INFORMATION MANAGEMENT

AN ARMA INTERNATIONAL PUBLICATION

SEPTEMBER/OCTOBER 2013

Propelling the Profession (and the Professional) to the Next Level

Page 20

RISKY BUSINESS
Choosing Information Service Providers

Page 26

The Trusted Information Payoff:
Productivity, Performance, and Profits

Page 35


rsd
RSD GLASS® IS YOUR GOLDEN TICKET TO INFORMATION GOVERNANCE
booth 617
TICKET
booth 617
TRANSPARENCY
ACCOUNTABILITY
REPEATABLE
AUDITABLE
MEASURABLE
ACHIEVABLE
COMPETITIVE
salesforce
THE ONLY PATENT PENDING SOLUTION FOR IN-PLACE ENFORCEMENT
THE OFFICIAL SPONSOR
IG
of Information Governance
SharePoint
www.rsd.com

INFORMATION MANAGEMENT

SEPTEMBER/OCTOBER 2013 **VOLUME 47 NUMBER 5**

Online
Info for
Offline
Success

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

ARE YOU AN ARMA PRO?

INFORMATION MANAGEMENT ONLINE

www.arma.org

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 Zlitni

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

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

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

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

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

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.

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

Information Stakeholders Unite!

This year's joint ARMA International/Forrester Research technology survey results affirm the direction ARMA has been advocating for the past few years: records and information management (RIM) professionals need to be developing broader information governance (IG) skills if they want to have more influence in and impact on their organizations.

IG skills, which encompass aspects of IT, legal, privacy, and business/audit, would allow survey respondents to meet what they identified as their organizations' second greatest challenge: "lack of IT, legal, compliance, and business stakeholder alignment." Understanding what these other stakeholders' information-related goals and challenges are and being able to work with them to help them meet those goals will result in stronger RIM and IG programs.

For example, working more closely with IT stakeholders would have a major impact on improving what survey respondents said is their organizations' third greatest challenge: "limited capabilities to integrate with other systems."

Perhaps, developing stronger relationships with IT stakeholders should be a major objective for RIM professionals. Forrester analyst Cheryl McKinnon, IGP, concludes in her cover article, "As IG concepts help propel the RM profession into its next level of maturity, areas of richest opportunity include deepening the relationship with IT to get a strong grasp on storage, technology roadmaps, and software budgets." Reading this issue will pay dividends in this regard.

Authors Karim N. Sidi and Dale A. Hutchinson explain in "The Trusted Information Payoff" how using an information management framework can address the problems that arise from incompatible information systems and data sources. This framework depends on data standards that are enforced through active governance to produce information that is true, has integrity, and can be trusted.

RIM, IT, and legal stakeholders all need to understand the risks of engaging service providers that will handle their information assets – digital and physical. In "Risky Business," National Association for Information Destruction President Robert Johnson provides a rundown of regulatory, due diligence, and contractual requirements organizations need to meet in these relationships.

RIM professionals also need to work closely with information stakeholders to implement technology solutions in organizations that want to progress toward having a paperless office. Anna Stratton, CDIA, explains in her RIM Fundamentals Series article that two of the primary factors that contribute to failed technology implementations are 1) jumping to a technology solution without first doing a needs assessment and 2) providing access to the technology without sufficient training or a model for end users to follow.

The most prevalent types of technology being implemented in organizations today are web-based, and the information being created or stored with these tools also needs the attention of all information stakeholders. The recent revelation about the U.S. National Security Agency's surveillance of web-based traffic and the data breaches that are frequently in the news also put pressure on information stakeholders to work together. Read Julie Gable's article to find out how technology law expert Michael Geist, J.S.D., believes these types of incidents will lead to the Generally Accepted Recordkeeping Principles® being extended in new ways.

What information challenges is your organization facing? E-mail *editor@armaintl.org* to tell us how we can help.

Vicki Wiler
Editor in Chief


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

PRIVACY

NSA Leak Shrouds EU-U.S. Trade, Privacy Discussions

Data protection and privacy were critical issues in the July trade talks between the European Union and the United States regarding the Transatlantic Trade and Investment Partnership (TTIP). Although these are not new issues, they have grown in importance thanks to recent reports on the U.S. National Security Agency's (NSA) PRISM project, which included the bugging of EU diplomatic offices in Washington, D.C.

As reported by *Politico*, the goal of TTIP is to "'liberalize' trade between the EU and the United States with a view to remove cross-border regulatory issues, which can bring about extra costs and stifle trade."

The first round of negotiations focused on online privacy and piracy as negotiators tried to reconcile the technology industry's "push for digital freedom with European desires for individual protections," according to the article.

Proposed reforms to the EU's data protection laws center on the concept of "clear rules for a clear Internet and the choice for the individual to give his data or not," said Viviane Reding, European commissioner for justice, fundamental rights, and citizenship, in a recent speech.

According to *ZDNet*, Reding further stressed that data protection rules must apply to any EU citizen data, regardless of whether the company holding that data is based outside the EU; to cloud software and platform providers; and to metadata.

The proposed data protection reforms that Reding referenced are the General European Data Protection Regulation, which concerns general data processing by companies, and the Data Protection Law Enforcement Directive, which relates to the processing of data by police and judicial authorities. A third is a "bilateral data protection agreement being negotiated between the U.S. government and the EU to try and establish the principle that any transfer of EU citizen data should take place through 'established legal channels,'" according to *ZDNet* writer Nick Heath. This agreement would likely have the most impact on intelligence gathering activities such as PRISM.

PRISM Fuels Cries for EU Clouds

One of the cornerstone issues in discussions of cloud services is whether to focus on building national clouds or take advantage of existing clouds offered by international providers, especially U.S. providers.

Estonian President Toomas Hendrik Ilves, chair of the steering board of the new European Cloud Partnership, contends Europe should have its own clouds rather than rely on those from U.S. service providers, reported *ZDNet*.

"Recent months have proven it again: it is very important for Europe to create its own data clouds, operating under EU law and completely safe for users," said Ilves.

Citing the claim that 95% of cloud services in Europe are provided by U.S. companies, Ilves said EU data protection legislation needs to be modernized and that people must understand that large private firms can gather more information than any state. Ilves added that Europe must establish its own cloud at a European level because "otherwise the economies of scale will leave us behind."

CLOUD

How's Your Cloud Insurance Coverage?

There is a big gap between the cloud computing insurance offered by conventional insurance companies and the risks presented by cloud computing, according to Eric Lowenstein, client manager with the financial services group of Aon, in Sydney.

"There is a broad range of cover options available but these have problems," he recently told *ITPro*. "What are the geographical exclusions in regard to data sent offshore? And there are uncertainties about the definition of networks. Do they include devices like iPads, laptops, etc.?"

Lowenstein stressed that this is not simply an IT issue. The cloud poses risks to many stakeholders – IT, marketing, legal, communications, and even the CFO and CEO – and they all need to be engaged.

A cloud computing insurance industry is emerging in the United States. Earlier this year, the MSPAlliance, an association of cloud service providers, announced a partnership with insurance broker Lockton that offers comprehensive protection for cloud and managed service providers around the world. MSPAlliance reportedly has been offering cloud coverage in Australia since 2008.

According to *ITPro*, the U.S. organization CloudInsure has also partnered with Lockton "to provide indemnity assurance to cloud service providers and enterprises in support of service level agreements, and financial protection for customers 'commensurate with their data risk within the cloud.'"

The U.S.A. Patriot Act and recent NSA PRISM project have added fuel to concerns over data risk within the cloud. Adrian Lawrence, a partner with the law firm Baker & McKenzie, warned that the Patriot Act, which grants wide-ranging powers to U.S. government agencies, could be applied outside the United States to any cloud service provider that is owned by, or a subsidiary of, a U.S. company. Lawrence said enterprises, cloud service providers, and insurers must take these types of issues into consideration sooner rather than later.

EHR

U.S. Doctors and Hospitals' EHR Use Is Up

In just three years, 40% of office-based physicians and 42% of hospitals in the United States have implemented at least a basic electronic health records (EHR) system, according to a report co-authored by the Robert Wood Johnson Foundation, Harvard School of Public Health, and Mathematica Policy Research.

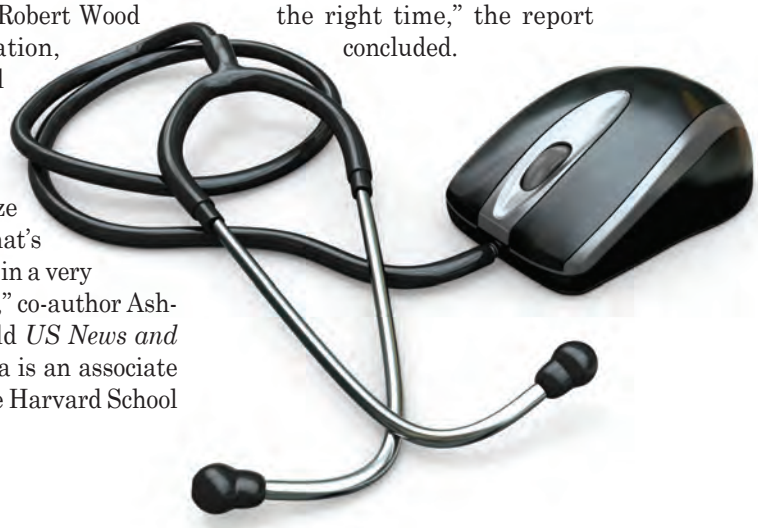
"Given the size of our country, that's amazing progress in a very short time period," co-author Ashish Jha, M.D., told *US News and World Report*. Jha is an associate professor with the Harvard School of Public Health.

The researchers credit three factors for driving the adoption of EHRs: society's increasing reliance on information technology, new federal funding to support the purchase of EHR systems, and future penalties for those who don't use EHRs.

"It's the right incentives at the right time," Jha said. "Doctors and hospitals have been thinking about buying electronic health records [systems] for some time. This is where our society is moving. But the finances have been a challenge. The federal incentives have been very well targeted. They were well designed to help push hospitals and doctors to adopt EHRs."

The study's findings weren't all quite as positive, however. For example, only 5% of the systems meet federal standards for exchanging that data with other providers to allow widespread physician access to a patient's records. The good news is that more healthcare providers are reportedly participating in initiatives that ultimately will connect their own electronic records systems to community-wide information exchanges.

Predictably, there are several improvements needed before EHR use can be optimized. "Even with improved functionality, high-quality patient education still depends on clinicians and educators with the time and skills to tailor the right materials to the patient at the right time," the report concluded.



MOBILE DEVICES

Mobile Safer than Desktops?

Yes, it could happen. By next year, mobile technology could actually be more secure than traditional computing.

This bold prediction was made by Marc van Zadelhoff, IBM vice president of strategy and product management, in a recent article in *USA Today*.

"Companies are adopting best practices that are rapidly enabling mobile computing to become more secure than traditional desktop computing," he said. "This is being led by chief information security officers who are driving change to ensure critical mobile security needs are addressed today."

Although mobile devices and tablets are primarily considered consumer products, they are increasingly being used for business purposes. Research conducted by Vertic, a digital ad agency, showed that tablet use in enterprises has grown nearly 50% annually since 2011. More than 96 million tablets are expected to have been shipped to enterprises by 2016. Further, 38% of senior executives were issued tablets in 2011.

Mobile usage has become a major driving force in IT over the past few years, a trend that is expected to continue in the near term. It has forced organizations to develop and expand policies that guide use and security of these devices. For example, a growing number of organizations now require employees to adopt solutions on their mobile devices that help keep personal data separate from corporate data.

Given the advances in mobile technology, van Zadelhoff concluded that security officers will have more finite control over mobile devices than they've had over traditional computers. "Going forward, mobile devices no longer have to be a security threat, but instead it can be seen as a 'do-over' in order to get it right," he said.

E-DISCOVERY

Gartner Predicts Growth, Consolidation in E-Discovery Market

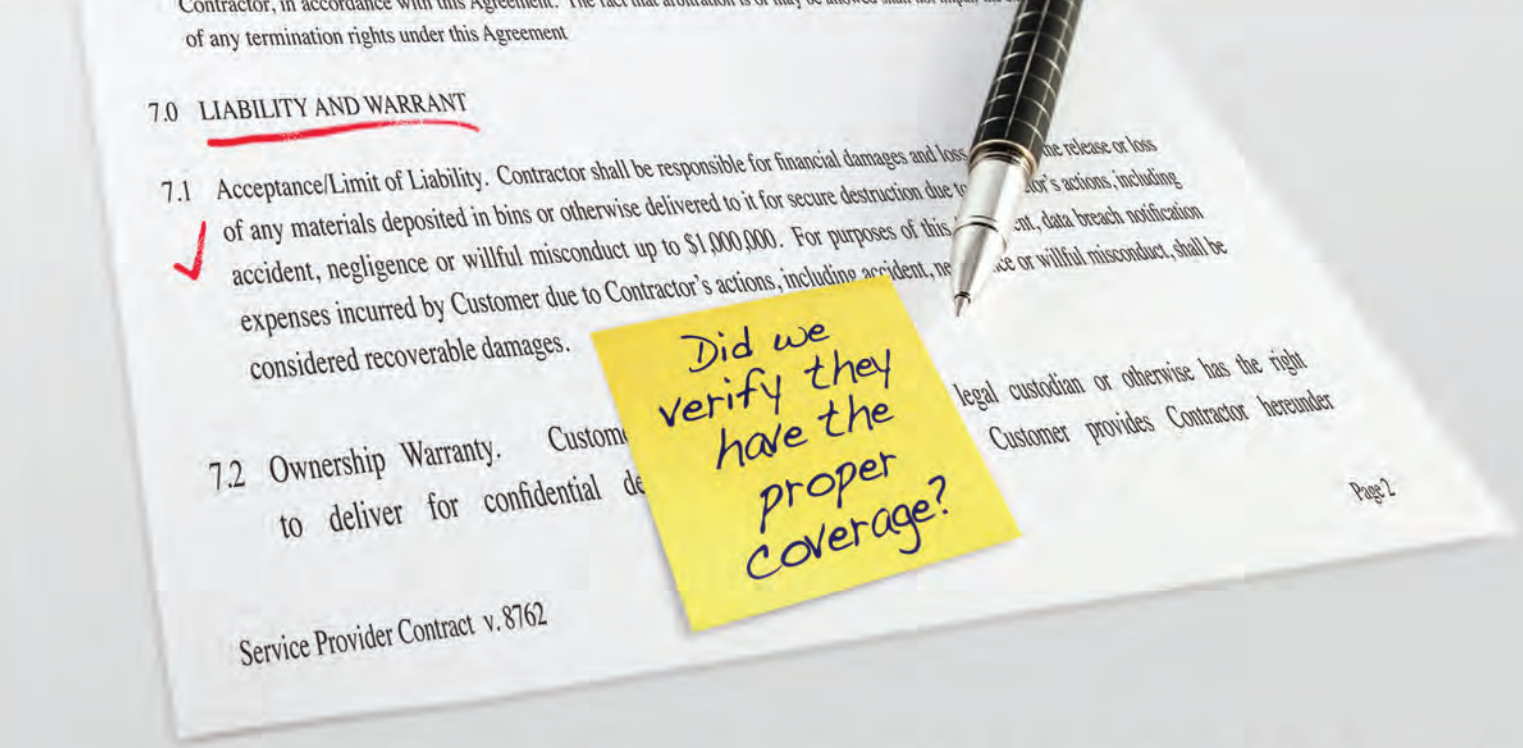
Double-digit growth and continued consolidation are likely in the global e-discovery market over the next few years, according to Gartner Inc.'s *Magic Quadrant for E-Discovery*, published in June.

Gartner expects the market to grow by about 15% annually, from $1.7 billion in 2013 to $2.9 billion by 2017. This growth will be largely attributable to two factors: increasing volumes of litigation and regulatory investigation; and the growing volume of content and data that must be searched in support of these activities.

The majority of this market growth will reside with U.S. vendors, but the increasing awareness of e-discovery issues in Europe and Asia will drive growth there, eroding the U.S. share of the total market from 81% in 2012 to less than 70% in 2017. In addition, software vendors in adjacent markets, such as enterprise content management, will likely extend their offerings to include e-discovery functions, and vendors already in the e-discovery market will acquire additional capabilities from the content analytics or workflow sectors, for example.

While revenues grow, the number of firms claiming to have e-discovery products and services is expected to shrink by 25% during the next two years. Most of that attrition is expected among service providers, not software vendors. Consolidation is already underway and is expected to continue, driven primarily "by the disintermediation of law firms, pricing pressure, and the need to develop economies of scale in data management," the report states.

Predicts Gartner: "The remaining legal-services firms will take one of two routes by becoming either large firms that are 'one-stop shops' but not technology developers, or large firms that are one-stop shops with proprietary technology for all aspects of the EDRM, not just the traditional hosting and review capabilities that have long sustained the industry. Although there is room for regional and specialist players, this is the part of the market that is consolidating and shrinking fastest. The larger players will need international presence in the form of data centers and local legal personnel to be competitive as the market opens up geographically."



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

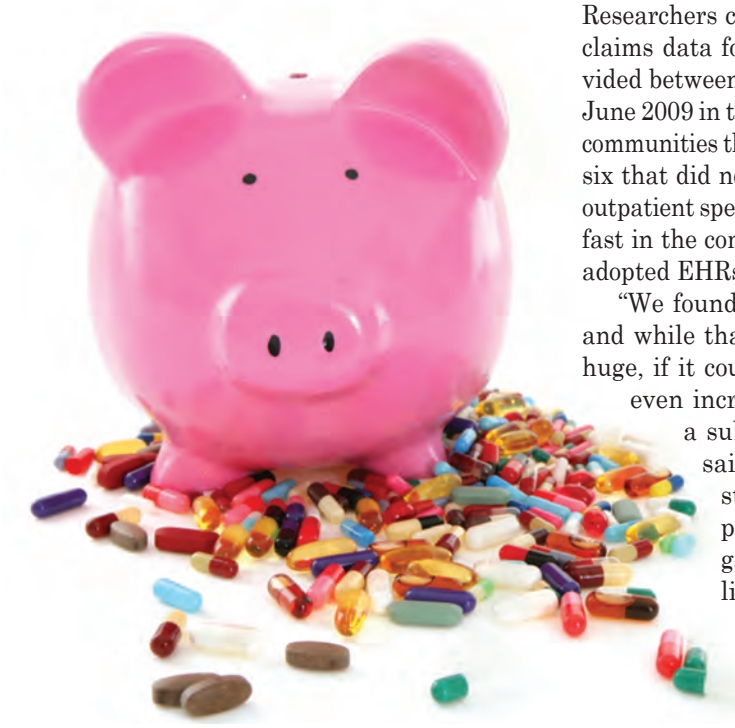
www.downstreamdata.com

NAID, the NAID logo, Downstream Data Coverage, and the Downstream Data Coverage logo are registered trademarks of the National Association for Information Destruction. Downstream Data Coverage is offered exclusively as a benefit of NAID membership to NAID AAA Certified member companies. All rights reserved.

EHR

Study Shows EHRs Do Lower Costs

A recent article on *Medical Xpress.com* indicates that doctors who use commercially available electronic health record (EHR) systems are seeing slower growth in healthcare costs, saving $5.14 per patient per month.



These savings were documented by a recent University of Michigan study of the impact of EHRs in community-based settings, including private practices and hospitals. Researchers compared insurance claims data for patient care provided between January 2005 and June 2009 in three Massachusetts communities that adopted EHRs to six that did not. They found that outpatient spending did not rise as fast in the communities that had adopted EHRs.

"We found 3 percent savings and while that might not sound huge, if it could be sustained or even increased, it would be a substantial amount," said Julia Adler-Milstein, an assistant professor at Michigan's School of Public Health and the study's lead author.

Most of the savings were in radiology. Adler-Milstein suspects doctors ordered fewer imaging studies because they had better access to patients' medical histories. This finding also contradicts the assertion that EHRs would actually raise costs because they make it easier to order tests, which is a key argument of critics who oppose using taxpayer dollars to fund EHRs.

The nine communities in the study had all applied to participate in the Massachusetts eHealth Collaborative's pilot, which gave funding and support for doctors' offices to convert their records.

"I think our findings are significant because we provide evidence to support the use of taxpayer dollars to invest in electronic health records," Adler-Milstein said. "We really have not had compelling evidence that proved that they would save money. It was assumed, but there are a lot of skeptics. This study helps clarify whether there are cost savings and what the magnitudes of those are in the near-term."

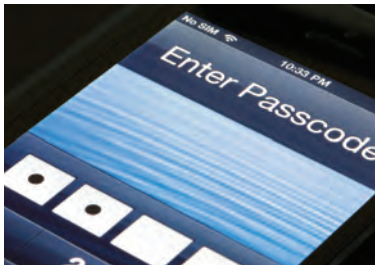
CYBERSECURITY

Online Security a Growing Concern for Insurance Industry

A recent study by Ernst & Young clearly showed that the global insurance industry takes cybersecurity very seriously. In fact, Ernst & Young expects it to be one of the top three issues facing the industry by 2015. It is currently ranked sixth.

Contributing factors cited by the report include the increasing availability of sophisticated hacking tools on the Internet; the growing pool of people capable of seriously breaching corporate security; the difficulty of developing a coordinated approach to Internet management, which offers an element of protection to criminals who route their attacks through multiple countries; the rising threat of state-sponsored cyber attacks; and the ease of staging distributed denial-of-service attacks.

"The key factor is to ensure an appreciation of cybersecurity as a due diligence and compliance issue, one that is recognized within the risk management function and regarded as a strategic risk at the highest corporate level. This is clearly a complex issue, but simple moves, such as regular CIO reports to the board and tracking cyber-attack incidents above a certain threshold in the company's key performance areas, can convey the seriousness with which it is taken at the top," the researchers concluded.



PRIVACY

Employees Don't Trust Employers with Mobile Data, Privacy

Use of personal mobile devices for sharing information on company networks has become commonplace. Most employees, however, don't trust their employers to protect their personal information.

A recent study of about 3,000 employees in the United States, United Kingdom, and Germany discovered that only 30% trust their employers to keep personal information private and not use it against them. Those in the UK were most trusting, with 34% saying they completely trust their employer, compared to 31% in the United States and 24% in Germany.

The survey further revealed confusion among the respondents as to what constitutes private information. Nearly 41% felt certain their employer could not see any private information on their mobile device. Only 28% thought the company could see their work e-mail and attachments.

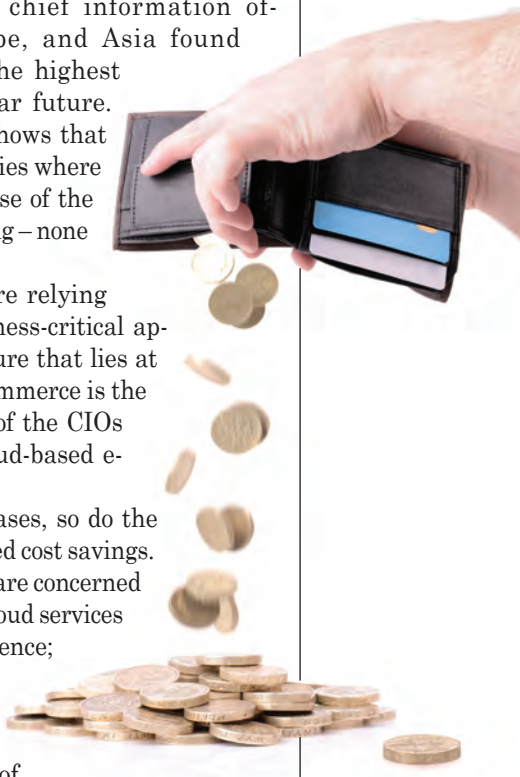
"The reality is that if these devices are used to get corporate email, employers can see work email and attachments on a mobile device as easily as they can on a PC. That's a gulf between expectations and reality," said Ojas Rege, vice president of strategy at security firm MobileIron, which sponsored the research.

"It's a new set of technologies, so there's immediately some level of confusion," Rege told *The Telegraph*. "Another thing is that IT departments are traditionally not very good at communicating; it's not their core competence."

He said the level of distrust among employees is due largely to a lack of transparency within organizations and the absence of clear policies around bringing mobile devices to work.

CLOUD

CIOs Cite Cloud's Hidden Costs as Chief Concern



A recent Compuware survey of chief information officers in the Americas, Europe, and Asia found that cloud computing will be the highest priority area for investment in the near future.

Current IT infrastructure spending shows that companies are exploiting cloud opportunities where they see them, which are primarily the use of the public cloud for backup, recovery, and testing – none of which directly affects the end user.

The study showed that companies are relying increasingly on the cloud to deliver business-critical applications and the supporting infrastructure that lies at the core of their business operations. E-commerce is the most commonly used cloud service; 81% of the CIOs are already using or planning to use cloud-based e-commerce platforms within the year.

As investment in cloud services increases, so do the stakes for the cloud to deliver on its promised cost savings. However, the majority of companies (79%) are concerned there will be hidden costs associated with cloud services prompted largely by poor end-user experience; 64% of the CIOs cited poor end-user experience as the most significant risk to managing the cloud.

Despite the business-critical nature of these cloud applications and the potential impact of poor end-user experience, the report revealed that 73% of companies are still using outdated methods to track and manage application performance. The most common tracking metric is simple availability or uptime, rather than more granular end-user metrics such as response time, page rendering time, and user interactivity time.

"The cloud is increasingly being used to deliver business-critical applications, so it is quite shocking that most companies are just waiting for problems to occur and then firefighting," said Thomas Mendel, managing director at Research In Action, which conducted the survey for Compuware. "The fact is that most traditional monitoring tools simply don't work in the cloud. Effectively monitoring and managing modern cloud-based applications and services requires a new approach designed to work in today's complex, hybrid, and dynamic environments. Failure to do so could have a hugely detrimental impact on reputation, customer loyalty, and revenues."

CYBERSECURITY

Hackers Attend Summer Camp

Maybe you've heard of Space Camp, but how about hackers' camp? The U.S. Cyber Challenge (USCC) is conducting four regional camps this summer to provide specialized cybersecurity training to some of the brightest young talent in cybersecurity.

The camps feature workshops led by college faculty, top System Administration, Networking, and Security Institute instructors, and cybersecurity experts from the community. The workshops and presentations focus on topics ranging from intrusion detection, penetration testing, and forensics. Campers can also participate in a job fair where they can meet USCC sponsors and discuss potential employment.

Cybersecurity experts who can bring a fresh perspective to the profession are in top demand in the private and government sectors. It's estimated there are as many as one million openings in this highly specialized job market in the United States alone.

USCC's program is working to find 10,000 of America's best to fill the ranks of cybersecurity professionals. Other countries see the need as well; France, for example, has conducted similar cyber challenges, according to the BBC News.

Academic institutions have increased their efforts to meet the need for cyber professionals, but the demand is still much greater than the supply, according to Diane Miller, who directs Cyber Patriot, a national high school cyber-defense competition that's presented by Northrop Grumman and the Air Force Association. "Everybody is scrambling to find that exceptional talent," Miller told BBC News.

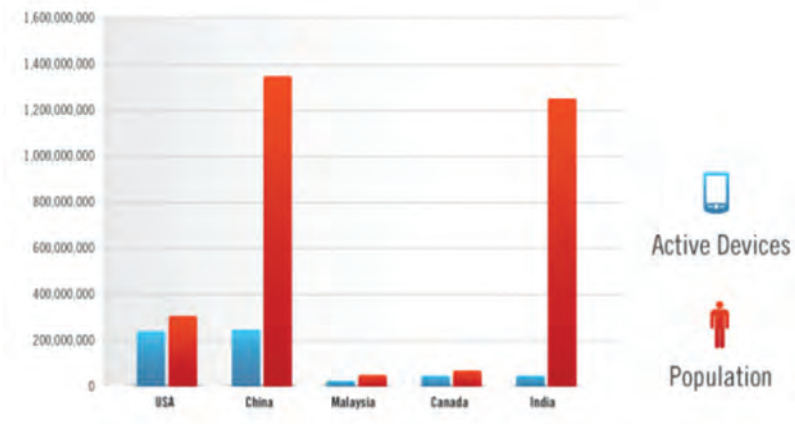
Some worry that this type of training could be turned against organizations and the government. Samuel Schneider, a representative of the global IT security organization (ISC)2, takes a different view: "The earlier we reach them, the less risk they are at . . . going out and performing illegal or illicit activities."

Headded that this is an excellent opportunity to "indoctrinate or incorporate a new security mentality into children."

MOBILE DEVICES

World Market Means Big Growth for Mobiles

The latest forecast from International Data Corp. (IDC) predicts a 33% increase in the number of smartphones shipped in 2013 alone. That equates to about 959 million phones, compared to nearly 723 million in 2012. Furthermore, this trend will likely continue for many years given the growing market in less-developed countries. With increasing demand from poorer markets come lower prices. IDC reports that smartphone average selling prices (ASPs) have declined to $372 in 2013, down from $407 in 2012 and $443 in 2011. The ASP is expected to drop as low as $309 by 2017, thanks largely to the continued emerging market demand.



Forecast: CLOUDY

Prepare for the future of electronic records management in the cloud by earning a Master's Degree in Archives and Records Administration (MARA) from the San José State University School of Library and Information Science.

Our convenient and flexible fully online program connects you to a global community of scholars, researchers, and information professionals. You'll learn to use sophisticated technologies to organize, preserve, and access a growing volume of digital and analog assets. And you'll be well-prepared to pursue a wide range of exciting career opportunities in the fields of information governance and corporate archives. **Join us today!**

We're hosting an online information session on October 1, 2013. **RSVP today!** bit.ly/MARAOpenHouse

"The greatest strengths of the MARA program are the small class sizes, online learning tools, and fantastic instructors."

– Spring 2013 graduate

SAN JOSÉ STATE UNIVERSITY | SCHOOL OF LIBRARY AND INFORMATION SCIENCE

Let the learning begin:
slisweb.sjsu.edu/mara

CLOUD

Spare Cloud Computing Capacity to Be Traded on German Stock Exchange

Beginning the first quarter of 2014, Deutsche Börse, the operator of the Frankfurt stock exchange and Eurex derivatives exchange, will start trading in its spare cloud computing capacity. Buyers and sellers of at least one terabyte in cloud-computing data space – the size of the average external home hard drive – will be able to match supply and demand through a new platform run by the exchange, with real-time prices.

International Data Corp. has predicted an annual growth rate of up to 40% in Europe's cloud infrastructure over the next seven years as it attempts to catch up with developments in the United States and Asia. The *Wall Street Journal* reported that Deutsche Börse and Zimory, a Berlin-based software developer that does not provide cloud capacity, recently formed Cloud Exchange AG in hopes of being a "catalyst" for that growth.

Buyers of cloud capacity apparently will be able to choose the location and jurisdiction of the servers, as well as stipulate how long they want to rent the cloud capacity. They also will be able to migrate between vendors, choose the safety level they want for their data, and choose their disaster recovery measures and data speed.

The article added that a group of up to 20 "early adapters" is working on the details to ensure the marketplace can go live with enough liquidity early next year.

Other commercial cloud marketplaces exist but are affiliated with specific vendors.

EHR

Despite EHR Growth, Australian Doctors Resist Letting Patients See Records

The use of electronic health records (EHRs) in Australia grew 62% from 2011 to 2012 – and the initial results have been encouraging. According to a survey by Accenture, 83% of Australian doctors are actively using electronic medical records (EMRs) and roughly 70% reported improved quality of diagnostic and treatment decisions as a result of sharing the EMRs. Indeed, most (77%) Australian doctors believe sharing health records electronically helped reduce medical errors in 2012.

Australia's personally controlled electronic health record (PCEHR) scheme has had a slow start despite support by government and prominent healthcare CIOs. When it comes to providing patients control over their personal EHRs, Australian doctors are more resistant than doctors in other countries. Fewer than one-quarter of Australian doctors believe patients should have full access to their records; 65% believe patients should have limited access; and 16% say they should have no access. Australia ranked second highest of the eight countries surveyed in the proportion of doctors who say patients should have no access to their records.

"The shift to patient-centered care has long been talked about, but we're now entering a new stage with the rise of the digital citizen and availability of electronic health records," said Leigh Donoghue, managing director of Accenture's health business in Australia and New Zealand.

"The combination of smartphones, faster broadband, mobile access to the PCEHR system, and a growing array of mobile health applications will trigger fresh demands from consumers for more active participation in managing their own care. To meet changing consumer expectations, Australian doctors' views on patient access will need to evolve," said Donoghue.

CYBERSECURITY

Medical Device Manufacturers Tackle Cybersecurity

It appears medical devices are not immune to the risks associated with cyber attacks. After all, many medical devices contain configurable embedded computer systems that can be vulnerable to breaches.

Although the U.S. Federal Drug Administration (FDA) is not aware of any targeted devices or of any injury or death as a result of a cyber attack, it said it has become aware of cybersecurity vulnerabilities and incidents that could directly impact medical devices or hospital network operations.

"Over the last year, we've seen an uptick that has increased our concern," said William Maisel, deputy director of science and chief scientist at the FDA's Center for Devices and Radiological Health. "The type and breadth of incidents has increased."

He said officials used to hear about problems only once or twice a year, but "now we're hearing about them weekly or monthly."

The Department of Homeland Security (DHS), which is working with the FDA to reduce these vulnerabilities, recently received reports from two researchers that found potential weaknesses in 300 medical devices produced by about 50 vendors, an official told *DelawareOnline*.

The FDA has been working closely with DHS and other agencies and manufacturers to identify, communicate, and mitigate vulnerabilities and incidents as they are identified, but the agency is asking device manufacturers to do more.

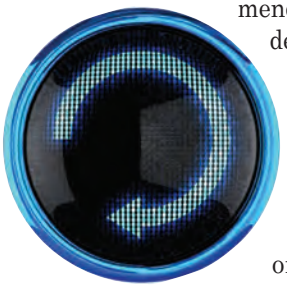
Specifically, the FDA recommends that manufacturers "review their cybersecurity practices and policies to assure that appropriate safeguards are in place to prevent unauthorized access or modification to their medical devices or compromise of the security of the hospital network that may be connected to the device. The extent to which security controls are needed will depend on the medical device, its environment of use, the type and probability of the risks to which it is exposed, and the probable risks to patients from a security breach."

The FDA has similarly requested that healthcare facilities evaluate their network security and take steps to protect the hospital system. That includes restricting unauthorized access to the network and networked medical devices; ensuring appropriate antivirus software and firewalls are up to date; monitoring network activity for unauthorized use; and working with the device manufacturer if they detect a security problem.

The FDA is working on guidelines – to be available this year – that will allow it to block approval of devices if manufacturers don't provide adequate plans for protecting the devices and updating their security protections over their commercial lifetimes.

MOBILE DEVICES

NIST Publishes BYOD Guidance



The National Institute of Standards and Technology (NIST) finally updated its 2008 *Guidelines on Cell Phone and PDA Security* to reflect the tremendous growth of mobile devices. The new *Guidelines for Managing the Security of Mobile Devices in the Enterprise* recommends using centralized device management at the organization level to secure both agency-issued and individually owned devices used for government business.

Centralized programs manage the configuration and security of mobile devices and provide secure access to an organization's computer networks. Many agencies currently use this type of system to manage the smartphones they issue to staff. The new NIST guidelines offer recommendations for selecting, implementing, and using centralized management technologies for securing mobile devices.

Other key recommendations include instituting a mobile device security policy, implementing and testing a prototype of the mobile device solution before putting it into production, securing each organization-issued mobile device before allowing a user to access it, and maintaining mobile device security.

GOVERNMENT RECORDS

Revisiting the '70s: More Watergate Records Released

"All the News That's Fit to Print"

The New York Times

LATE CITY EDITION

VOL. CXXIII ... No. 42,566 NEW YORK, FRIDAY, AUGUST 9, 1974 15 CENTS

NIXON RESIGNS

HE URGES A TIME OF 'HEALING'; FORD WILL TAKE OFFICE TODAY

'acrifice' Is Praised; Kissinger to Remain

By ANTHONY RIPLEY

The 37th President Is First to Quit Post

By JOHN HERBERS

POLITICAL SCENE SHARPLY ALTERED

Rise and Fall

Appraisal of Nixon Career

JAWORSKI ASSERTS NO DEAL WAS MADE

The U.S. National Archives and Records Administration (NARA) has released additional records that had been sealed since the criminal trial of seven men involved in the Watergate burglary (*U.S. v. Liddy, et al.*) in the 1970s. NARA released 36 folders of documents totaling approximately 950 pages upon an order from the U.S. District Court for the District of Columbia.

All trial records have been "unsealed," but NARA said it is still required to withhold personal privacy information, grand jury information, and illegal wiretap information, as appropriate.

Newly unsealed records include the names only of those overheard by the bugs installed in the break-ins at the Democratic National Committee headquarters at the Watergate. They also contain the pre-sentence reports for the Cuban burglars. NARA said such records of living persons are not usually released publicly, but the court stated in its opinion that "the public's interest in clarifying the historical record and further identifying the facts that led to the resignation of President Nixon outweigh their individual privacy interests."

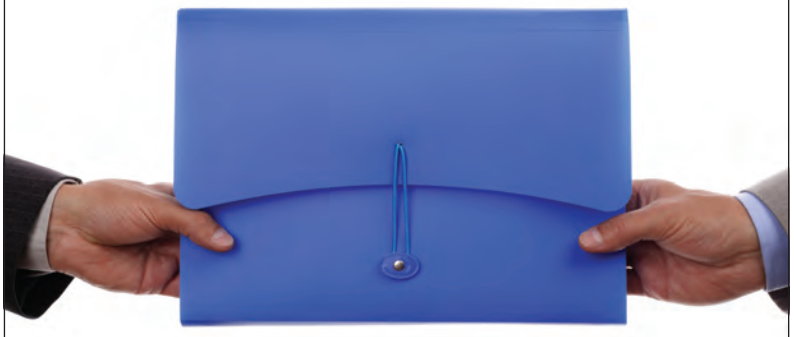
FACTOID

52% of U.S. physician groups planning to implement electronic health record (EHR) systems do not plan to replace their current practice management system with an integrated practice-EHR management system.

Source: 5th Annual U.S. Ambulatory Electronic Health Record & Practice Management Study, released by HIMSS Analytics

E-DISCOVERY

New Service Concept in E-Discovery Technology Emerges



As e-discovery technology moves beyond litigation into the realm of investigation, the volume of data continues to grow, making it difficult for many corporate legal departments to keep up. They are searching for a solution that is agile, up-to-date, and economical – a solution that provides control over their data, said Lynn Frances, a legal technology analyst, in her recent article in *Metropolitan Corporate Counsel*.

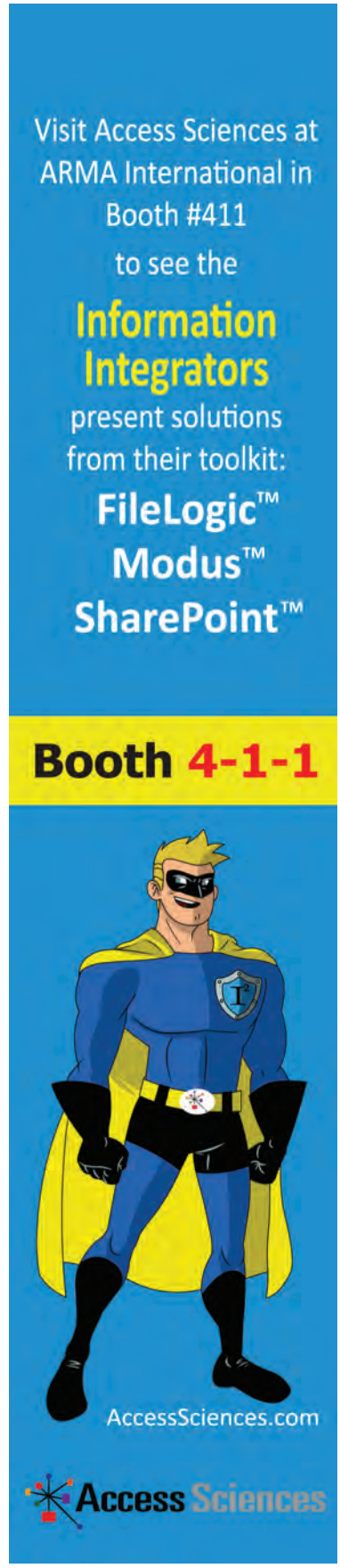
Historically, legal departments that wanted to maintain tight control over their data have kept it in-house. Some built such large litigation support departments that they could have been fully operational e-discovery services companies. When technology wasn't changing as quickly, the in-house model was a valid option for those that could afford the up-front investment, according to Frances.

Predictably, the do-it-yourself (DIY) solution wasn't viable for smaller organizations that couldn't afford the investment in technology and personnel or that chose to focus on their core business. They chose outsourcing as the solution.

In the outsourcing model, corporations relinquished control of their data, workflow, and protocol to outside counsel and e-discovery service providers. "Unless they established their own case-tracking and analysis systems in-house, general counsel, whose cases were spread among various service providers, lacked the business intelligence that the DIY departments enjoyed," Frances wrote.

Because of the tremendous changes the field has seen in the last several years, the cloud is a third option that offers the benefits of the other two models. In the cloud model, the initial and ongoing investments in software, infrastructure, and security lie with the service provider. This allows the client to determine what portions of the processes will be run in-house and places the final control of the data in the organization's hands. Of course, to provide assurance on data security, a cloud-based offering that hosts legal data must be housed in a highly secure environment with verified security protocols.

"This type of model was not possible in the legal industry just three years ago because attorneys were uncomfortable with the cloud as a legal data environment," noted Frances. Indeed, a 2011 survey of in-house counsel found that only 29% of the responding companies used cloud technology. That number has changed drastically: the 2013 Corporate Counsel Survey showed that four out of five respondents reported a good experience with cloud-based computing.



Even the Caveman kept records. It's how you store, access and protect your records that separates you from the pack.

Call iScan today for a consultation and quote!

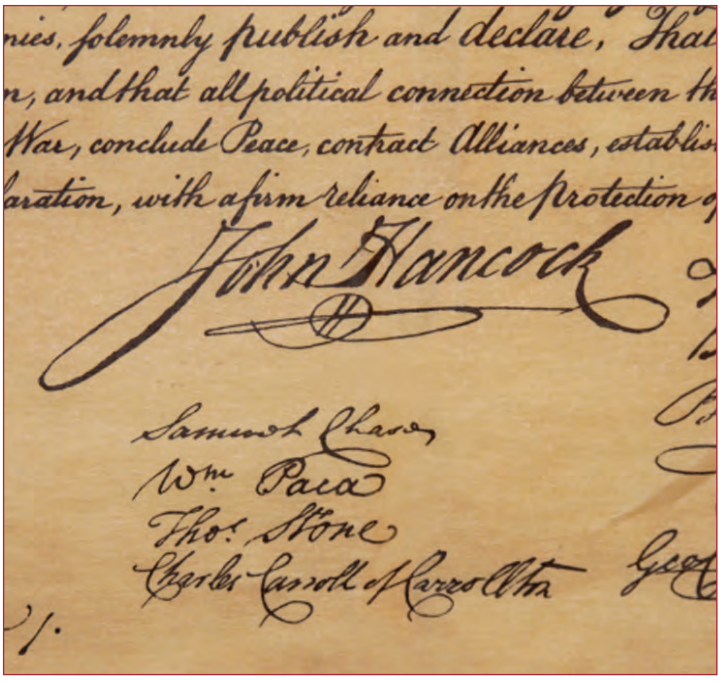
(410) 800-8332

iSCAN

document scanning, storage & shredding

www.iscan.com

Contact:
Jeff Edwards
jedwards@iscan.com
(410) 800-8332



ARCHIVES

Attention U.S. History Buffs: Founders' Papers Are Online

If you haven't yet discovered the new *Founders Online* website, launched this summer by the U.S. National Archives and Records Administration (NARA), now may be a good time to do so. The site, which was still in beta at the time of printing, features correspondence and other writings of George Washington, Benjamin Franklin, John Adams, Thomas Jefferson, Alexander Hamilton, and James Madison.

For the past 50 years, through its National Historical Publications and Records Commission, NARA has invested in documentary editions of the original historical records of the Founding Era. Dedicated historians and experts in editing historical documents have collected copies of original 18th and 19th century documents, transcribed them, provided annotations, and produced hundreds of individual volumes – all of which eventually will be fully searchable and available for free on the *Founders Online* site.

Founders Online will include thousands of documents, replicating the contents of 242 volumes drawn from the published print editions. As each new print volume is completed, it will be added to this database of documents.

The site launched with 119,000 searchable documents, fully annotated. All of the unpublished and in-process materials (about 55,000 documents) will be posted online over the next three years. Researchers will be able to view transcribed, unpublished letters as they are being researched and annotated by the editors and staff. Altogether, some 175,000 documents are projected to be on the *Founders Online* site. **END**

Versatile RFID Solutions™

Process your records in "record" time!

ZASIO

RECORDS & DOCUMENT MANAGEMENT EXPERTS

Have you ever thought about what having superpowers would mean in your world? You would be able to see all the files in a box with a single glance. You could inventory thousands of records in "record" time. With Radio Frequency Identification (RFID) tags on your files and boxes, you can!

Because radio signals pass through paper, cardboard, and wood, you can quickly locate a file within a box without even taking off the lid. RFID readers can scan multiple tags at once, so processing large batches of records for storage, check-in, and check-out is fast and efficient. Entire file rooms and record centers can be inventoried in a fraction of the time it would require with a standard barcode reader.

Zasio's newest mobile reader software takes traditional barcode processing to a new level. Another reason to choose Zasio's Versatile Software for your records management needs!

Stop by booth #107 at the ARMA 58th Annual Conference & Expo to see our latest software developments, including Versatile RFID Solutions, SharePoint integration, mobile enablement, and more.

800 513 1000 | www.zasio.com

Connect with us:

© 2013 Zasio Enterprises, Inc.

Propelling the Profession (and the Professional) to the Next Level

The results from Forrester Research and ARMA International's recent online records management survey show rising support and professional knowledge of information governance principles. But, if records managers want to propel their careers, as well as the profession, to the next level, they need to get better acquainted with resource planning, technology roadmaps, and their colleagues in IT.

Cheryl McKinnon, IGP

2013 marks the fifth year ARMA International and Forrester Research have surveyed records management (RM) decision makers in an effort to track key trends in adoption, challenges, and technology rollout. Conducted June 5-July 12, 2013, the "Forrester Research and ARMA International Records Management Online Survey, Q3, 2013" gathered responses from 397 RM decision makers from around the globe.

Forrester's findings show a continued rise in awareness of the Generally Accepted Recordkeeping Principles® (Principles), as described and promoted by ARMA International and its members. The survey results, however, also reveal that not all RM professionals are able to consistently put the Principles into action.

Developed to "foster general awareness of information governance standards and principles and to assist organizations in developing information management systems that comply with them," the Principles describe characteristics of information governance (IG) program success.

Ninety-one percent of survey respondents claim familiarity with the Principles, a slight increase from the 2012 survey, which revealed that 85% of respondents had familiarity. (See the 2012 survey highlights at *http://tinyurl.com/l4fps65.)*

Despite this strong awareness, many RM decision makers still have work ahead to bring the Principles of Accountability, Integrity, Protection, Compliance, Availability, Retention, Disposition, and Transparency into fruition in their workplaces.

Accountability: No Clear Home for Program Oversight

The 2013 survey shows that one-fifth of RM teams report to legal, slightly fewer to IT (17%), and 13% to business units directly. "Other" reporting relationships comprise 38% of survey responses.

Regardless of where RM professionals sit in the company organization chart, most enterprises have more than one key executive providing sponsorship of the RM program. Nearly half have the general counsel or other most-senior legal officer as a key sponsor, followed by the chief information officer/chief technology officer or other most-senior IT executive (39%). Chief executive and financial/administrative officers are the next most-highly represented roles, at 25% and 22%, respectively.

An executive or steering committee provides program sponsorship for 38% of respondents' organizations. In a postitive sign, only 6% of respondents report that they have no C-level sponsorship for their RM programs. (See Figure 1.)

Figure 1: Sponsors for RM Programs

Integrity: People, Systems Stymie Consistency

The Principle of Integrity describes how RM and IG programs must demonstrate consistent adherence to approved policies and procedures in order to establish the reliability and authenticity of information. People who engage with records must be given training on systems and appropriate practices, and the technologies used to control information need to be reliable. People and systems are core to establishing the Principle of Integrity.

The survey asked respondents to identify the top RM challenges in their organizations. The most pervasive issues pertain to either people (staffing and skills development, user adoption, or stakeholder alignment) or systems (limitations presented by current technologies). (See Figure 2.)

People Challenges

Difficulty in hiring or developing in-house expertise, lack of stakeholder alignment, and inconsistent classification by end users are the top three challenges that involve people. IG programs need to have input and guidance from IT, legal, compliance, and business unit leaders, yet this coordination of priorities is perceived as difficult

for about two-thirds of the survey respondents.

RM teams are scrambling to find the right mix of skills and knowledge to move their programs forward, and end users are struggling to consistently classify their business records. These challenges may indicate that training programs are insufficient, commitment to employee development is low, or current applications are overly complicated.

Systems Challenges

Top challenges with systems and technologies include limited integration capabilities with other systems and an inability to capture a broader range of information types. The inability for RM systems to integrate with other enterprise applications or capture new and emerging information types means that the RM system may be incomplete or that items generated in different formats are left out of the information life cycle or handled inconsistently.

Protection: Not Comfortable with Cloud…Yet

The Principle of Protection helps ensure that sensitive information is guarded against inappropriate disclosure or leakage and that essential records are available as part of business continuity.

Overall, security and privacy concerns present less of a problem to RM professionals than other challenges. Satisfaction with how current RM systems address privacy requirements is solid. More than half (55%) of respondents indicated they are fine with how their applications handle privacy requirements, including for confidential or personal information.

Comfort with protecting confidential information, however, has not yet translated into using cloud-based RM systems. Only 10% of survey respondents have adopted a cloud or software as a service (SaaS)-based RM solution (up marginally from 8% in 2012). Nearly one-fifth (18%) are planning to adopt cloud-based RM in the future, but a resounding 64% have no adoption plans at all. The top reason for low interest in cloud RM, at 58%, is "potential privacy or security concerns," followed by "policies, regulations or laws prevent this approach" at 25%.

Compliance: Low Confidence in ESI Drives IT Needs

The Principle of Compliance helps organizations ensure that an IG or RM program is designed to comply with applicable laws and abide by internal policies and other relevant authorities.

Confidence in meeting compliance obligations has been somewhat steady year over year, with approximately one-fifth of respondents continuing to report "high confidence" when asked, "How confident are you that, if challenged, your organization could demonstrate that your electronically stored information is accurate, accessible, and trustworthy?"

Of the 2013 survey participants, 41% reported some level of confidence that they could defend their information if challenged, with 26% – more than a quarter – reporting low or no confidence. (See Figure 3.)

E-Discovery Compliance

Compliance with discovery orders issued by auditors, regulators, or legal counsel is also an important issue for survey respondents. Just over two-thirds (68%) report that it is important that their RM solution providers support capabilities to meet the collection, review, and other activities in an e-discovery process.

Standards Compliance

Compliance of RM applications with functional standards also continues to shape product selection. Nearly one-third (32%) of respondents say it is "very important" or "extremely important" for their product to meet the U.S. federal government's DoD 5015.2-STD *Design Criteria Standard for Electronic Records Management Software Applications*.

Figure 2: Top-10 RM Program Challenges

NAIDing

There's more to paper and electronics destruction than simply feeding material into a machine. Policies, procedures, access control, employee screening, regulatory compliance, contracts and indemnification are all important.

Don't shred discarded sensitive material, ***NAID 'em.***

You'd be crazy not to!

www.naidem.org

Other global standards are rated substantially lower, with *Model Requirements for the Management of Electronic Records* (MoReq), International Council on Archives' *Principles and Functional Requirements for Records in Electronic Office Environments* (ICA Module 2), and the Victorian Electronic Records Strategy (VERS) considered essential by 17%, 12%, and 10% respectively

.

Availability: Search OK, Preservation Doubtful

The Principle of Availability outlines how an IG program should ensure timely and accurate retrieval of information to meet the needs of business users, as well as the RM team.

Search

Survey respondents are relatively satisfied with the search capabilities in their current systems. Search concerns don't even crack the top 10 list of RM program challenges, as described in Figure 2.

Long-Term Preservation

This principle also addresses the requirement to protect information over long periods of time to ensure it can be retrieved, as well as migrated to sustain on-going accessibility.

When asked how confident they were that records could be retrieved in 15 years, 15% of survey respondents indicated a high degree of confidence, with 42% claiming some level of confidence. 25% expressed a lack of confidence in their ability to retrieve this historical information.

Well-designed storage systems are important to meet availability requirements. Nearly half (46%) of survey participants reported that they either make or influence decisions about storage systems for RM applications, such as tape, disk, optical, or servers.

Furthermore, 60% of respondents indicated that RM stakeholders are included as part of IT strategic planning in their organization, including selection of vendors and requirements definition – a figure that has remained relatively flat over the past five years' surveys.

Deeper alignment with IT is required if RM professionals want to overcome the challenge of better content capture and easier integration with other business systems. (See Figure 2.)

Retention: Buckets Shrinking, Content Overlooked

The Principles of Retention and Disposition outline how, why, and for how long an organization keeps information and how it should be destroyed or handed over to an external custodian after a designated period of time. Balancing the retention and disposition needs from stakeholders, such as legal, business, IT, and even institutional historians or knowledge managers, can be a complex undertaking.

Records managers take the lead in this activity, with more than 90% of survey respondents indicating a high degree of involvement in setting retention policies. The next two largest groups of participants include corporate legal at 53% and business managers at 41%. IT, compliance officers, and external consultants/technology vendors follow at 29%, 27%, and 28% respectively.

Despite this broad set of participants, getting retention schedules established or approved is still identified as a top challenge for more than half of respondents. (See Figure 2.)

Big Bucket Schedules

The number of retention policies varies from organization to organization – reflecting the move by early adopters to a "big bucket" approach to RM – a specific effort to flatten, simplify, and reduce the number of retention policies to take advantage of electronic systems and leave behind the complex set of policies that originated in the world of paper. Nearly one-fourth (22%) of respondents still have more than 150 retention policies, while 34% claim fewer than 10.

Surprisingly, this trend to fewer retention policies appears to be reversing itself. In the 2011 survey, when this question was last asked, 15% of organizations had

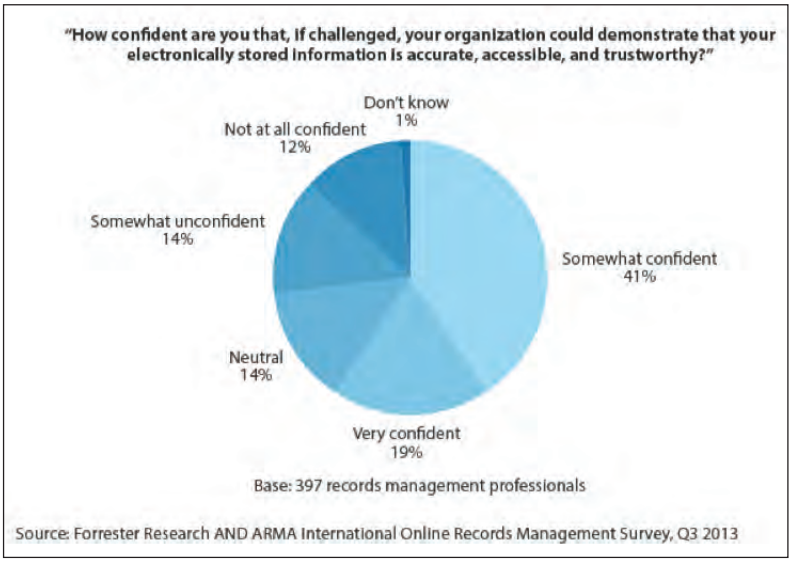


Figure 3: Confidence in ESI Trustworthiness

more than 150 retention policies, with 50% reporting fewer than 10.

New Content Types

RM decision makers are also looking at technology in an effort to manage retention for a broader set of formats and content types. IG strategies should be format-neutral, though many RM programs either ignore or struggle to capture and manage newer digital content types.

Content from social media/collaboration sites, cloud-based file-sharing systems, and instant message systems is of the lowest interest to RM professionals when implementing technology to manage retention. The risk of not managing the retention for these emerging content types must be carefully assessed, particularly in regulated industries. The viral nature and fast rise of social media, enterprise social networks, and SaaS document-sharing applications mean many potential business records could go unmanaged.

Disposition: IT Partnership Needed

The companion to the Principle of Retention – the Principle of Disposition – is essential not only for reducing the risk of retrieving obsolete, irrelevant, or inaccurate information, but also for keeping storage and overhead costs in check. Here, a partnership with IT to ensure consistent execution of electronic records ready for disposal is performed in line with laws, policies, or regulations.

Nearly one-third of records managers, however, are unsure about the volume of electronic records under their control; 32% of survey respondents selected "Don't Know" when asked what volume of content their RM applications are managing. This is only marginally better than the 36% who chose this response when the question was last asked in 2010.

RM and IG vendors are beginning to add intuitive dashboards, helping their RM users get more insights into storage metrics and capacity planning, make informed decisions on changes to retention policies with "what-if" modeling, and forecast costs and disk requirements. These data points can be valuable when planning for technology acquisition and rollout or making a case for enhanced budget or personnel.

Transparency: Budgets, Rollout Plans Often Opaque

The Principle of Transparency describes how an organization's IG program should be documented in an open manner, demonstrating the recordkeeping policies, procedures, and implementation activities.

Transparency and open communication about new technology rollouts, changes to procedures or systems, and what is expected of end-users and business stakeholders are important parts of a communication strategy and change management.

The resources available for system deployment, however, appear to be an area of the unknown for survey respondents, as 35% selected "Don't Know" when asked how much is budgeted for RM software acquisition in 2014. (This, however, is an improvement from the 43% that selected the same response when this question was last asked in 2011.)

Nearly one-third (29%) of 2013 respondents say they have no budget or less than $50,000 for technology rollout in 2014. Despite the high percentage of respondents who either have a small budget or do not know what their budget is, an optimistic 64% of respondents said they expect to expand or roll out new RM products in the coming year – the highest percentage of affirmative answers in the survey's five years.

This shows that RM professionals must become more deeply versed in the budgeting cycle and resource planning and be confident that any planned rollouts are adequately funded, staffed, and communicated internally.

Areas of richest opportunity include deepening the relationship with IT.

Opportunities for Growth

As RM professionals become familiar with the Principles, they have an opportunity to set benchmarks and success metrics and begin to measure their contribution to both the top and bottom lines within their organizations. The next step is action.

As IG concepts help propel the RM profession into its next level of maturity, areas of richest opportunity include deepening the relationship with IT to get a strong grasp on storage, technology roadmaps, and software budgets.

Opportunity is also present in aligning with the often-changing demands of business users as new forms of electronic communication and content are generated in cloud, mobile, and social applications. Tuning or updating incumbent RM systems to encourage better user adoption and consistency of classification and to integrate more easily into a broader set of record-generating applications are all considerations when planning an RM roadmap. **END**

Cheryl McKinnon is a principal analyst at Forrester Research. She can be reached at cmckinnon@forrester.com. *See her bio on page 47.*

Risky Business

Choosing Information Service Providers

Robert Johnson

Organizations seeking service providers that will handle their corporate information must ensure the providers' ability to comply with a variety of regulatory requirements and industry standards for protecting it – or leave themselves open to legal liability, public embarrassment, or financial ruin if that information is compromised.

There is liability inherent in selecting any service provider, whether for landscaping the campus or cleaning the office. Mitigating such liabilities usually falls to the purchasing or contracting department or to a firm hired to handle procurement and contracting.

But, there is one type of service provider that every organization must scrutinize more closely: information-related vendors, such as records storage firms, billing services, imaging services, IT asset management firms, and data disposal contractors. Following are important criteria to evaluate when selecting a service provider in this category.

Regulatory Requirements

Data protection laws around the globe apply to selecting data-related vendors, including these U.S., Canadian, and EU regulations.

HIPAA, GLB

The grandfathers of these U.S. laws are the Health Insurance Portability and Accountability Act (HIPAA) and the Financial Services Modernization Act, which is more commonly referred to as Gramm-Leach-Bliley (GLB). The former law applies to medical information and the latter to personal financial data.

Ironically, neither is a data protection law at heart; they both deal with a wide range of issues surrounding the explosion of electronic data, and GLB concerns issues as eclectic as interstate banking and co-mingling of banking, equities, and insurance by financial institutions. Still, they both include meaningful and specific provisions on data protection.

A quote on the U.S. Department of Health and Human Services' (HHS) website speaks to an organization's due diligence burden:

> The [HIPAA] Privacy Rule requires that a covered entity obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity.

In this context, the "covered entity" is the information owner, or the organization for whom the information is being handled. The "business associate" is the service provider.

A defense for this provision can be found in *Proposed Modifications to HIPAA under HITECH*, a 2010 HHS publication that provides early implementation advice.

> …The covered entity remains liable for the acts of its business associate agents, regardless of whether the covered entity has a compliant business associate agreement in place. This change is necessary to ensure, where the covered entity has contracted out a particular obligation under the HIPAA rules, that the covered entity remains liable for the failure of its business associate to perform that obligation on the covered entity's behalf.

Further evidence is less direct but also telling. Under the new breach notification requirements, the service provider must notify only the information owner that a breach has occurred.

If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any information required to be provided by the covered entity in its notification to affected individuals.

While the service provider *could* be held responsible for the HIPAA violation that caused a breach, it is apparent the information owner would bear the liability and cost to perform the actual notification of individuals, media, and regulators, as well as bear the public embarrassment.

In the financial sector, there are a number of similar examples indicating the information owner's responsibility for validating the data-related service provider's qualifications. Within GLB, data security regulations are contained in the Safeguards Rule.

As quoted specifically from the *Federal Register* (Vol. 67, No. 100), "[T]he Safeguards Rule covers any financial institution that is handling "customer information" – i.e.,

Selection Criteria for Information Service Providers

Protect your organization by choosing information service providers that:

- Demonstrate compliance with regulatory requirements (e.g., U.S. HIPAA, Gramm-Leach-Bliley, FACTA; Canada's PIPEDA; other countries' privacy acts and directives)
- Screen potential employees for criminal backgrounds and substance abuse, and to verify previous employment and experience
- Train and verify employee training on information-handling policies and procedures
- Disclose subcontractors
- Agree to return or destroy informations at the end of the engagement

not only financial institutions that collect nonpublic personal information from their own customers."

It further explains the financial institution's responsibility for service provider selection:

> (d) Oversee service providers, by: (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and (2) Requiring your service providers by contract to implement and maintain such safeguards.

FACTA, IRS Pub 1075, PCIDSS

If HIPAA and GLB represent the first generation of meaningful data protection regulations in the United States, the Fair and Accurate Credit Transaction Act (FACTA) Final Disposal Rule represents the second generation. The FACTA Final Disposal Rule, one of 19 FACTA provisions, was enacted on June 1, 2005. It and the Red Flags Rule – which requires many organizations to implement a program that identifies the warning signs, or "red flags," that indicate possible identity theft in their daily operations – are the only two provisions dealing with data protection.

The Final Disposal Rule requires the destruction of all discarded "consumer information," as defined by the law. During the rulemaking, the U.S. Federal Trade Commission (FTC) was concerned that the new law – the first national law specifically requiring the destruction of discarded data – would lead to a proliferation of unqualified vendors attracted to a new demand for destruction services.

From the *Federal Register* (Vol. 69, No. 235), here is how the FTC addressed the specifics of performing due diligence when selecting such providers:

> After due diligence, entering into and monitoring compliance with a contract with another party engaged in the business of record destruction to dispose of material, specifically identified as consumer information, in a manner consistent with this rule. In this context, due diligence could include reviewing an independent audit of the disposal company's operations and/or its compliance with this rule, obtaining information about the disposal company from several references or other reliable sources, requiring that the disposal company be certified by a recognized trade association or similar third party, reviewing and evaluating the disposal company's information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the potential disposal company.

So, while references to service provider selection due diligence in HIPAA and GLB apply to all data-related service providers and the FACTA Final Disposal Rule refers specifically to data destruction firms, each clearly indicates the expectation of the information owner for demonstrating care in its selection of vendors.

And it doesn't stop there. Other standards, such as Internal Revenue Service *Publication 1075* and the Payment Card Industry Data Security Standards, clearly define a similar responsibility.

Global Requirements

The responsibility is not confined to the United States. The European Data Protection Directive, Canada's Personal Information Protection and Electronic Document Act (PIPEDA), Australia's Privacy Act, and other data protection laws and guidelines either specify or refer to the same requirements.

Of course, it would be difficult to justify any other approach to selecting such service providers. Individuals are entrusting their information based on assurances given by the information owner and the regulations. It would be completely antithetical to the intent of those regulations – and illogical – not to hold those information owners responsible for demonstrating care in selecting downstream service providers who will touch the same information.

THE HARSH REALITY OF DOCUMENT SCANNING

PREPARING DOCUMENTS FOR SCANNING IS COSTLY, TEDIOUS, AND TIME-CONSUMING.

UNTIL NOW.

With OPEX prep-reducing scanners, we're taking the work out of document imaging. While many companies focus on faster scanners, we create smarter solutions that make it possible to scan even the most challenging documents with little or no document preparation. Our technology brings new simplicity to an otherwise complex process – helping you reduce labor requirements, save money and enhance productivity.

VISIT US AT ARMA BOOTH 446

See how OPEX can help you find a better way.
opex.com/HarshReality

OPEX® CORPORATION

If those service providers are found obviously inadequate, no one would accept the information owner saying, "Oh well, they offered the lowest price" or "We liked their logo." Organizations finding themselves in such a position must be able to defend their decisions with documented vendor qualifications and selection criteria.

Due Diligence Requirements

The good news is the elements of information-related vendor qualifications and the selection process do not differ much across the spectrum of services that fit in that category. The major categories to be evaluated are:

- Employee screening and training
- Written policies and procedures
- Contracts/fiduciary warranties
- Certifications/third-party monitoring

Employee Screening, Training

With employee screening, two types of problems often arise: false claims and inadequate screening. Any service provider can claim it conducts employee screening, but it is critical to require proof. Periodic inspection of invoices from screening companies is a good way to get that proof without looking at each file.

Consider these additional screening-related questions for your service provider:

- Are criminal and substance abuse screening done only pre-employment or periodically?
- Are criminal background screens limited to a local police report, or are they also done at the county, state, and federal levels? (The latter is far more preferable.)
- Is past employment verified?
- Is a Social Security header check used to validate, as best as possible, past employment and residence? (This check helps identify applicants who are trying to hide something in their past.)

Employee training is also important to validate. This requires evaluating the policies and procedures that show training is required, identifying what the employee is trained to do, addressing how subcontractors are vetted, and verifying that regulatory issues, such as security breach notification and whistleblower assurances, are included.

Policies and Procedures

It is unlikely an information owner would be found non-compliant for failing to intensely evaluate a service provider's policies and procedures, and it remains to be seen how deeply the new, random HIPAA audits will probe. Regardless of the risk of non-compliance resulting from an outside audit, the absence of such policy scrutiny would certainly reflect poorly on any organization should it come to the attention of regulators – or plaintiffs' attorneys – after a data security breach involving a service provider.

The information owner must document the use of such subcontractors and its expectations for how they are vetted and contractually bound by its information-related service providers.

Contracts/Fiduciary Warranties

Vetting service provider contracts and fiduciary warranties is another important component of due diligence. While a full discussion of this issue is worthy of its own lengthy article, these are areas that are often overlooked or misunderstood:

- Disclosure on the use of subcontractors
- The destruction or return of sensitive information
- Employee awareness and acceptance of fiduciary responsibilities
- Indemnification expectations and limitations

Third-Party Involvement

Data-related vendors sometimes use subcontractors to fulfill their contractual obligations. At face value there is nothing wrong with this. A subcontractor could be used to transport materials or provide an intermediate or isolated service beyond the main operations of the primary contractor. Policymakers acknowledge this fact within the regulations.

The information owner must document the use of such subcontractors and its expectations for how they are vetted and contractually bound by its information-related service providers. It may not be reasonable to expect every subcontractor be named, depending on the scope of service and the information owner's comfort level. It is, however, only prudent to acknowledge contractually that they might be used and their expectations of these engagements.

Depending on the type of service it is providing, the subcontractor may end up in possession of the information owner's sensitive information. While this would not be an issue for a data destruction firm that is hired to make the information unrecoverable or unreadable, it would be for

A BETTER WAY

The document conversion market is growing as more companies are deciding to convert their paper to digital. More organizations are getting into the business of scanning archived records – often a natural extension of their offerings to clients.

This increased competition demands more aggressive bids that often result in tighter margins. As a result, every business is looking for ways to squeeze more waste out of the document conversion process and hopefully turn a profit. In addition, the best companies are constantly vying for fresh streams of income and new ways to add to their customer base. In order to be successful in this market, companies need to be resourceful and manage their costs more effectively than their competitors.

Service bureaus are always looking for new scanning projects across a wide range of industries. Therefore, the type of work processed constantly changes. Operations managers design jobs by calculating the most efficient way to prep documents, extract data, and determine document breaks on items that are usually difficult for the software to identify automatically.

There is a lot to consider when bidding for this work: The client's demand for superior image quality, numerous image settings, a multitude of index fields or document separator sheets, and tight service level agreements (SLAs) across a broad array of clients. Looming over all of these considerations is the question, "How much labor needs to be applied to this bid to meet those requirements and still turn a profit?"

Here's the harsh reality: Document prep labor is the most time-consuming, tedious, and often most expensive component of any scanning job.

Most service bureaus perform document prep as a separate step before scanning. Operators touch almost every page because they have to check for staples, paper clips, folded items, and post-it notes. Their goal is to create piles of paper that are clean enough to be auto-fed on their scanners. As needed, pieces are unfolded, flattened, repaired, taped onto larger sheets, and placed into auto-feed ready stacks.

Documents with meaningful color require special handling. Other pieces require photocopying, such as the front of every folder that contains a label with vital information, or that piece that just will not scan without tearing. Some sections demand heavy prep such as taping credit card receipts to full sheets of paper and center-aligning class registration cards on the pile so that they can be auto-fed. Moreover, document separator / index sheets need to be added, tracked, and then manually outsorted for re-use.

But what if there was a better way?

What if you could prep and scan as fast as or faster than your current prep-only rate?

There is a better way to handle the wide range of media described above and reduce or eliminate much of the document prep. It is simply not necessary to constantly tape small or odd-shaped items to full sheets, photocopy folders and fragile pieces, or manually flatten sheets before scanning.

What if you could eliminate most separator sheets, or your need to re-use them? There is a better way to handle document separation. Most separator sheets can be eliminated by using the physical characteristics of a piece or by deploying electronic intervention, based on the requirements of each project, in line with the scanning process. Generic separator sheets are easily re-used by automatically outsorting them.

What if you could improve image quality, adjust image capture settings, and decrease re-scans by optimizing exception items during scanning? There is a better way. By defining page types via software, operators can apply different settings on each image (i.e."snippets"), and capture them quickly and easily.

There is a better way, and we'll always help you find it.

OPEX Corporation knows efficiency. Over the years, we have developed innovative products that address the root causes of the workflow issues our customers face. We strive to understand and solve those issues by designing the best products to meet those challenges rather than simply addressing the symptoms.

This market-driven approach, coupled with unparalleled service and excellent ROI, form the backbone of our long-term customer relationships. We continuously look for ways we can team with third-party integrators and software vendors to provide our clients with complete solutions.

As a result of these efforts, OPEX offers various prep-reducing scanners, including the DS2200 and AS7200 models, that provide you with attractive business opportunities and the flexibility to:

- Identify and aggressively bid projects with more challenging paper, or more recurring-revenue transactional work (we have thousands of scanners in the field capturing transactional documents);
- Decrease prep headcount, or increase output using the same number of people; and
- Increase your profit margin.

OPEX CORPORATION

Learn more at www.opex.com/harshreality

a scanning firm, a records storage firm, and a host of other service providers.

While no current data protection regulation requires the service provider to indemnify the information owner for loss of any type, the information owner has every right to ask for it.

Contract Requirements

Contracts with information service providers should address several issues, as follows.

Disposition of Information

Contracts should specifically detail the fate of the information that resides with the subcontractor when it is no longer needed. In fact, this provision could easily be justified when dealing with any vendor that will possess the organization's client, employee, or competitive data.

The options are to have the information destroyed, which brings up the issue of subcontractor requirements, or to be returned. Either way, expectations and agreements on its fate must be detailed. Typically, if they are mentioned, the requirements are so loosely worded as to be of little value should the information owner need to hold the vendor accountable in the future.

Employee Training

According to the eighth annual *Ponemon Global Cost of a Data Breach* study, employee error was the leading cause of data breaches in 2012. This finding applies to service providers to the same extent as the information owners. While policies and training are critical in mitigating such risks, it is also important that employees accept that they are exposed to sensitive data. They must acknowledge their responsibility to protect it at all times and make management aware of potential security breaches.

Recent amendments to HIPAA set a precedent for holding individual employees legally responsible for breaches they knowingly cause. No employee of a service provider should ever be able to seek refuge in the fact that he was unaware of his responsibilities or the nature of the information he was entrusted with. Contractually, service providers should be required to obtain such fiduciary employee acknowledgements.

Liability, Indemnification

The final service provider contract issue to discuss is fraught with misconceptions: vendor liability and indemnification. While no current data protection regulation requires the service provider to indemnify the information owner for loss of any type, the information owner has every right to ask for it.

A common professional indemnification mistake made by information owners is to require their vendors to accept such liability but then fail to confirm if they have enough coverage. A second common mistake is requiring unreasonable or unrecoverable indemnification limits.

It will surprise no one that professional liability is becoming a staple of data-related vendor contracts, but what is surprising is there's often no requirement to *confirm* the service provider has coverage. Sometimes general liability coverage is mistakenly accepted, and other times the professional liability policy supporting vendors is an off-the-shelf policy so riddled with exclusions that it would be useless in protecting the vendor or the information owner.

These mistakes are often exacerbated by service contracts that require the vendor to accept unlimited liability. There is no such thing as professional liability coverage with unspecified limits. Essentially, the information owner is asking the service provider to put its entire enterprise on the line.

Because aggressive restrictions and irrational fiscal requirements are typically tossed out by the courts, it's best to agree on a reasonable indemnification limit that's based on the mutual risks and the amount of business transacted. No information owner is likely to collect on a professional liability claim beyond what the vendor is covered for, and even then only if the policy is appropriately vetted.

Trust, but Verify

Most of us are trustworthy and are eager to be trusting as well. Unfortunately, when it comes to service providers' claims and promises, we can be too eager to trust. There will always be some vendors who have credible-looking websites, who know the jargon and the hot buttons, and who offer temptingly low prices. That's why regulatory compliance requires, and common sense dictates, that information owners make reasonable attempts to look deeper and to test the service providers' assertions. **END**

Robert (Bob) Johnson is the chief executive officer for the National Association for Information Destruction. He can be reached at rjohnson@naidonline.org. *See his bio on page 47.*

Log It or Get Fined!

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

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

Our Books Cost 10-40% Less than Competitors

Quality construction that lasts and stands up to regulatory scrutiny

Sample Log Book Titles We Make:

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

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

Visit www.bookfactory.com/arma

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

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

BookFactory®

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

Call us today for a free sample:

1-877-431-BOOK

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

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**

ICRM®
Institute of Certified Records Managers

The Trusted Information Payoff: Productivity, Performance, and Profits

Building an information framework to ensure effective data management produces information that is true, has integrity, and can be trusted. This leads to a continuous improvement culture that can increase employee productivity, improve operational performance, and grow profitability.

Karim N. Sidi and Dale A. Hutchinson

Large organizations, especially those that have grown through consolidation, mergers, and acquisitions, are often fraught with incompatible systems and data sources that are costly and difficult to manage. The systems usually do not avail efficient extraction, aggregation, and sharing of data within or across the boundaries of the business process.

To address this problem, organizations can turn to an information management framework that facilitates managing raw data to create useful information that can be shared across the organization.

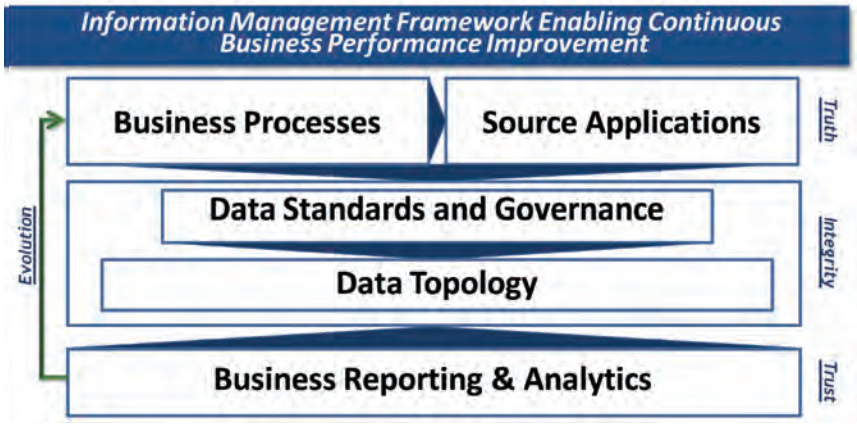


Figure 1: IM Framework for Continuous Business Performance Improvement

The IM Framework

An effective IM framework treats data as an asset, applying the same methodologies as for any other intellectual asset. As shown in Figure 1, the IM framework needs to address the following elements of data:

- *Truth* – It must maintain the consistency of meaning and common understanding throughout the organization. In data management, this is about ensuring through business processes and IT applications that the data element's meaning, consistency, and understanding do not change even though its format and storage topology may change to standardize and centralize the access.
- *Integrity* – The IM framework must enforce the truth through standards and governance.
- *Trust* – Trust is about consistency, reliability, and quality, which result from defined rules for standardization that are enforced through active governance.
- *Evolution* – The IM framework must have a process of continuous improvement to increase the value of the information.

These elements are described further below.

Truth: Data Standards Required

The holy grail of data management is to identify the single version of the truth. This could be defined as it was in the 2008 Oracle Thought Leadership White Paper "The Myth of One Version of Truth" as "a single set of reports and definitions for all business terms, a way, in short, to make sure every manager has a common understanding of accurate corporate information."

It is a great challenge for distributed systems in an IT architecture to find a common meaning and data type definition for common data elements. For example, as John Schmidt wrote in the June 12, 2012, *Informatica* blog "Perspectives," "Multiple versions of the truth are often a result of the same information being captured and stored in slightly different ways by different systems."

Because data type definitions determine how a database stores information, there will be problems if the date on one application is defined as an integer (e.g., 20130414) while on another application it is defined as a string of characters (e.g., 04/14/2013).

As another example, consider the problem that occurs if one system of record uses the entry date as the date of transaction and another system uses the posting date. Which is the correct transaction date?

Often, enterprise applications consist of a mix of home-grown, function-specific applications and third-party systems built by disconnected teams without a shared reference for data definition. The solution – forethought and planning to create well-defined data standards – may appear obvious from an architectural perspective but may not be so easy to accomplish. The steps described below will help.

Establish Processes, Rules, Policies

Identifying the "truth" first and foremost requires that business processes, rules, and policies be clearly defined, shared, and understood inside and outside the organization. Metrics and audit checkpoints must be established to monitor the processes for accuracy and consistency.

Map Data Flows

The next step is to map the data flow from the source applications to define the required flow from one process step to the next so the organization's data needs are well understood.

The single version of truth can then define a common understanding of the data, one that's accepted across operational boundaries.

Use ETL Tools

Having a documented definition for the information – that is, a data standard – then enables the enterprise to properly integrate third-party and legacy applications into the organizational IT infrastructure using appropriate Extract Transform and Load (ETL) tools. These tools extract data from a source system, transform the data to change its format, and load this transformed data into a different database.

ETL tools are used for many functions, such as automating the cleaning of data to improve its quality, performing validation, and integrating data from multiple source systems into a single database to increase the depth of the information.

Integrity: Collaboration with IT Required

Data without integrity – that is not complete, accurate, and consistent – is not very useful. Standards and governance rules provide a disciplined approach to managing business processes and source applications, reinforcing the "truth" and enabling the seamless sharing of data.

Developing a standards and governance infrastructure requires a partnership between business and technology subject matter experts (SMEs). The SMEs must be empowered to develop an understanding of the organization's *data topology* – which describes the hierarchy of the storage architecture from primary data sources to data warehouses – and its tactical and strategic information needs. (See Figure 2.)

Developing Data Models

Standards enable the development of *entity relationship models* (ERMs), which are business models that abstract the data definition from the database system's design. ERMs build consistency in data meaning and optimize data structures for storage, retrieval, and exchange.

The attributes that form the basis of a data model for any business application are the processes, the people working those processes, and the products or services that are acted upon to create a customer experience.

Consider this example of a customer relationship management application. The ERM defines the business needs to capture specific information, such as the customer's name, the company's name, and the customer's address, phone number, e-mail address, and purchase history. This data is independent of how it may be collected and stored in a database.

A data model for a particular platform and database then defines how an application would be implemented and the format in which the above information would be stored.

Implementing data standards and governance leads to good data quality, as shown in Fisgure 3. **Data standards**, which encapsulate the collective knowledge of the SME team, are used to create business and **technical application data models** for the information framework. These models meet the business needs and provide criteria for a minimum level of data availability and inter-system compatibility, as well as storage, retrieval, and exchange needs.

With a documented data standard, new application development teams have a reference source that influences the data model for the software applications being designed.

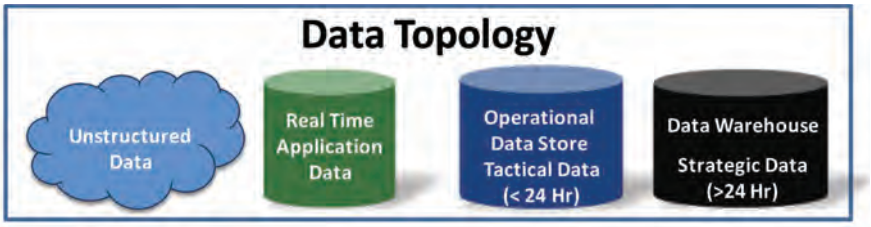


Figure 2: Data Topology

Figure 3: How Data Standards and Governance Lead to Data Quality

Governance rules establish audit checkpoints to ensure ongoing conformance. They also assign IT the responsibility to enforce data format rules and the organization to enforce the meaning and timing of the data.

The governance rules should also include managing and enforcing **data quality**, a fundamental challenge in many source systems. Data quality should be managed using a combination of manual and automated systemic audit procedures and corrective actions.

Using Data Repositories

Understanding the data topology is an essential part of the information framework. As shown in Figure 2, there are four types of data repositories in the information framework that are necessary to perform specific value-added functions:

- The *unstructured data* repository facilitates the storage of unstructured data, such as open-ended comments on social media and other internal and external sources. This component can also address the transformation, validation, and corroboration functions that may be needed to make the unstructured information "trusted."
- *Real-time application data* comes from applications supporting a business process. This current-state information on business processing may provide inputs for real-time dashboards or aid real-time decision making.
- *Tactical data* is information that is not more than 24 hours old. This is processing information that is used for intra-day operational reporting and supporting tactical decision making. It should be stored in an operational data store that aggregates multi-system real-time data to provide a richer

Figure 4: Reporting and Analytics

information base for improved tactical management.

- *Strategic data* is historical – from 24 hours up to several years old. It is stored in a *data warehouse* and used to study trends in revenue, production, and human resources and to improve business processing. It can provide significant information to aid strategic decision making, be a valuable source to simulate "what if" scenarios, and be used to identify and rate performance improvement opportunities by effort and value. Strategic data can also provide insight into structural issues that may affect competitiveness and sustainability. ETL tools can address the issue of standardizing legacy systems' data and integrating third-party systems into the enterprise architecture, thereby creating a seamless data exchange across business functions and process boundaries.

Trust: Standards, Governance Foundation Required

Trust in the data comes with its consistency, reliability, and accuracy, especially when built upon a foundation of data standards and governance for known business processes and application sources that enable "trusted" analytics to provide ongoing value-based information.

As shown in Figure 4, the right IM framework will not only provide the flexibility of generating standard operational reports, such as scorecards and dashboards, it can also support *ad hoc* reports, planning, forecasting, and a wide spectrum of analytics with varying degrees of complexity.

Evolution: Ongoing Investment Required

Effective and sustained data management is an evolutionary process requiring the organization to make regular structured investments in improvements to the infrastructure to enhance the quality and value of the information that is derived.

Once "truth," "integrity," and "trust," have been established, a continuous improvement culture can expand the ecosystem to improve the quality of business reporting and analytics. This advance can be leveraged to improve business processes, execution, and decision making and to gain efficiencies through process optimization and cost reduction. Further, the output of the reports and analytics can also evolve and improve the IM framework, which would lead to additional improvements in business performance management.

Organizational leadership must understand that a good IM strategy requires significant initial investment and may not deliver short-term benefits. It should be viewed as a long-term initiative and nurtured through the levels of maturity to deliver sustainable results. Performance improvements should be tracked through such metrics as costs, benefits, and efficiencies to ensure that investments in the data infrastructure are delivering the desired results.

A common point of failure in many organizations is the intention of implementing an IM strategy but then falling short on the required follow-through due to changes in business conditions, leadership, or organizational priorities. Building this framework will require a well-planned and enduring commitment to investment in the right people, processes, and technologies.

Sound Fundamentals Lead to Strong Results

Effective data management does not require a "Mercedes" solution in the first attempt. Instead, it is better to build a framework with strong fundamentals and a standards-driven approach to governance that can be sustained through regular reviews. The framework must be able to leverage the available tools and software to continuously improve the systems and processes.

The payoff to an effective data management strategy is the value of the trusted information. This information can provide advantageous competitive insight, enable sophisticated business performance management, increase employee productivity and satisfaction, and deliver a superior customer experience.

The ultimate benefit will be visible in revenue growth, improved operational efficiency, increased customer and employee retention, and increased profitability. **END**

Karim N. Sidi consults with organizations to leverage technology for knowledge management strategies to improve operational efficiency, strategic performance, and quality of management decision making. He can be contacted at knsidi@gmail.com.

Dale A. Hutchinson is executive director of Business Information Services at one of the nation's leading financial services firm. He can be contacted at dalehutchinson111@gmail.com.

See their bios on page 47.

IRON MOUNTAIN®

INFORMATION IS...

A STORY

CONGRATULATIONS TO THE INAUGURAL CLASS OF CERTIFIED INFORMATION GOVERNANCE PROFESSIONALS!

Working in an ever-changing industry like information management requires constant education and evolution, and you've embraced both. Three new letters at the end of your signature (IGP) makes it plain that you are a strategic business partner - and someone who is doing what it takes to rule your world. We at Iron Mountain salute you!

IRONMOUNTAIN.COM/ARMA

ARMA 2013 | LAS VEGAS, NV | BOOTH 403 | OCTOBER 28-30

© 2013 Iron Mountain Incorporated. All rights reserved. Iron Mountain and the design of the mountain are registered trademarks of Iron Mountain Incorporated in the U.S. and other countries.

Extending the Principles to the Internet: A Way to Restore Trust

By Julie Gable, CRM, CDIA, FAI

Almost from its inception, the Internet has spawned thorny, complex issues that are not easily resolved. Matters such as online piracy of copyrighted material, theft of trade secrets, cybersecurity, and trans-border data transfer issues constantly confront governments, Internet service providers, businesses, individuals, and watchdog groups.

In recent weeks, the balance of personal privacy and the need for national security have been the subject of high-profile news coverage. With revelations about the U.S. National Security Administration's (NSA) electronic surveillance program called PRISM, the parallels of data mining for marketing purposes and for surveillance purposes came into sharp focus.

Technology has given us the ability to store vast amounts of data cheaply. Now, with highly sophisticated data analytics tools, it is possible to exploit stored personal data not only for more effective marketing, but also for more effective detection of potential security threats.

The key difference is that while users freely give personal information to social media sites, e-mail services, marketers, and other Internet presences, they don't necessarily suspect that this personal data can then be handed over to federal investigators. That's because many people don't realize that the background architecture for storing such data is the cloud.

A Battle in the Cloud

According to *The State of Cloud Storage 2013 Industry Report* from storage vendor Nasuni, cloud storage providers put more than one exabyte of information – that's more than 1 billion gigabytes – under contract in the previous year.

With surprising revelations about how large providers such as Amazon, Microsoft, and Google, have responded to federal warrants has come a public outcry. According to reports in *The New York Times*, some providers have had teams of in-house experts charged with finding ways to cooperate with the NSA, a strategy aimed to keep the information-mining process under the company's control rather than the federal agency's control.

Cloud service providers – and the companies that use them via Internet connections to provide flexible processing for transactions, communications, and storage – have suffered huge reputational damage. Internationally, some countries have exploited the NSA revelations to maintain that those who fear their communications are being intercepted should not use services that go through American servers.

In short, an atmosphere of deep mistrust has arisen that could prove damaging and costly to cloud service providers as well as to any entity that collects customer information in business-to-business or business-to-consumer transactions.

Principles Show Way Forward

Into this maelstrom steps Michael Geist, J.S.D., who believes that issues associated with cybermistrust are going to put pressure points on the Generally Accepted Recordkeeping Principles® (Principles) and extend them in ways

that people may not have been thinking about up to now.

Evaluating Service Providers

In addition to using the Principles to measure the effectiveness of in-house records programs, organizations may come to use them as a means to judge the information management maturity of their service providers. Going further, Geist believes the Principles and the Information Governance Maturity Model (Maturity Model) may also provide a template for devising solutions to restore trust.

Geist believes that companies offering cloud-based services – whether e-mail, social media, voice over Internet protocol, applications, or storage – will face some hard times in the wake of the U.S. surveillance scandals. Recent surveys have shown that U.S. cloud providers could lose as much as 20% of the international market for these services over the next three years.

Why? "Public trust is crucial for service providers," says Geist. "The providers were functioning in the hope that there wouldn't be a Snowden," he says, referring to NSA contract worker Edward Snowden, who leaked classified information about NSA surveillance activities.

Records and information managers will recognize this mind-set as similar to the one that believed (or wished) that electronic discovery would never be part of litigation and that a gentleman's agreement that implied "if you don't ask for our electronic records, we won't ask for yours" would prevail.

"Google's 'don't be evil' mantra is increasingly hard to reconcile," Geist contends, when, "as a service provider organization, it becomes difficult to promise your customer that their data isn't being disclosed to agencies that are actually collecting it with your knowledge and permission."

Michael Geist, J.S.D.: A Career Overview

Michael Geist, J.S.D., is a law professor at the University of Ottawa, where he holds the Canada Research Chair in Internet and E-commerce Law. He earned his doctorate in the science of law degree from Columbia Law School in New York.

Geist is an internationally syndicated columnist on technology law issues, has edited two books on Canadian copyright law, is the editor of several monthly technology law publications, and is the author of a popular blog on Internet and intellectual property law issues.

He serves on boards for CANARIE, the Canadian Legal Information Institute, the Privacy Commissioner of Canada, the Electronic Frontier Foundation, and the Open Society Institute. He has received numerous awards and recognition for his work in the areas of intellectual freedom, policy leadership, and public leadership.

Geist warns that "once the NSA has the information, the line up of other agencies that want to use it runs right out the door. Drug enforcement, copyright infringement, and other uses suddenly appear. The highest level national security purposes become a slippery slope of something far different."

Restoring Trust

According to Geist, the biggest collectors of personal information in the private sector are scrutinized by non-governmental organizations (NGOs) who bring citizen concerns to governments, advocate and monitor policies, and encourage political participation through provision of information.

One example is the Electronic Frontier Foundation. While NGOs may be the guardians of individual legal rights in a digital world, these watchdogs may not have the tools needed to measure good stewardship of information.

Principles to Apply

Geist offers, "It is useful to begin looking at what is important from the perspective of ARMA's Principles for recordkeeping performance and to see how Amazon, Google, Microsoft and other providers could be judged in terms of information governance maturity."

Transparency

The Principle of Transparency will be essential to restoring trust. According to Geist, "It will no longer be enough for these providers to say 'here's what we do,' but rather, 'here is what we have done.' Policies might include requiring a warrant for surveillance or law enforcement requests, telling users about government requests for data, publishing guidelines for law enforcement, and being ready to stand up and fight for their customers' privacy rights."

Geist is a proponent of transparency reports that disclose requests for user data and tell how the company has complied with these requests. "Up to now," he says, "most transparency has been about the processes involved with complying with data requests rather than with the actual actions themselves."

Geist believes that transparency reports foster public confidence in service providers. Steps will also

likely have to be taken to demonstrate that the provider functions at a transformational level of transparency, including a continuous improvement program to ensure that transparency is maintained over time.

referred to at level five of the Maturity Model, the idea that retention is perceived holistically and is applied to all information in the organization, not just to official records. Will consumers have the right to request that their data

"Businesses that are regulated and have a high priority on information security are under threat if they move to the cloud," Geist says.

Accountability

Accountability is another key element that has sometimes been lacking, particularly where the provider's stated goals related to accountability have not been met. "Greater oversight is a start," says Geist. "Many people think that accountability is not what it should be, particularly when elected officials are not told the truth. This means that NGOs – people invested in watching the watchers – are not able to do so."

Greater accountability would likely have to be at the board level to have a truly transformational effect. The Principles recommend a chief records or information governance officer who reports at the senior management level.

Retention

"Retention is another issue that is interesting," notes Geist. "The ongoing ping-ponging of 'how long a retention period is enough' will get new momentum. The longer data is kept, the more susceptible it is to breaches or to government requests."

This is the aspect of retention

is not kept very long? Will it be possible to actually comply with this request? The answers remain to be seen.

Protection

Protection for records and information that are private, confidential, privileged, or secret, of course, is a huge concern. While general businesses can have legal frameworks built on the privacy of their own systems, moving to the cloud provides another source of access with lower safeguards.

"Businesses that are regulated and have a high priority on information security are under threat if they move to the cloud," Geist says. "Cloud-based models are based on public confidence in the level of security in the cloud vs. the level of security on network servers. With the new revelations, cloud providers just can't make those claims anymore."

Clearly, there is much work to be done.

The Need to Collaborate

"Within normal businesses, the answer to security varies by

the type of business, the data collected, and the context in which it is used," says Geist. "National governments must insure that the Internet functions the way its users expect, and many countries work together on how to do this."

As a global phenomenon, the Internet transcends geographic borders but is not necessarily free of political or cultural restrictions. Following the scandals, some have questioned whether the US-led Internet Corporation for Assigned Names and Numbers, more often referred to as ICANN, should continue as the governing model for the Internet. A year ago, there was debate on whether a government-led, United Nations-style model that would include countries such as Russia and China should have control.

No doubt the line between national security and Internet freedom will continue to be debated. In a post-9/11 world, the emphasis has been on security rather than on privacy.

But Geist believes that the pendulum may swing back after Snowden, with Amazon, Google, and Microsoft becoming far more vocal and trying to build on public concern for more privacy.

Meanwhile, proposed laws, such as the U.S. Cyber Intelligence Sharing and Protection Act (CISPA), seek to allow more sharing of Internet traffic information between the U.S. government and technology companies.

How service companies deal with issues of balancing cybersecurity and Internet freedom going forward will be key. Geist contends that they will do best by confronting the issues and using the Principles to guide information governance policies. **END**

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

Vendors, Products & People

BULLETIN BOARD

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

XACT DATA DISCOVERY
Because you need to know

RSD
RSD recently announced information governance capabilities for Amazon Web Services S3. RSD GLASS® integrates with AWS S3, as well as existing on-premise repositories, to enforce corporate policies on all information – wherever it resides. Using RSD GLASS, organizations immediately turn cloud storage into a system of records and optimize storage costs without impacting how users access and retrieve documents. For more information, visit ***www.rsd.com/en/aws.***

ZASIO Versatile RFID Mobile RT™

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

Total Recall Records Management Software
DHS Worldwide, the global leader in records management software solutions, recently announced the latest release of Total Recall Records Management Software, version 7.0. The latest version of Total Recall gives records management professionals new and innovative tools to boost productivity. A special thanks to the Access conversion team and all of the Access employees for their hard work during the conversion process of all of the Access locations to Total Recall. We appreciate the ideas from the operations team during the training process—many of their great suggestions are found in this release. To find out more, visit ***www.dhsworldwide.com*** or call 904.213.0448.

TOTAL RECALL™ SOFTWARE
BY DHS WORLDWIDE

OPEX Corporation
The document conversion market is growing as more companies are deciding to convert their paper to digital. The harsh reality of document scanning is prep labor: it is the most time-consuming, tedious, and often the most expensive component of any scanning job. There is a better way to scan a wide range of media and reduce or eliminate much of the document prep. ***www.opex.com***

recall™
Your Information. Securely Managed.

Recall
As a global leader in information management, Recall is committed to providing the services you need across the full lifecycle of information management with the recent addition of our new service line, Information Governance Solutions. Through leading edge technologies, proven protocols, and top-notch information management expertise, Recall brings you the power of transformational information management.
www.recall.com/information-center/

Pursuing the Possibility of a Paperless Office

Anna Stratton, CDIA

There are many advantages to going paperless: electronic files allow better access and information sharing, cost less in terms of physical space and personnel, and can increase productivity – all of which add to the bottom line.

Why, then, have so few organizations fulfilled what many have set as a goal: a paperless environment? For many, it may be the cost – not only the cost of converting paper to electronic files, but also the cost some employees fear they will pay in giving up paper.

Understanding the People Problem

The irony is that these same people likely use smart phones and tablets to manage every aspect of their personal lives, embracing the ease of electronic transactions and the advantages of mobility. But the office is one area of their world where paper still works.

Although they use electronic documents in the office, they often don't manage them well. They have folder structures that go 10 deep, which made sense when created but are now the cause of carpal tunnel syndrome for all the clicks required to get to the needed documents.

So, they resort to saving their electronic documents to the desktop where they know they can find them – except soon their monitors become mirrors of chaos that make them long for those paper file folders. So, when they finally find the documents they want, they print them so they can finally get to work on what started their searches. For a single moment, they feel a sense of control and inner peace. It's no wonder they meet the idea of a paperless office with such resistance.

Getting to the Root of the Problem

In many organizations, the introduction of a new technology is not a good experience. Employees are frequently given access to it, but they are not provided training or a succinct model to follow. This leaves them feeling lost and frustrated.

Their questions about converting paper to digital files will likely include very fundamental ones: "What do I call it?" "Where do I store it?" "How do I access it later?" and "How is it secured?"

They may also be confused about compliance issues. They might ask: "Is the digital version a copy – or a record? If I destroy the paper, is the digital version now considered the original?"

Therefore, as organizations begin to talk about going paperless, employee paralysis may set in. This is natural. People often dig in their heels when they perceive that something is being taken from them. Some will cling tightly to their desire to keep paper just because they are told it is going away.

The need to understand, acknowledge, and address these responses is one of the most underestimated elements in implementing change. Involving staff in the investigative stage of such a project will help them buy into it. Work with them to identify how they use paper, and ask them to document their workflows. Give them "what if" scenarios that will help them understand whether these paper processes are valid or if they exist only because they have "always been done that way."

People also need time. Even the best plans will be easily undermined (or sabotaged) if people are not allowed time to adapt. In addition to providing sufficient transition time, education, and training on new processes and procedures, organizations must earn their employees' confidence by ensur-

ing that they can continue to be productive during the transition from a paper to a digital working environment.

Realizing that Technology Is a Tool, Not a Solution

Organizations that get past this initial resistance will have another hurdle if they begin looking for a technology "solution" before they have identified their unique needs for the paper scanning project. They need to realize that technology is a tool – not a solution. Document scanning, automated workflows, and cloud storage are all tools that may contribute to the paperless office solution, but that cannot be determined until an organization identifies its needs.

Identifying Needs

Despite the benefits of document scanning (for both current and back-file collections), organizations should not aim to go paperless in one shot. It is critical for them to evaluate what files, perhaps even what specific documents, will address their core objectives.

For example, an organization may determine that scanning executed contracts is the solution to their need to provide access to multiple users or for reducing resources dedicated to researching these contracts before executing new ones. For organizations that don't have those needs, scanning executed contracts may not be a good solution.

That is why it is important to bring all stakeholders into the needs analysis at its inception. This fosters a culture of informed decision-making, prevents lengthy and duplicative processes – including the need to "sell" the concept to some stakeholders after decisions have been made – and ensures alignment with high-level objectives.

Key Decision Points for Moving Toward a Paperless Office

Important factors for deciding to convert paper information to a digital format include whether it:

- Solves operational issues, such as providing access to multiple users or to remote users
- Allows the information to be used in innovative ways
- Provides opportunities for operational improvement and efficiencies
- Makes it less expensive to use and preserve during its projected life cycle
- Aligns with the Generally Accepted Recordkeeping Principles©

Determining the ROI

Organizations that are committed to continuous improvement understand the straight-line relationship between specific processes and their hard cost return on investment (ROI). But, analyzing the hard costs for converting paper to digital format is not as simple as comparing the cost of scanning a box of documents to the cost of storing it offsite. Several other factors need to be considered.

Hard Costs

In addition to determining the actual costs associated with converting paper documents to digital ones, organizations need to consider at what point in the paper's life cycle they intend to do the scanning. This is because as paper moves through its life cycle, it not only loses value, it also begins incurring hard costs for such activities as retrieving, re-filing, transporting, storing, and – for the majority of paper – destroying it. Clearly, scanning early in paper's life cycle reduces hard costs.

Organizations also need to consider how good their policies and procedures for managing paper records are. Their hard costs will be even higher if they do not have good policies or if they have high personnel turnover, as those factors can result in escalating, perpetual offsite storage bills. If no one is really sure what's in all those boxes, no one will want to pull the trigger to have it destroyed.

Soft Costs

Some organizations fail to consider the soft costs involving resources. Add sections to the analysis that include a reasonable estimate of intangibles, including workflow efficiencies and the benefits of electronic formats for worker mobility, disaster recovery, and security.

Other Considerations

Organizations should not approach document conversion as a "scan it all or do nothing" decision. In fact, the best decision may be to focus the ROI analysis on smaller projects that will stop the growth of paper or address large collections of legacy paper.

Factors to consider for inactive documents. For example, by scanning inactive documents that have a long (or permanent) retention requirement, not only will the cost

of storing, retrieving, and returning the paper be eliminated, but the information will be much more accessible and usable.

On the other hand, scanning inactive documents that are close to their disposition date may have little value, especially if key data was captured in the creation stage.

Factors to consider for active documents. For organizations that need time to prepare for change, implement tools, and provide training on managing electronic documents, keeping paper during the active part of its life cycle may make the most sense.

Other lifecycle factors to consider. Organizations must also remember to determine the value of converting paper at each of the stages of its life cycle to identify the true ROI. This also will help them determine whether they should begin their paperless office project with their legacy information or work on a day-forward basis.

Coming Down from the Cloud

Records and information management (RIM) professionals have made their way out of the basement. To find answers for dealing with information being created by social media, instant messaging, and e-mail, many have made the leap to the clouds. For some, though, that has meant neglecting their organization's years of legacy information that doesn't have wings.

Meanwhile, employees are doing everything they can to hold on to what they know – in this case, paper – so they can do what they need to do. Paper isn't going away for quite a while, and RIM professionals need to be okay with that. People need information in whatever ways allow them to be efficient.

But, RIM professionals also need to be fiscally responsible, and dealing with paper – both legacy and active – by converting some to digital files may be the most fiscally responsible thing to do. For them, developing and implementing plans that make sense for the way business needs to be done and allowing paper that is created or received to be used, scanned at some point, and then shredded allow all stakeholders to be satisfied. **END**

Anna Stratton, CDIA, is a records and information management professionall withh 22 years of experience. She can be contacted at annastratton@mac.com. *See her bio on page 47.*

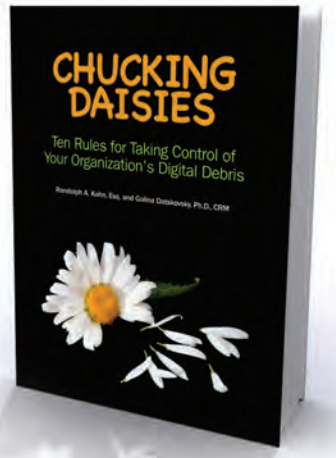
ARMA INTERNATIONAL

New!

Chucking Daisies

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

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



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

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

Available now! ARMA INTERNATIONAL **BOOKSTORE**

Contact Information

AUTHOR INFO

GABLE HUTCHINSON JOHNSON MCKINNON SIDI STRATTON

Propelling the Profession (and the Professional) to the Next Level Page 20

Cheryl McKinnon, IGP, is a principal analyst at Forrester Research, covering enterprise content management (ECM), records management, information governance, and e-discovery. As a certified Information Governance Professional, she brings a broad perspective to this role, with deep experience in many areas, including ECM, social media, collaboration, and standards. Previously, she founded Candy Strategies Inc., where she provided advisory services to public and private sector clients, was vice president of marketing for AIIM, chief marketing officer of Nuxeo, and a senior manager with OpenText and Hummingbird.She can be reached at c*mckinnon@forrester.com*.

Risky Business: Choosing Information Service Providers Page 26

Robert (Bob) Johnson is the chief executive officer of the National Association for Information Destruction (NAID), the non-profit secure destruction industry watchdog organization he founded in 1994. He speaks and writes internationally on a wide range of issues related to data protection legislation, policy and compliance issues, and vendor selection criteria. In addition, Johnson is frequently sought out by policy makers around the world for guidance on data protection issues. He can be reached at *rjohnson@naidonline.org*.

The Trusted Information Payoff: Productivity, Performance, and Profits Page 35

Karim N. Sidi consults with organizations to leverage technology for knowledge management strategies to improve operational efficiency, strategic performance, and quality of management decision making. His more than 18 years of experience in IT and data science includes projects in business analysis, predictive modelling, dynamic capacity allocation, and data-driven process control and optimization. He can be contacted at *knsidi@gmail.com*.

Dale A. Hutchinson is executive director of business information services at one of the nation's leading financial services firm. He has a BA in Management Information Systems with more than 20 years of experience in developing enterprise data warehouse and information management solutions and delivering strategic decision support to improve business effectiveness and efficiencies. He can be contacted at *dalehutchinson111@gmail.com*.

The Generally Accepted Recordkeeping Principles® Extending the Principles to the Internet: A Way to Restore Trust Page 40

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

RIm Fundamentals Series Pursuing the Possibility of a Paperless Office Page 44

Anna Stratton, CDIA, has 22 years of records and information management (RIM) experience, including in enterprise-wide RIM plan development, digital migration planning and implementation, and document purge process development. Stratton was a digital migration consultant and subject matter expert for the U.S. Food and Drug Administration, completing an 18-month business case analysis and centralization plan for more than 2 million records in 19 locations and six product centers. She is a Certified Document Imaging Architect and continues her education in Lean Six Sigma process improvements and RIM best practices. She can be contacted at *annastratton@mac.com*.

ADVERTISE IN IM MAGAZINE

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

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

Talk to Karen or Krista about making a splash.

Advertise today!

Karen Lind-Russell/Krista Markley
Account Management Team
+1 888.279.7378
+1 913.217.6022
Fax: +1 913-.341.6823
Karen.Krista@armaintl.org

AD INDEX

With our leading edge technologies, proven protocols and top notch information management expertise, we put you in **TOTAL CONTROL** of your information.

recall™

Your Information. Securely Managed.

INFORMATION GOVERNANCE
Total governance. Total control.

DATA PROTECTION
Guarantee Business Continuity

SECURE DESTRUCTION
Mitigate Risks

DOCUMENT STORAGE
Ensure Compliance

DIGITAL SOLUTIONS
Improve Workflow

Step into the **NEW GENERATION OF INFORMATION MANAGEMENT** with recall™

Learn More: recall.com | 1.888.RECALL6

ARMA 2013 | LAS VEGAS, NV | BOOTH 403 | OCTOBER 28-30

*2013 Iron Mountain Incorporated. All rights reserved. Iron Mountain and the design of the mountain are registered trademarks of Iron Mountain Incorporated in the U.S. and the other countries.