government, and the lives of individuals. They have strong capabilities in issues that are increasing in importance, such as retention and disposition of records, legal applications, risk management, and privacy.

But RIM programs should expect – and welcome – change, sometimes gradual and incremental and other times rapid and transformational. Leading that change in a positive way is one of the greatest challenges – and opportunities – we face. **END**

Bruce W. Dearstyne, Ph.D., can be contacted at dearstyne@verizon.net. See his bio on page 47.

Recent Useful Leadership Books

Amabile, Teresa and Steven Kramer. ***The Progress Principle: Using Small Wins to Ignite Joy, Engagement, and Creativity at Work.*** Boston: Harvard Business School Publishing, 2011.

Baldoni, John. ***Lead With Purpose: Giving Your Organization a Reason to Believe in Itself.*** New York: Amacom, 2012.

Andersen, Erika. ***Leading So People Will Follow.*** Hoboken, NJ: John Wiley & Sons, 2012.

Collins, Jim and Morten T. Hansen. ***Great by Choice: Uncertainty, Chaos, and Luck – Why Some Thrive Despite Them All.*** New York: Harper-Collins Publishers, 2011.

Davenport, Tom and Brook Manville. ***Judgment Calls: 12 Stories of Big Decisions and the Teams That Got Them Right.*** Boston: Harvard Business School Publishing, 2012.

Duggan, William. ***Creative Strategy: A Guide for Innovation.*** New York: Columbia University Press, 2013.

Gostick, Adrian and Chester Elton. ***All In: How The Best Managers Create a Culture of Belief and Drive Big Results.*** New York: Free Press, 2012.

Lafley, A.G. and Roger L. Martin. ***Playing to Win: How Strategy Really Works.*** Boston: Harvard Business School Publishing, 2013.

Mellon, Liz. ***Inside the Leader's Mind: Five Ways to Think Like a Leader.*** Harlow, UK: Pearson Education Limited, 2011.

Menkes, Justin. ***Better Under Pressure: How Great Leaders Bring Out the Best in Themselves and Others.*** Boston: Harvard Business School Publishing, 2011.

Ries, Eric. ***The Lean Startup: How Today's Entrepreneurs Use Continuous Innovation to Create Radically Successful Businesses.*** New York: Crown Publishing Group, 2011.

Sims, Peter. ***Little Bets: How Breakthrough Ideas Emerge from Small Discoveries.*** New York: Free Press, 2011.

Zolli, Andrew and Ann Marie Healy. ***Resilience: Why Things Bounce Back.*** New York: Free Press, 2012.



The Only **3 Letters** That Matter

If you're ready to take your career in records management to the next level, there are only 3 letters that matter. Becoming a **Certified Records Manager** shows that you're ready for today's complex and changing information environment.

Stand Out The CRM designation shows a solid mastery of records management

Confidence You'll prove your ability to apply records and information management knowledge

Career Opportunities It's the well-known competitive advantage you need in business today

For more information, call **877.244.3128**
or visit **www.ICRM.org**



USING DATA PROFILING TO MITIGATE 7 'RED FLAG' INFORMATION RISKS



Data profiling technology can help an organization identify what electronic information it has and where it is located, which is the first step to ensuring that information governance policies are applied to it, reducing the organization's costs and mitigating its seven greatest information risks.

Jim McGann

Today's records and information management (RIM) professionals are tasked with mitigating the risks that come along with ever-changing regulations and escalating threats to information security, all while controlling exponentially growing data costs.

More like detectives than RIM professionals, they are charged with uncovering sensitive records, such as Out-

look personal storage table (PST) e-mail archives and aged e-mails created by former employees, unencrypted files containing personally identifiable information (PII), and copies of contracts and research data lost within network file shares.

But before they can find and manage this data, they must determine what information exists across the enter-

prise, where it exists, and who created it. To address the risks that come with not knowing this, some RIM professionals are using data profiling.

Data Profiling Defined

Data profiling examines data from all sources and collects metadata-level information on the content to create a searchable and reportable repository about the information, identifying such things as the information's owner, age, type of file, location, date last accessed or modified, and whether it is a duplicate.

Data profiling allows RIM professionals to create a map of what data exists and where, so they can actively enforce and audit compliance with the information governance policies that dictate the use, disposition, retention, and management of corporate data, protect the firm's assets, and manage long-term risk.

This helps organizations control costs and risks, as well as address the seven greatest issues – red flags – that have a critical impact on their electronic records systems today: PII, hidden PSTs, user shares, departmental servers, legacy backup tapes, aged data, and large multimedia files.

The Information Governance Landscape

The volume of information is exploding. More and more business information is digitized, and users create data 24/7 as they carry their office in their pockets. It is estimated that data growth is reaching unprecedented levels, with Gartner stating in its June 2012 research report "Organizational Collaboration and the Right Retention Policies Can Minimize Archived Data and Storage Demands" that the volume is growing 40% to 60% annually. The numbers are nearly impossible to comprehend and rising each year. Technology teams are keeping up with this data growth by increasing storage capacity.

The data environment also has become more complex; for example, copies of user content are typically replicated and archived many times to ensure it is never lost, leaving records managers with multiple versions of the same mess to clean up.

Archives that were created to store specific important data, such as content preserved for legal holds and documents required for compliance, have become bloated unstructured repositories where other data is put in and never seen again. Highly sensitive information becomes lost in the shuffle and largely unmanageable.

The Legal, Regulatory Climate

Over the past decade, e-discovery has provided an expensive learning lesson for some organizations. They have spent significant time and resources identifying sensitive user data and collecting it to support active litigation. It is not unusual for a single litigation to cost hundreds of thou-

sands or even millions of dollars. The Searle Civil Justice Institute's 2010 "Litigation Cost Survey of Major Companies" found that for the period 2006-2008, the average *Fortune* 200 company that responded to the survey paid average discovery costs of \$621,880 to \$2,993,567 per case.

Ten years ago, it was fairly easy to claim that specific content was not easily found within the complex corporate infrastructure and, therefore, it was "inaccessible," or it placed an "undue burden" on the party being asked to produce it for litigation. Today, this argument is less successfully used.

Judges, opposing counsel, and expert witnesses have all been educated on and have a better understanding of the corporate data environment. Today, it is a high-risk proposition to enter a court without the requested data, as there is a good chance for the judge to admonish or even issue fines and sanctions for not producing it.

Data profiling examines data from all sources and collects metadata-level information on the content

Beyond the growing demand to produce information for e-discovery, compliance and regulatory requirements have been increasing, resulting in renewed emphasis on RIM strategies. These growing and evolving regulations – such as requirements to encrypt sensitive records or archive specific classes of correspondence – require significant updates to corporate policies and new strategies for data managers.

As a result of these issues, organizations are taking a fresh look at policies and implementing information governance strategies, such as using data profiling, that are aimed at protecting them from risk and liability by providing them knowledge they need to make proper decisions.

Data Profiling and Policy

Corporate data policies are complex. For many organizations, the complexity stems from their attempts to define policies without having adequate knowledge about what data exists. Policies are created, but they can't be enforced or monitored.

By default, then, many organizations are leaving it up to end users to implement the policies. But users tend to neglect making decisions about data, opting to keep it forever "just in case" they might need it. Very few know such things as how PST files are made, where they go, or what the consequences of sending a client's credit card number through an e-mail could be.

Along the way, needed information gets lost in the shuffle. Over time, research and intellectual property data ages and becomes difficult to leverage. This hidden data, which has value but cannot be found within the infrastructure, is not tapped to help support current users.

As knowledge workers leave the organization, their data typically remains scattered about the network infrastructure. Since the owner is no longer around to manage this content, it quickly gets lost; current users don't even know it exists.

Data profiling helps both sides of the information quandary. Using it, content can be searched, found, and leveraged to support business needs, and it can be purged, encrypted, or secured to mitigate risks.

... personal media files have no business value but are being managed and backed up daily

The 7 Red Flags

The profiling process begins by becoming aware of the greatest threats to data breaches, compliance issues, and bloated storage budgets. As described below, these seven red flags will have the most immediate and critical impact on an organization's management of electronic records.

1 PII

PII includes credit card and Social Security numbers that, if lost, could put customers at risk. Organizations usually have privacy policies that prohibit sending PII through e-mail and mandate the encrypting of all files containing PII, but that doesn't mean they are being followed. Organizations are responsible for safeguarding this information, and any violations – such as of the requirements of the U.S. Health Insurance Portability and Accountability Act or the Fair and Accurate Credit Transactions Act – make them financially and legally liable.

2 Hidden PSTs

Microsoft Outlook allows users to create PSTs and store messages, contacts, appointments, and other information on their hard drives or a network server. PSTs, much like PII, usually have a policy surrounding them that isn't readily enacted or enforced. The truth is, most non-IT personnel probably don't know what PSTs are, let alone that they are creating them. Managing PSTs can be challenging; even from an IT standpoint, finding PSTs is difficult. Legal and

compliance teams are often surprised to find this hidden e-mail during high-profile litigation. Auditing for PSTs helps legal teams evaluate these highly sensitive e-mail archives and determine disposition.

3 User Shares

Organizations typically set up network shares where users can store files and other content. These shares often grow to the point where managing the content is impossible. With data profiling, this mystery content can be analyzed and an action plan defined. For example, data profiling can find all data that has not been accessed for a specific length of time, allowing it to be moved off this environment or even purged if it has no business value.

4 Departmental Servers

Profiling the content on shared servers and desktops within a network that was created by a department that frequently works with valuable content, such as intellectual property, consumer information, or research data, is a logical place to begin. This will provide the knowledge required to determine its disposition; much of the data may be archived for long-term retention or secured to protect sensitive intellectual property.

5 Legacy Backup Tapes

Backup tapes contain copies of all existing user files and e-mails amassed over time. In the past, these were often considered burdensome to access, so courts did not always demand for it to be produced for litigation. However, technology now makes this content reasonably accessible and, thus, a corporate liability if not managed according to policy. Organizations are now cleaning up this content based on a data profile and preserving only what has value.

6 Aged Data

Profiling aged data – that which is more than seven years old and has not been accessed for a long period – will reveal what and where it is, allowing it to be moved to less expensive storage platforms, migrated to the cloud, archived with related documents, or purged if its retention is no longer required.

7 Large Multimedia Files

Chances are that audio, video, and photo files are not putting organizations in legal jeopardy unless there is a possibility of copyright infringement, but they could be affecting storage budgets. User shares likely are packed with personal files from employees watching movies or searching through vacation albums during breaks or downloading music libraries to listen to while working. These personal media files have no business value but are being managed and backed up daily. Locating them enables organizations to audit how

much space these files are using, purge them from storage, and develop policies governing the use of company resources to play or view and store them.

Data Profiling and Disposition

Data profiling helps organizations understand and manage the needs of their information governance policies by ensuring the policies are followed with the proper action and data dispositions. It finds the red flags before breaches or litigation can. It often prevents problems and saves valuable storage costs.

Data profiling is one of the best resources that RIM professionals have to support information governance policies. It provides a deeper understanding of assets and is the key to being able to control risk and liability. Without a data

profile, it's nearly impossible to manage mystery content and enforce policy.

Common dispositions include moving essential content to an archive, preserving data for legal holds, removing duplicate content, encrypting sensitive data, migrating to less expensive storage, and purging data that has no business value.

No longer should data remain on networks unmonitored and unmanaged with uncontrolled growth. Using policy as the foundation and data profiling as the support, organizations can leverage and manage data more effectively. **END**

Jim McGann can be reached at Jim.McGann@Index-Engines.com. See his bio on page 47.

Studying for the CRM?

ARMA International's CRM Study Packs

ARMA International has created specially priced packages of recommended resources to help you study for the **Certified Records Manager (CRM)** exam.

Available Study Packs:

- **Part 1: Management Principles and the Records and Information Management Program**
- **Part 2: Records and Information: Creation and Use**
- **Part 3: Records Systems, Storage, and Retrieval**
- **Part 4: Records Appraisal, Retention, Protection, and Disposition**
- **Part 5: Technology**
- **CRM Mega-Pack (combined version of all CRM Study Packs)**

CRM candidates (or potential candidates) should also consider enrolling in ARMA International's online **Essentials of RIM Certificate Program**; completing this program will help establish a great foundation for passing parts 1-5.

Get details at www.arma.org/learningcenter.

Available online in the ARMA Bookstore!

BOOKSTORE ARMA INTERNATIONAL
www.arma.org



The Principles Assessment as a Collaborative Tool

Julie Gable, CRM, CDIA, FAI

John Isaza, Esq., FAI – a 24-year veteran attorney with a dozen years of records and information management (RIM) experience who works for international law firm Rimón PC – regularly uses the Generally Accepted Recordkeeping Principles® (the Principles) and the Information Governance Maturity Model (Maturity Model) in his work for clients. (See www.arma.org/principles for more information about the Principles.)

The majority of his time, about 65%, is spent doing compliance assessments and audits of existing programs, and the rest is devoted to formulating new RIM and/or information governance programs.

One of Isaza's main tools for accomplishing this work has been ARMA International's automated Principles Assessment tool. His first-hand experience has yielded several insights on how to use this tool most effectively in real-world environments and provides many lessons learned that will be useful for RIM practitioners.

Conducting the Assessment

The Principles Assessment is a computer-based tool that provides an automated way to determine how an entity's information management practices measure up against the Maturity Model.

The tool requires answers to 100 questions related to the eight principles: accountability, transparency, integrity, protection, compliance, availability, retention, and disposition. By selecting the answer that most closely



matches the current situation, the Principles Assessment will calculate a score for each principle. The scores correlate to levels ranging from 1 to 5, with 1 being substandard and 5 being considered transformational. The Principles Assessment can be used for a single department, a division, or the entire organization.

As with all tools, there are tips and techniques that can enhance the usefulness of the assessment. Isaza's solid consulting experience has yielded several pointers that he generously shares here.

Involve Others

"Don't just do it all yourself," cautions Isaza. In situations where the records manager performs the entire assessment, there is the risk of rating too high or too low on various program aspects, and the outcome will be subjective and, therefore, less credible. Isaza advises that the best way to ensure objectivity is to get responses from others in the organization. How to do this can be challenging, though.

"Don't think that you can just send the tool to everyone in the firm and have them answer questions on their

own,” advises Isaza. Many questions seem to be redundant from one principle to the next, but they actually have a different context and may need clarification for those who are not involved with RIM as their primary responsibility. “What’s more,” says Isaza, “Each question must be answered before going on to the next, and people will not necessarily be able or willing to do this.”

Use Facilitated Workshops

Isaza has found that workshops can be an ideal setting for a collaborative use of the Principles Assessment, and his experience with four clients in diverse industries – automotive, non-profit, insurance, and financial services – has proven that this approach works.

A workshop is a way to gather several people in a single place and poll them for their opinions and perceptions of RIM. The workshop setting also offers a relaxed atmosphere where discussion and informal RIM education can take place.

Preparing – Advance preparation is key, however. Isaza notes, “If you choose a workshop setting, recognize that you will need to do some preparation. First, and most importantly, you will need to have someone with RIM knowledge in the room to help with explanations where needed.”

According to Isaza, it is unrealistic to expect to get through the tool’s 100 questions in a workshop lasting an hour and a half. The best practice is for the RIM manager to spend time analyzing which questions should be presented to the workshop group and which can best be answered in advance. Given the limited time available for most workshop participants, it pays to select the questions that deliver the biggest return. Isaza also notes that some questions and proposed responses may profit from being simplified for better understanding.

“Using the tool in real time before a live workshop audience can also be

John Isaza: A Career Overview



John Isaza, Esq., FAI, is a leader in Rimon PC’s Corporate Governance and Records and Information Management practice areas. Rimon is an international law firm with offices in the United States and Israel. The firm’s name is the Hebrew, Arabic, and Aramaic word for pomegranate, a traditional symbol of excellence, community, and innovation, the firm’s three core values.

A lawyer for 24 years, Isaza has been in the records and information management (RIM) field since 2001, and his prior experience in litigation, corporate law, and investment banking serves him well in his current position. His work has included engagements in oil and gas, financial services, government, technology, insurance, food, entertainment, manufacturing, automotive, and legal services sectors. In addition to his law degree, Isaza holds a real estate license and several securities industry licenses.

challenging because of slow response time in some environments,” says Isaza. Providing the selected questions on PowerPoint or by other means may make for a smoother, more productive experience in a live setting.

Scoring – Each workshop participant chooses a response for each question. The results are averaged to arrive at a score (from 1 to 5) for how the organization is doing in that particular principle. For example, if 10 workshop participants choose answers to questions about the Principle of Availability that range from level 2 to level 4, the average might be a level 3 for that principle. There may be multiple workshops with different participants in each, depending on the size of the organization.

In addition, Isaza and the records manager each completes his or her own scoring. Isaza then averages his rating and the records manager’s, using this as an additional workshop session. To arrive at the overall rating, Isaza’s methodology is to average the scores from each workshop for each category. He notes that comments are captured during the process and that he supplements the workshops with some individual interviews as well.

Balance Effort with Need

Concerns about accuracy need to be balanced with practical considerations. Approaching an assessment as

an audit can be cost prohibitive, advises Isaza. Asking to see documentary evidence for every aspect of each principle generally puts a strain on organization resources and may not necessarily yield better data than the multiple opinions available in the workshop setting.

Another consideration is to recognize that the degree of rating accuracy in a collaborative setting will probably be just fine for the purpose of the assessment. Attempting to get very scientific or statistical with the ratings can also be expensive and more than is actually needed for the organization’s purpose.

Using the Results

The assessment scores provide a way for those at all levels of the organization to understand how the firm is doing in regard to information management. Many times Isaza is dealing with chief executive officers and director-level management. Assessment results are often delivered with a supplemental report identifying major technology, people, policy, and risk considerations based on the assessment outcome and observations.

Set Metrics

“One of the most useful outcomes of the Principles Assessment and the Maturity Model is the ability to set baseline metrics that can be tracked

“For many organizations, scores increase dramatically by increasing the role of RIM in decision making and improving communication between departments.”

over time. These become something that the organization can use to gauge improvement, to base future audits on, and most importantly, to communicate to the C-level suite what the folks in information management are doing,” says Isaza.

Furthermore, Isaza notes, “If you overlay the factors significant to a particular industry, you can put together a roadmap for future activity and set priorities that make sense for that organization within that industry.”

Plan, Prioritize Activities

For example, one of Isaza’s financial services clients had completely acceptable ratings in the areas of integrity, protection, and compliance, but recognized the importance of these principles given the increasing regulation, the growing amount of personal information associated with its work, and the reputation risk associated with its industry. Even with acceptable scores, this client sought recommendations that would take the organization to higher levels of maturity in these areas.

In another example, the law department of a national non-profit, already aware of certain challenges with availability, retention, and disposition within the department, was able to identify and prioritize areas for improvement and to take positive steps that would boost scores almost immediately. For this client, immediate steps included hiring a records manager, revising old retention schedules,

and putting technology in place to foster secure storage, collaboration, remote access, and other Principles-guided capabilities.

Benchmark Against Others

Within the corporate world, there are ways to judge one organization’s performance against that of others in the same industry segment. Financial ratios, for example, measure such things as an organization’s ability to meet its short-term debt or its overall effectiveness based on the returns generated on sales and investment. Financial analysts expect to see such ratios fall within a certain range for segments such as manufacturing or retail.

Although there are no such industry benchmarks for information management, consultants are often knowledgeable about what similar firms in a given industry have done regarding information management. In the absence of industry metrics, they can be a source of general guidance regarding what project priorities should be in terms of a Principles-based action plan.

In addition, consultants often have access to multiple layers of management and can be useful in raising awareness at the highest levels of the firm. While consultants will not divulge the names of their clients or provide specific details of any client’s program, they can provide a general idea of how your organization compares to others.

Increasing the Score

“For many organizations, scores increase dramatically by increasing the role of RIM in decision making and improving communication between departments,” Isaza says. “For example, information technology (IT) may rate itself a 5 in one aspect, but the law department may rate IT only a 2, simply because IT has not communicated the steps it has taken to ensure a higher level of maturity.”

Another item that can immediately boost scores, says Isaza, is the establishment of an information governance committee as a way to increase senior management sponsorship and communications.

“On the other hand, clients are sometimes surprised at the number of things they hadn’t thought of. Folks in IT may not be as aware of the principles of retention and disposition because they are in charge of transporting data, he notes. “Sometimes they are surprised at how much there is in terms of specific rules and laws.”

Assessing Your Organization

Used in a workshop setting, the Principles Assessment tool can be an excellent way to focus attention, guide understanding of the Maturity Model, and produce a credible picture of an organization’s information management practices. The workshop itself is an opportunity to raise RIM awareness and provide education on the foundations of a standards-driven RIM program. The facilitated workshop is also an excellent way to cross organization lines and to begin taking a cross-disciplinary, collaborative approach to managing contemporary information issues and concerns. It’s definitely worth a try. **END**

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

**NAID**

NAID is the non-profit trade association for the secure destruction industry, which currently represents more than 1,900 member locations

globally. NAID's mission is to promote the proper destruction of discarded information through education, the NAID 'em initiative, and encouraging the outsourcing of destruction needs to qualified contractors, including those that are NAID-certified.

www.naidonline.org

Downstream Data Coverage

Downstream Data Coverage offers professional liability coverage that specifically addresses the risks associated with NAID-certified companies that provide data-related services. Call **877.710.2498** to learn more.



XACT DATA DISCOVERY
Because you need to know

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



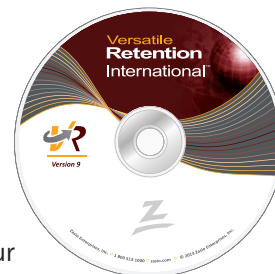
RSD recently announced IGaaS™, or Information Governance as a Service. Whether governing information stored on premise or within the cloud, IGaaS™ provides all services for in-place information governance including: policy definition, information classification, policy enforcement, information access, life-cycle management, audit, and compliance. For more information, please watch our complimentary on-demand webinar "The Future of Information Governance is Here: IG as a Service" at **www.rsd.com/webinar-igaas**.

**ZASIO**

Records Management Software and Consulting Services

Zasio's powerful suite of intuitive records management software lets you effectively manage both your physical and electronic records, regardless of where they are located—on-site and/or off-site. Whatever the size of your organization or the scope of your records management needs, Zasio has the solution.

To choose the right solution for you, visit our website and download the Versatile™ Selector Guide! **www.zasio.com**.

**DHS**

DHS Worldwide Software Solutions recently held its 2013 Total Recall User Conference in San Antonio, Texas, with nearly 50 in attendance. During the conference, DHS announced exciting news and innovative developments, including a completely redesigned and responsive company website. For more information please visit **www.dhsworldwide.com**.

A 5-Step Strategy for Harnessing Global Information Growth

Brian Nowak



Our global records management and compliance department faced a huge challenge: handling the explosive growth in information being received from businesses located around the world – the result of both organic and inorganic growth due to the acquisition of a complementary financial entity. We realized the company needed a global approach to records management; playing its traditional role, our records management team simply could not support the needs of our growing global company.

In transforming our team from that traditional to a more strategic role, we established objectives, took actions, and learned lessons that should be of value to other organizations struggling to harness the ever-widening pools of information they

must manage efficiently in their daily course of business.

Program Assessment

First, we took a critical look at our current processes and the future of information management. We found that our global records management team was primarily focused on the transactional elements of records management, such as preparing items for offsite storage, reacting to internal business units' needs, and responding to crisis requests.

These were all complicated by the wide variation in the level of records management sophistication among lines of business and locations in various countries, and dealing with these tasks left very little time to prepare for exponential information growth or to coordinate our efforts globally. We de-

termined that to provide much greater value to the company, we needed to shift our records management team's focus from transactional to the strategic components of information management.

Strategic Objectives

We focused on five strategic actions to harness, use, and control information:

1. Consolidating retention schedules throughout our worldwide operations
2. Establishing processes and methods for universal information subject categorization and indexing
3. Aligning access to and management of both paper-based and electronic information
4. Creating processes to continuously solicit stakeholder feedback regard-

ing information management, including from within the institution, operational lines of business, regions and country management, legal, audit, and other corporate functions

5. Establishing a truly global information management strategy

Action Steps

Because of our growth, there was a widespread realization that we needed a more comprehensive way to manage information, and our internal environment was primed for change. That made it easier to “sell” the need to change our team’s approach from task-oriented to strategic.

any, concerns about their “turf.”

These liaisons played a pivotal role in executing our new global records management strategy. They knew their operations intricately and were better suited to manage the daily records management tasks, such as contracting with local service providers who could dovetail services to satisfy our global information and records management strategic goals.

Ultimately, the liaisons took on additional responsibility for records management, and in a number of cases, they had notable expansions of responsibilities. For example, the role of a liaison in the UK who was very effective in watching over and caring

complying with myriad regulations worldwide.

3. Establish Corporate Department Liaisons.

We also needed to establish additional relationships in functional departments, such as legal, audit, compliance and IT – all corporate functions with operations in the lines of business and regions. Like in the lines of businesses, personnel in these functions shared the realization that something needed to be done to handle and manage information for our expanded and growing business; each had a vested interest in doing so.

Because of our growth, there was a widespread realization that we needed a more comprehensive way to manage information ...

There were certainly growing pains along the way, but we began to transform ourselves into internal consultants by taking the following five steps.

1. Establish Line of Business Liaisons.

The first step in becoming more strategic and consultative was to establish liaisons from each of our eight lines of business that were headquartered throughout the world with subsets at the regional and, in some cases, country levels.

Our department had established good relationships with these lines of business, which helped pave the way for our successful outreach to them. Our conversations and presentations about the importance of managing, using, and retaining information for business efficiency, productivity, and regulatory compliance, coupled with what lines of business owners and regional management already knew about their needs convinced them to assign their employees to liaison roles.

After the first line of business came on board, the others followed suit in rapid succession with minimal, if

for records was expanded to provide expertise throughout our European region.

2. Provide Education and Support.

With the liaisons’ relieving the global records management team from transactional responsibilities, the team had time to consult and educate the lines of business and regions about more strategic things, such as retention schedules, privacy, and compliance.

We structured our robust educational sessions through individual meetings, “lunch and learns” for larger groups, and telephone conferences for folks in regions outside the United States. We also supported the liaisons with project management and direction.

With these liaisons in place, our global records management team now could concentrate its focus on strategic projects designed to integrate globally sourced information into a cohesive resource, transforming our records management function into one that could accommodate and sustain our growing worldwide business while

4. Partner to Develop the Strategic Plan.

The functional department liaisons became strategic partners in the development of the global records management strategy; their input and involvement were critical in making it successful. They welcomed a collaborative approach to determining how to manage information on a global basis. They knew the importance of doing so and appreciated the opportunity to help establish the processes.

Each member brought a unique perspective, which we debated until reaching agreement about our global strategic direction. As an example, we identified and discussed the issues related to electronic records management, which previously had been considered the IT department’s concern.

With the rapid expansion of the business, IT had an immediate and pressing issue: how to manage – especially for retention and regulatory compliance – tens of thousands of e-mails generated and received worldwide every day. IT needed help and welcomed the opportunity to have

input into the strategy and tactics to carry it out.

Previously, the company did not have a forum for lines of business and functional departments to express ideas and concerns related to information management. This new forum allowed the team to work together to establish the priorities for the global strategy.

5. Take the Lead.

Although it was broadly acknowledged that we needed to get a handle on our global information growth to

giving the lines of business and functional departments the opportunity to participate in the development of the strategy created buy-in. No one likes a mandate from corporate!

2. Establishing a global strategy doesn't mean everything is done in one manner.

This was particularly evident as we expanded beyond the U.S. borders. This concept goes beyond simply accommodating differences in culture, language, and country records retention laws.

subject matter experts in information management, became a more valued resource to the company, and developed stronger working relationships.

4. Change is not easy.

We had numerous growing pains during the transformation, some of which affected members of our staff. Transforming our organization to meet ever-growing global responsibilities represented a sea change for our team as it became more strategic and shifted tactical processes to the lines of business.

... the results of our efforts improved dramatically as we brought the lines of business and functional departments into the process.

be effective, no single functional department took the lead in addressing this concern. This created a leadership void into which the global records management team gladly jumped! With our former transactional responsibilities managed by the liaisons, our team was able to accept the responsibility for managing the project and completing its priorities.

Lessons Learned

The transformation process that allowed us to accomplish our global record management strategy required hard work and perseverance and generated a number of take-aways and lessons learned:

1. A group decision will take longer, but the results will be better.

There was a temptation to believe that we had all the answers and didn't need input from others. But, the results of our efforts improved dramatically as we brought the lines of business and functional departments into the process.

Not only were the decisions better, but the scope of records management expanded to information management, taking into account all information. Even more important,

One of our initial strategies was to use one global records management provider in all the countries where we were operating. The provider was the incumbent in the United States, and we were under the impression that it was positioned to meet our global needs. Some of the benefits we expected included global access to our information, singular account management, consistent operating procedures, and reduced expenses.

However, as we tried to mandate this approach with our regions and countries, we found the provider didn't have the ability to service some countries, as we had expected. We ultimately adopted an approach that involved a global strategy in terms of managing and maintaining information, but provided local flexibility to make decisions on things like choosing the optimal provider for that location.

3. You must be willing to step up and take the lead.

As we met with the lines of business and functional departments, it became very apparent that our role would expand if we were willing to take the lead on the various priorities. By taking the lead, we assumed much more enriching and strategic job responsibilities, showed ourselves as the

Some team members were more comfortable with the transactional tasks of records management, so we helped place them in new roles that more closely matched their interests. The majority, however, embraced and thrived in an environment that included challenging work assignments and interaction with all levels of employees across many countries.

The Bottom Line

The transformation of our global records management team involved hard work and dedication. Our team members took a critical look at our current organization and responsibilities and realized we were not prepared for the information explosion that had become part of the company's daily operations. We created partnerships with internal stakeholders, taking advantage of their collective thoughts and considering their needs. Through the efforts of the entire team, we created a global records management team that has enriched job responsibilities and adds true value to the organization. **END**

Brian Nowak can be contacted at brian.nowak@rhinodox.com. See his bio on page 47.

Addressing Security Concerns: The Expanding Role of Information Governance

Andrew Altepeter

Over the past decade, cyber security has become a major concern in the public consciousness. From WikiLeaks, to state-sponsored attempts to steal valuable intellectual property, to highly publicized retail companies' credit card breaches, information professionals face a constant barrage of threats to their organizations' information.

These threats erode an organization's ability to prosper and threaten American competitiveness as a whole. While traditionally, information professionals have focused on helping the organization meet legal, regulatory, and business requirements, the equally pressing concern of securing information assets provides them new opportunities.

Protecting these assets are not only the responsibilities of the firewall administrators, network architects, and others who sit in IT. In his book *Safeguarding Critical E-Documents: Implementing a Program for Securing Confidential Information Assets*, Robert F. Smallwood argues an important piece of this strategy must be information governance.

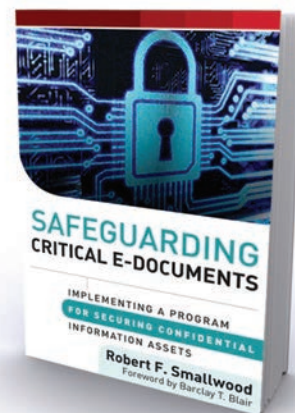
While acknowledging that there are several competing definitions of *information governance*, Smallwood characterizes it as an interdisciplinary subset of corporate governance: the melding of records management, IT governance, e-discovery, business continuity, disaster recovery, information security, and privacy. Its ultimate aims are to manage and control the output of IT through policies and tools that control access to and use of information.

Although Smallwood is not the first to use this definition of information governance, it is a relatively new approach that greatly expands the scope of what until quite recently has been a field primarily rooted in the disciplines of records management and e-discovery.

Smallwood's book is divided into five parts. He first outlines the major security problems and risks organizations face and introduces basic information governance principles. In Part II he describes the risks and countermeasures that can be taken for specific platforms, such as unstructured content, e-mail, instant messaging, social media, mobile devices, and cloud computing. Part III is devoted solely to e-records management issues, specifically defining and protecting vital records and long-term preservation of electronic records. Part IV introduces technologies that can help protect information assets, such as encryption, digital signatures, data loss prevention tools, and information rights management. The final part of the book provides strategies for obtaining executive sponsorship, managing projects, and selecting vendors.

Readers will find helpful the concrete steps the book gives for rolling out and maintaining a secure environment for information assets. Each chapter has text boxes that outline key points and chapter summaries that reinforce the main takeaways.

Non-technical readers will find Smallwood's descriptions of information governance technology tools easy to understand. Appendices give stan-



Safeguarding Critical E-Documents: Implementing a Program for Securing Confidential Information Assets

Author: Robert F. Smallwood

Publisher: John Wiley & Sons

Publication Date: 2012

Length: 263 pages

Price: \$75

ISBN-13: 978-1-118-15908-8

Source: www.arma.org/bookstore

dards for digital signatures, regulations for records management, and lists of technology and service providers. Chapter endnotes provide readers with additional resources.

In total, Smallwood's book gives readers a solid foundation for making informed governance decisions and presenting them in a way that upper management will find appealing.

The book would be strengthened by a more robust discussion of the "low-tech" ways organizations can help secure their environment, such as employee training, awareness presentations, newsletters, portal messaging, and office posters; these are all important pieces of an information protection program.

The book also largely neglects the most common entryways of data breaches, such as phishing and social engineering scams, although Smallwood does devote some discussion to insider threats, such as careless or malicious employees. Nevertheless, more emphasis should be given to the fact that while technology is necessary to secure information, employee vigilance is the first step.

Despite these omissions, *Safe-*

guarding Critical E-Documents is an important call to arms for information professionals. To stay relevant, the profession must expand beyond the established business justifications of improved efficiency, regulatory compliance, and legal retention requirements. Protecting information from security threats is a way to add significant value to the organization by addressing a concern that is on the mind of every executive in the country.

For American businesses to stay competitive with the rest of the world, organizations must continually be vigilant in protecting their information assets. Proper information governance policy and controls are important elements in any security strategy. **END**

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



Learning Center



Like Your Favorite Drive Thru ... Only Better.

Who has time between 9 to 5 to slip away for career development?

Us either.

ARMA International's online courses offer convenient and flexible training on YOUR schedule. From RIM and Generally Accepted Recordkeeping Principles® to professional development, our online courses allow you to keep on top of your game and get ahead of the field, at a time and place that is most convenient for you.

Slippers optional.

Open 24 hours a day, 7 days a week, 365 days a year.

See what's available at www.arma.org



Altepeter



Dearstyne



Gable



McGann



Nowak



Phillips

Clearing the Hurdles of International Technology Implementations page 22

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

Accelerating out of the Recession: New Approaches to Executing RIM Program Strategies page 27

Bruce W. Dearstyne, Ph.D., has more than 30 years of experience as a practitioner, professor, and consultant in records, archives, and related information work. He is the author of numerous articles and several books, including *Managing Records and Information Programs*, published by ARMA International. He can be contacted at dearstyne@verizon.net.

Using Data Profiling to Mitigate 7 'Red Flag' Information Risks page 34

Jim McGann is vice president, Index Engines. He has extensive experience with e-discovery and information management in the *Fortune* 2000 sector. McGann is a frequent writer and speaker on the topics of big data, backup tape remediation, electronic discovery, and records management. He can be reached at Jim.McGann@IndexEngines.com.

The Generally Accepted Recordkeeping Principles® Series: The Principles Assessment as a Collaborative Tool page 38

Julie Gable, CRM, CDIA, FAI, is president and founder of Gable Consulting LLC. She has more than 25 years of experience specializing in strategic planning for electronic records management, including business case development, cost-benefit analysis, requirements definition, and work plan prioritization. In 2003, she was named a Fellow of ARMA International. Gable has authored numerous articles and frequently speaks at national and international conferences. She holds a master's degree in finance from St. Joseph's University and a bachelor's degree in management from Drexel University. Gable can be contacted at juliegable@verizon.net.

RIM Fundamentals Series: A 5-Step Strategy for Harnessing Global Information Growth page 42

Brian Nowak is general manager for RhinoDox, a data management and archival supplier for companies and government organizations of all sizes. He has more than 10 years of experience as an information management solutions provider and practitioner. Nowak can be contacted at brian.nowak@rhinodox.com.

Addressing Security Concerns: The Expanding Role of Information Governance page 45

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

Reach Your Target: Information Management Decision Makers and Influencers



There's only one source
you can count on
to give you the impact
you want:

ARMA INTERNATIONAL'S
**INFORMATION
MANAGEMENT
MAGAZINE**

Karen Lind Russell/Krista Markley
Account Management Team
+1 888.277.5838
Karen.Krista@armaintl.org

AD INDEX Contact Information

- 15, 17 **Access Sciences**
800.242.2005 – Intl. 904.213.0448 –
www.accesssciences.com/SharePoint
- 13 **DHS Worldwide Software**
800.377.8406 – Intl. 904.213.0448 –
www.dhsworldwide.com
- 3 **Downstream Data Coverage**
www.downstreamdata.com
- 33 **Institute of Certified Records Managers**
877.244.3128 – www.ICRM.org
- BC **Iron Mountain**
www.ironmountain.com/advantage
- 19 **NAID**
www.naid-em.com
- 29 **Paralegal Today**
877.202.5196 – www.paralegaltoday.com
- IBC **Recall**
888.RECALL6 – www.recall.com
- IFC **RSD**
www.rsd.com
- 5 **Xact Data Discovery**
877.545.XACT – www.xactdatadiscovery.com
- 9 **Zasio Enterprises Inc.**
800.513.1000 Opt. 1 – www.zasio.com





Thinking about advancing your career?

ARMA International's CareerLink has helped hundreds of members find new and exciting positions in the information management profession.

The Job Board lists current openings from companies around the globe. You can find valuable resources and tools to help your career evolve.

Create your confidential profile and get started today at www.arma.org/careers.

recall™

Your Information. Securely Managed.

www.recall.com | 1-888-RECALL6

INFORMATION GOVERNANCE

Use Data Strategically

DATA PROTECTION

Guarantee Business Continuity

SECURE DESTRUCTION

Mitigate Risks

DOCUMENT STORAGE

Ensure Compliance

DIGITAL SOLUTIONS

Improve Workflow



STEP AHEAD WITH A NEW GENERATION
OF INFORMATION MANAGEMENT





EMPLOYEES WASTE VALUABLE HOURS EACH WEEK CHASING HARDCOPY DOCUMENTS.

(SOMETIMES, THEY EVEN FIND THEM.)

Companies today are trying to find new ways to cut costs. Chances are, yours is too. And yet, you may well be missing out on a major opportunity. Simply by making your records management more efficient, you can dramatically cut operational costs.

Eliminating the time employees waste searching for documents is just one way to potentially put money back on your bottom line.

Learn more about how Iron Mountain® can help you cut costs and turn records management into a source of opportunity at: ironmountain.com/advantage

