INFORMATION MANAGEMENT

AN ARMA INTERNATIONAL PUBLICATION

MAY/JUNE 2014

Plug Internal Data Leaks with an Effective IG Program

Page 20

Proposing a Charter of Personal Data Rights

Page 27

Leveraging the Principles in Mergers, Acquisitions, and Divestitures

Page 32

INFORMATION MANAGEMENT

MAY/JUNE 2014 **VOLUME 48 NUMBER 3**

INFORMATION MANAGEMENT

AN ARMA INTERNATIONAL PUBLICATION

Publisher: Marilyn Bier

Editor in Chief: Vicki Wiler

Contributing Editors: Cyndy Launchbaugh, Jeff Whited

Art Director: Brett Dietrich

Advertising Sales Manager: Elizabeth Zlitni

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

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

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

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

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

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

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.

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.

WHEN IT COMES TO SCANNING WE ARE THE PREP-REDUCING EXPERTS

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

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.

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

OPEX® CORPORATION

Collaborating for Effective Information Governance

Coming together is a beginning, staying together is progress, and working together is success." These words, from Ford Motor Company founder and noted industrialist Henry Ford, could well be the motto for IG professionals who are intent on ensuring that their organizations' information assets are protected, managed properly, and leveraged to help them meet their strategic goals. This idea of the value of sustained collaboration is reinforced in every article inside this issue.

In the cover article, John Phillips, CRM, CDIA, FAI, addresses protection with solutions for stemming the tide of insider data leaks. Brought into the spotlight by the exposure of millions of classified files in the WikiLeaks and NSA file theft cases, insider threats represent a significant shift in focus away from external threats for IT professionals, Phillips writes. He says that because the high volume of information overwhelms the limited technology available to combat this threat, an effective IG program that focuses on policies, procedures, and people is the best solution.

The foundation for a strong IG program – The Generally Accepted Recordkeeping Principles® (Principles) – can also be leveraged by organizations involved in mergers, acquisitions, and divestitures to assess and improve their resulting IG programs. In the Principles Series article, Julie Gable, CRM, FAI, provides two case studies that show how it also requires a mixture of IG expertise from key players in several business units.

Two other articles focus on how collaboration can help ensure information security and privacy. In our new, occasional "Point of View" series article, Marc Kosciejew, Ph.D., writes that a charter of personal data rights is necessary to return the control of personal data – which is frequently collected and used without consent – to the individuals that data identifies. Implementing such a charter would certainly require collaboration, for it would involve using metadata for access control; imposing auditing requirements, encrypting data rights; connecting data with verified identifies; and punishing violators.

Ensuring the privacy of healthcare information stored in the cloud takes the effort of IG, RIM, legal, and IT. According to author Rebecca Shwayri, J.D., cloud vendors are likely to be considered "business associates" that must comply with the Health Insurance Portability and Accountability Act (HIPAA) and the 2013 HIPAA Omnibus Final Rule. And, while the latter imposes direct liability for security breaches on business associates, Shwayri writes, the covered entity is also liable. Therefore, organizations must assess the cloud vendor's compliance with HIPAA by

examining its audit reports and its administrative, technical, and physical safeguards.

Many IG stakeholders must also be involved to ensure the success of a records survey, which Ann Bennick, Ed.D., CRM, and Judy Vasek Sitton, CRM, write about in the RIM Fundamentals Series article. The authors introduce a tool that provides interview questions for conducting an effective records survey.

We hope these articles will spur you to step up your collaboration efforts with other IG stakeholders in your organization. Please take a few moments to let us know your results by e-mailing us at *editor@armaintl.org*.

Vicki Wiler
Editor in Chief

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

MOBILE DEVICES

Surveys: Mobile and Cloud Are Paying Off

Embracing bring your own device (BYOD) and other consumer technologies in the workplace can pay big dividends. The majority – 70%, according to one study – of companies that have deployed mobile and cloud solutions have experienced some sort of return on investment (ROI) from using consumer devices such as tablets and smart phones in the workplace. These devices are giving companies a competitive advantage and contributing to a healthier bottom line.

These conclusions were echoed in two surveys, one conducted by IDG Enterprises involving 1,155 IT decision makers and the other by *Computerworld*, featuring 313 business and IT professionals who influence buying decisions.

The *Computerworld* "2014 State of the Enterprise Survey" found that an increasing number of businesses consider mobility (59%) and collaboration (58%) technologies to be very important or critical to creating a competitive advantage for their organizations' long-term future. Therefore, it's no surprise that the vast majority of the respondents said they are in the process of adopting, have completed deploying, or have optimized their ROI from mobility (74%), collaboration technologies (73%), cloud (58%), and consumer IT (45%) initiatives.

This growing trend translates to increased spending on such devices. Almost half of the IDG respondents to the "2014 Consumerization of IT in the Enterprise" survey plan to invest in tablets and employee training to make the most of this technology; 43% will invest in smart phones. On a business level, this trend is prompting IT leaders to move beyond first-responder status to craft a long-term strategy for success.

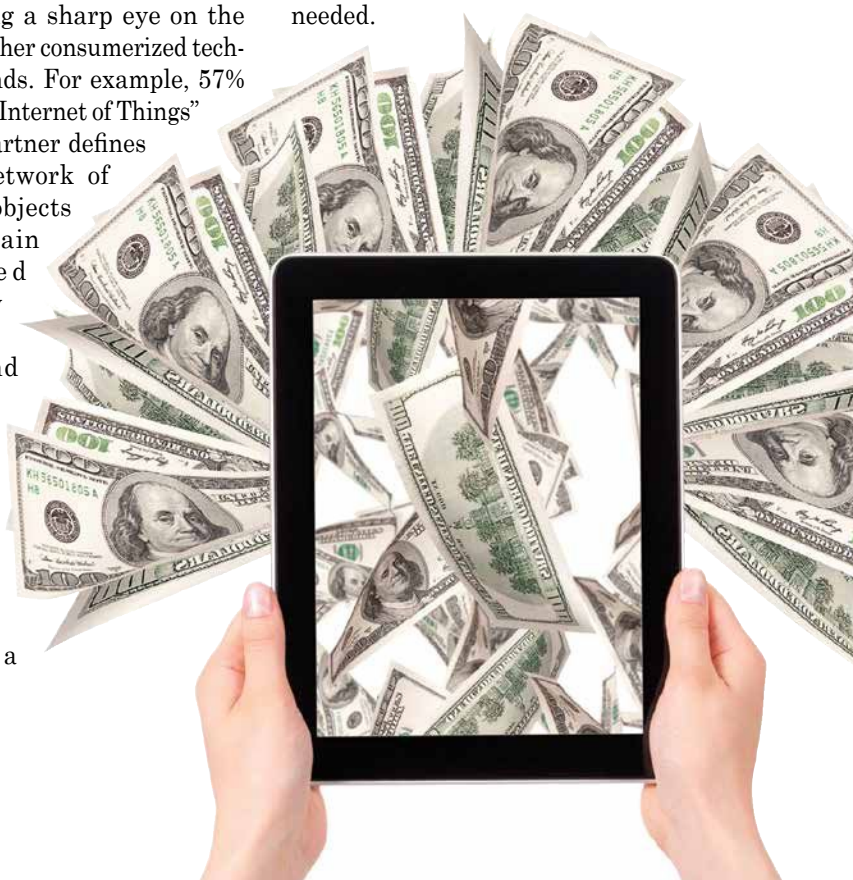
"Driven by widespread mobile device usage, the spread of consumerized technologies such as mobile devices appears poised to move from the mainstream to a transformative technology that will trigger widespread changes in how business users work," the IDG survey report stated.

Indeed, more than 80% of the IDG respondents are making at least one organizational change as the result of the increased use of consumer technology in the workplace, and more than half have implemented formal policies to regulate how corporate data is accessed and shared on consumer technologies such as mobile devices or cloud computing.

IDG respondents reported they are keeping a sharp eye on the impact of other consumerized technology trends. For example, 57% expect the "Internet of Things" – which Gartner defines as "the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment" – will have a significant or moderate impact on the business landscape.

Moreover, consumer technologies are driving adoption of related technologies, creating a snowball effect at many companies. For example, more than 60% of respondents said that consumer technology use will increase the use of cloud computing services at their company, while a little more than half expect a similar impact regarding Web 2.0 technologies such as web applications, mashups, and social media, according to the IDG report.

Companies investing in these and other emerging technologies expect to reap financial, operational, and strategic benefits. Consequently, many IT departments, especially in larger companies, are struggling to balance business expectations with the challenges of integrating new technologies with legacy systems that are still needed.



INFO SECURITY

Beware Security Pros: The Wearable Revolution Is Coming

Remember the old Dick Tracy walkie-talkie watch? That was hightech.

Now we have Internet-connected spectacles (Google Glass) and computers on wrist watches (smartwatches), also known as *wearable technologies*. Some predict that 2014 may well be the year wearables will become mainstream.

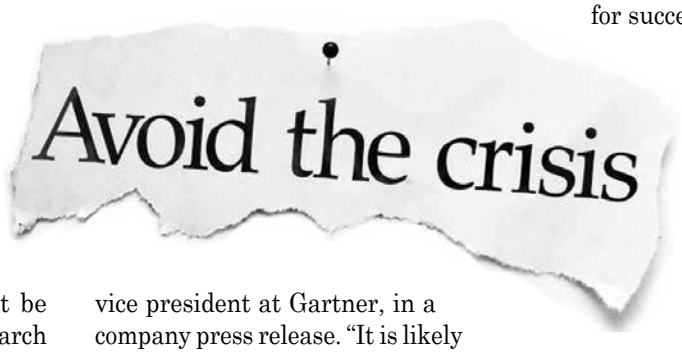
These new technologies are vulnerable to cyber attacks, warned Rashmi Knowles, chief security architect at RSA, EMC's security division, in a recent digital article on *TechRadar Pro*. He pointed out that Google Glass is expected to be commercially available by the end of the year. Although many consumers are skeptical of the technology, Knowles sees significant possibilities for businesses, especially those dealing with advanced engineering or electronic technology. The technology could enhance the capabilities of their staff, but it could also become extremely vulnerable considering there are viruses that can control the microphone and camera of a mobile device.

Knowles also noted that the inherently small screens are designed to make information decipherable at a glance. That means a lack of domain names and graphics, which will make it more difficult to detect phishing e-mails and other "deception-based cyber-attacks."

"…[A]s security professionals we need to be aware that, as wearable technologies make their way into the workplace, they represent a multiplication of potential attack surfaces. This will affect everything from BYOD policy to information infrastructure design, and we would be well advised to prepare now," Knowles said.

INFO GOVERNANCE

Gartner Warns of Information Crisis by 2017



Fortune 100 organizations beware: an information crisis might be looming. Gartner, an IT research and advisory company, predicts that one-third of the Fortune 100 will experience an information crisis because of their inability to "effectively value, govern and trust their enterprise information."

"There is an overall lack of maturity when it comes to governing information as an enterprise asset," said Andrew White, research vice president at Gartner, in a company press release. "It is likely that a number of organizations, unable to organize themselves effectively for 2020, unwilling to focus on capabilities rather than tools, and not ready to revise their information strategy, will suffer the consequences."

Business leaders need to be more proactive and manage information for business advantage rather than just maintain it, emphasized White. IT leaders must design enterprise information management (EIM) initiatives so sharing and reusing information creates business value that contributes to enterprise goals. An EIM program must help an organization identify which information is important to its success – not all information is.

Unfortunately, according to Gartner, more than 75% of an organization's individual information management initiatives are isolated from each other. Consequently, EIM is not being realized, sustained, or fully exploited.

Gartner recommends that "IT leaders identify the crucial business outcomes in need of improvement or that are being hampered by poor information management. Second, they need to determine the business processes and leaders most affected by those outcomes and use their findings to start setting priorities for a new EIM program. Finally, they need to adopt a program management approach for EIM, to identify work efforts, resource commitments, stakeholder expectations, and metrics for success."

As EIM focuses on linking projects, using assets, and aligning organizational efforts, there is also demand for information governance, said White. "With effective information governance, business users will understand the impact of poor quality data on the outcome of desired business processes. This understanding leads to a desire, on behalf of the end user, to assure or 'steward' the data so that it supports their day-to-day business activities."

CYBERSECURITY

Boards Seek Cybersecurity Risk Experience

Experience overseeing cybersecurity risk is increasingly in demand in the boardroom, according to a key finding of the 2014 "What Directors Think" survey report. In fact, the report shows information technology expertise is the fourth most-desired attribute for new corporate board members, following only financial expertise, industry expertise, and CEO experience.

The survey of nearly 600 corporate directors revealed that 20% of directors are not confident their board understands the many facets of cybersecurity risk. According to a press release about the report, "Overall, boards indicated they were confident in their ability to monitor cyber risks; however, about 40% acknowledged there was room to improve knowledge and understanding of risk oversight in general."

"Risk oversight has always been a key focus for boards but with developments in technology and the rise of social media, many are reassessing their skillset or partnering with organizations that specialize in risk management," said NYSE Euronext Head of Global Issuer Services Jean-Marc Levy in the press release.

The survey was released by NYSE Governance Services and senior executive search firm Spencer Stuart.

E-DISCOVERY

Can Contract Provisions Reduce Discovery Risks?

The pressure is on. Corporate counsels are looking for ways to reduce the impact of e-discovery and lower its price tag, which are not easy tasks given the tremendous volume of electronically stored information and plaintiffs' growing sophistication in aggressively seeking e-discovery. Add to that the court's willingness to sanction defendants for non-compliance, and it's understandable why corporate defendants are feeling pressured. After all, according to an article in *Law Technology News*, it's estimated that discovery costs now account for up to 50% of total litigation costs.

One approach that may help control costs is the use of contract provisions whereby parties negotiate the terms of e-discovery at the beginning of the relationship. Many issues could be addressed, including specifying when the duty to preserve begins, specifying the types and sources of data to be preserved and searched, determining fee and cost-shifting provisions, and limiting the availability of discovery sanctions.

How successful this approach could be is unknown due to the lack of case law. Corporate counsels should be prepared for the court to override the contract provisions. For example, the Federal Rules of Civil Procedure state that the duty to preserve begins when a party can reasonably anticipate litigation. Regardless of what date the parties agreed the duty to preserve begins, the court could determine a different date and assess sanctions, particularly if it perceives the contractual provisions to be one-sided. Courts are more likely to enforce a provision when it is the result of legitimate arm's-length bargaining between parties of equal bargaining power; thus it's possible that contracts between two corporations are better candidates for such provisions than employment contracts or those between corporations and consumers.

Clearly there are risks associated with this approach; it could increase discovery costs if the court doesn't enforce the provisions, so parties taking this route should beware.

XACT DATA DISCOVERY

Fact: The world is digital.

Fact: Paper hasn't disappeared.

Xact Data Discovery is both

IN-HOUSE FORENSICS	ELECTRONIC DISCOVERY	NO-FEE PROJECT MANAGEMENT	DATA HOSTING & MANAGED REVIEW	PAPER DISCOVERY

XDD delivers EVERYTHING you need to tackle today's complex discovery challenges.

xactdatadiscovery.com
1.877.545.XACT

XACT DATA DISCOVERY
Because you need to know

INFO GOVERNANCE

How Does Your IG Program Measure Up?

Implementing a legally defensible retention schedule is a key component of an organization's data management program. It can speed up the e-discovery process and reduce costs associated with document preservation and reproduction. U.S. companies understand this. Unfortunately, the same can't be said for most companies in other countries, according to a recent *Mondaq* article.

If your CEO asked you to assess the condition of your information governance (IG) program, how would you respond? You might begin at the core of any comprehensive IG program: your records and information management (RIM) practices. If your organization is among the 13% who recently reported they don't have a RIM program, you're already in trouble.

Most (87%) of the organizations that participated in the 2013/2014 Information Governance Benchmarking Survey conducted by Cohasset Associates, ARMA International, and AIIM International confirmed they have a RIM program. That's the good news. The fact that few organizations (12%) fully integrate RIM and the other key IG disciplines – compliance, security, IT, risk management, audit – is the not-so-good news.

Some of the other findings of note are listed here:

- At 78%, the greatest challenge RIM programs face is changing the keep-everything culture.
- 42% said their programs are mature (according to the Information Governance Maturity Model) in protecting private, confidential, and sensitive information.
- 27% gave their programs a mature rating for the handling of electronically stored information as part of the legal hold process.
- 74% reported they have a legal holds process in place, and 72% of them think it is generally efficient and effective.
- The top three IG disciplines RIM is most integrated with are privacy (39%), information security (38%), and legal holds (36%).
- Only 35% train all employees on what information to manage and how to manage it at least every two years; more than 50% basically don't provide any training.
- 45% have either incorporated (18%) or are in the process of adding (27%) RIM compliance to service provider contracts.

CYBERSECURITY

Japan Holds Cybersecurity Drill

Preparations for the 2020 Olympics in Tokyo are underway, including those aimed at strengthening national security. In March, Japan gathered more than 150 cyber defense experts to simulate an attack across 21 state ministries and agencies and 10 industry associations, reported Reuters. The exercise simulated a phishing attack, where government officials or businesses opened up their servers to a computer virus by visiting a fake website.

Britain had employed a similar tactic in preparation for the 2012 London Olympics. It warded off multiple attacks during the event.

"Cyber-attacks are becoming more subtle, sophisticated and international, and strengthening Japan's response to them has become a critical issue," the Japanese government's spokesman, Yoshihide Suga, said during the drill in Tokyo. Suga is the chief cabinet secretary and is in charge of Japan's cybersecurity.

"It's not that we haven't put effort into cybersecurity, but we are certainly behind the U.S.," said Ichita Yamamoto, the cabinet minister in charge of IT policy.

The drill marked the first time Japan's government and businesses have worked together to counter the threat of cyber attacks. The test is expected to help break down some of the current silos.

Also in March, IT minister Yamamoto convened the first meeting of cybersecurity officials from the ministries and police agency, joined by outside experts, to create a unified approach to Japan's online security. The group is expected to make its recommendations by summer.

E-DISCOVERY

India Lags in E-Discovery

Finding e-discovery services in India is extremely difficult, to say the least. According to a recent *CJNews India* blog posting, only a handful or more of law firms provide e-discovery services in India, and only one or two cyber law firms do. The deficit is due largely to a lack of the necessary techno-legal experience in the law firms and in law enforcement. India's law enforcement and revenue authorities have failed to take advantage of e-discovery and cyber forensics in their investigations, despite the fact that cyber laws were broken in several notable cases.

One high-profile example noted in the news posting was the Target Corp. breach, which exposed the personal information of up to 70 million customers. The company is facing litigation threats from around the world, including from India, for failing to comply with techno-legal requirements of applicable Indian laws.

According to the post by Priyanka Sharma, owner of the "Cyber Laws in India" portal, clearly needed are e-discovery and cyber forensics best practices that national and international companies operating in India would be required to adopt.

"In the absence of various techno legal compliance on the part of Indian and foreign companies operating in India, there is an urgent need to formulate effective and robust techno-legal e-discovery and cyber forensics regulatory regimes for India," Sharma posted.

Cyber forensics and cyber crimes investigation capabilities also need to be seriously strengthened, Sharma stressed.

E-DISCOVERY

More Companies Strive to Emulate U.S.-Style Retention Policies

Implementing a legally defensible retention schedule is a key component of an organization's data management program. It can speed up the e-discovery process and reduce costs associated with document preservation and reproduction. U.S. companies understand this. Unfortunately, the same can't be said for most companies in other countries, according to a recent *Mondaq* article.

"Except for truly global companies that have plenty of experience in U.S. litigation, many non-U.S. companies do not know how broad and burdensome the discovery process can be," said Masahiro Tanabe, an attorney who focuses on cross-border business transactions and disputes in the Tokyo office of Foley & Lardner LLP, in the article. "Similarly, many of them do not know that there is an obligation to preserve relevant documents pre-litigation. Accordingly, they are not always fully aware of the importance of a defensible document retention policy."

Tanabe said many companies typically have retention schedules that were developed in accordance with their home country standards. The more business they do with the United States, the more prepared they must be for U.S. litigation. That's why many Japanese and other non-U.S. companies are trying to implement U.S.-style, company-wide document retention policies. Unfortunately, some practices that are unique to a country become obstacles. For example, in Japanese companies, it is common for each business department to have its own information system or encryption method.

Likewise, U.S. companies need to review their retention policies concerning their operations outside the United States. Privacy is an excellent example of a facet of information retention that trips up some U.S. companies. Google and other organizations have faced sanctions in European countries that have more stringent privacy policies than the United States has.

CYBERSECURITY

NIST Presents Cybersecurity Standard

The U.S. Commerce Department's National Institute of Standards and Technology (NIST) released the first version of the "Framework for Improving Critical Infrastructure Cybersecurity" in February. It was presented exactly one year after President Obama issued an executive order directing the agency to collaborate with industry to create a voluntary framework for managing cybersecurity-related risk based on existing standards, guidelines, and practices.

According to NIST, the framework uses a common language to address and manage cybersecurity risk in a cost-effective way, based on business needs without adding regulations. It focuses on using business drivers to guide cybersecurity activities and on considering cybersecurity risks as part of the organization's risk-management processes. Furthermore, because it references globally recognized standards on cybersecurity, it "can serve as a model for international cooperation on strengthening critical infrastructure cybersecurity."

Per the executive order, the framework also provides guidance on how organizations can incorporate the protection of individual privacy and civil liberties into a comprehensive cybersecurity program.

NIST has stressed that the framework is not a one-size-fits-all approach to managing cybersecurity risk. "Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances – and how they implement the practices in the framework will vary."

The agency recommends that companies begin by prioritizing their business objectives and identifying the digital threats to those priorities; then determine how they would identify, protect against, detect, respond to, and recover from a cyber attack. The next steps should be to conduct a risk assessment and define their cybersecurity objectives. Once they've identified the gaps between their current and desired cybersecurity profiles, they should be ready to develop an action plan.

The framework is generally regarded as a good first step, but some don't think it goes far enough. Ann M. Beauchesne, vice president of national security and emergency preparedness for the U.S. Chamber of Commerce, stated: "[T]he Chamber believes that the framework will be fundamentally incomplete without the enactment of information-sharing legislation. Businesses need policies that foster public-private partnerships – unencumbered by legal and regulatory penalties – so that individuals can experiment freely and quickly to counter evolving threats to U.S. companies."

Greg Nojeim, director of the Center for Democracy and Technology's Project on Freedom, Security and Technology, said, "The framework will be useful to companies and their privacy officers, because it will remind them that processes should be put in place to deal with the privacy issues that arise in the cybersecurity context. However, we are concerned that the privacy provisions in the framework were watered down from the original draft. We would have preferred a framework that requires more measurable privacy protections as opposed to the privacy processes that were recommended."

NIST noted that the framework "is a living document and will continue to be updated and improved as industry provides feedback on implementation. As the framework is put into practice, lessons learned will be integrated into future versions."

In conjunction with the release of the framework, the U.S. Department of Homeland Security launched the Critical Infrastructure Cyber Community C^3 (pronounced "C cubed") Voluntary Program to encourage use of the framework and serve as the coordination point within the federal government for critical infrastructure owners and operators interested in improving their cyber-risk management processes. Initially the program is focused on working with sector-specific agencies and organizations to develop guidance on how to implement the framework.

Compliance monitoring is just a click away

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

NAID just made this a lot easier!

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

Data Destruction Co.

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

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

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

NAID AAA Notification

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

PRIVACY

What's Posted to the Internet Stays on the Internet – or Does It?

The European Parliament passed new online privacy rules in March that could shorten the Internet's memory, so to speak. One of the measures, the so-called "right-to-be-forgotten" rule, would allow consumers to request that companies delete selective data from their systems. If they have no legitimate grounds for keeping the data, the companies would have to comply.

While this is an idea that seems to be growing in popularity (as evidenced by the growing popularity of apps like Snapchat, whose messages automatically disappear within a few seconds), particularly in Europe, it has some in the technology world concerned. They fear, Felix Gillette wrote in a recent *Bloomberg Businessweek* article, that it would turn providers such as Google and Facebook into "global censors" as they are bombarded with requests to edit, alter, or delete consumers' information.

The impact of the new measures, if approved by the 28 member states, would be felt by companies outside of Europe as well. The measures are not expected to progress until after the May elections.

CLOUD

Cisco to Build Global 'Intercloud'

Network giant Cisco announced in March that it will spend $1 billion over the next two years to create the world's largest global, open, hybrid cloud, a network of clouds it is calling an "intercloud."

"…[W]e saw an opportunity, by building an Intercloud with more national cloud nodes than any rival, to address rising data sovereignty concerns," Robert Lloyd, Ciscos's president of development and sales, wrote on the Cicsco blog "The Platform."

"Our cloud will be the world's first truly open, hybrid cloud," said Lloyd. "[It] will be built upon industry-leading Cisco cloud technologies and leverage OpenStack for its open standards-based global infrastructure. We plan to support any workload, on any hypervisor and interoperate with any cloud."

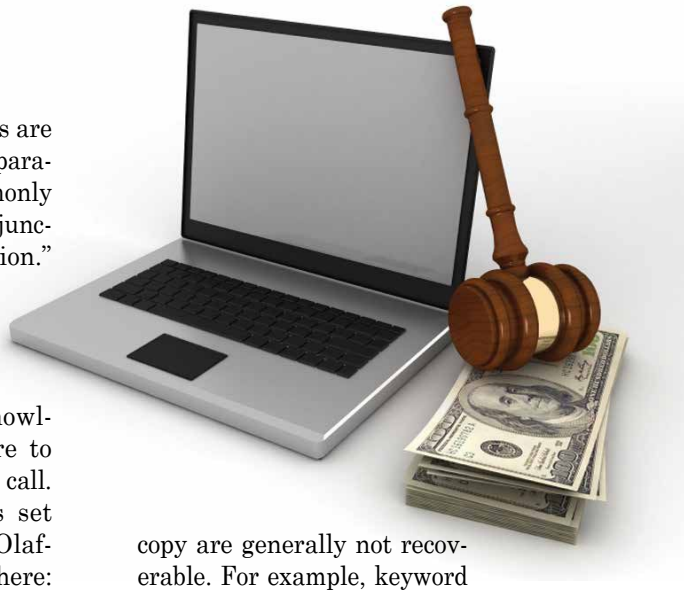
Lloyd said the intercloud is being built for the Internet of Everything – which Cisco defines as "bringing together people, process, data, and things to make networked connections more relevant and valuable than ever before – turning information into actions that create new capabilities, richer experiences, and unprecedented economic opportunity for businesses, individuals, and countries." It will be, according to Lloyd, "capable of scaling to billions of connections, and trillions of events, all supported by real-time analytics to help customers get the insights they need from the connections of people, processes, data and things, as they happen."

The goal is a "Star Alliance" of technology companies, Cisco Senior Vice President for Cloud Sales Nick Earle told *The New York Times*. Star Alliance is a global network of 28 major airlines, the article explained.

At the time of the announcement, Telstra, a telecommunications and information services company in Australia, had signed on as Cisco's first partner. Cisco will deploy and run a cloud infrastructure on Telstra's behalf, and Telstra will provide both Cisco-specific and Telstra-specific solutions to customers. Several other companies have also announced their support for the Intercloud.

E-DISCOVERY

Court Clarifies Standard for Recovery of E-Discovery Costs



The costs of producing documents for litigation have become a significant burden for the parties involved. In fact, e-discovery costs often reach into the hundreds of thousands of dollars. A recent decision by the U.S. Court of Appeals for the Federal Circuit (*CBT Flint Partners, LLC v. Return Path Inc.*) provides a guideline for determining the recoverability of those costs.

28 U.S.C. § 1920 states that among the recoverable expenses are "the costs of making copies of any materials where the copies are necessarily obtained for use in the case," according to Shane Olafson, a partner at Lewis Roca Rothberger LLP, in a recent *The National Law Review* article. "District courts have been all over the map when deciding what constitutes 'making copies' for purposes of recovering taxable costs associated with e-discovery," Olafson wrote.

The federal circuit court reviewed the history of Federal Rules section 1920, The Sedona Conference® principles, and other federal court decisions in concluding that section 1920 applies only to documents produced in accordance with Rule 26 or other discovery rules and does not apply to documents a party creates for its own litigation or other use.

Stated the federal circuit: "[R]ecoverable costs under section 1920(4) are those costs necessary to duplicate an electronic document in as faithful and complete a manner as required by rule, by court order, by agreement of the parties, or otherwise. . . . But only the costs of creating the produced duplicates are included, not a number of preparatory or ancillary costs commonly incurred leading up to, in conjunction with, or after duplication."

In its final opinion, the federal circuit focused on whether various tasks were necessary to fulfill a party's discovery obligation, acknowledging that deciding where to draw the line is a judgment call.

Some of the guidelines set forth in the opinion that Olafson summarized are listed here:

- If a party must convert electronic documents to a uniform production format (e.g., TIFF or with metadata included), those steps are considered "making copies" for purposes of recovery. If such processing steps are unnecessary, they are not recoverable. For example, if metadata can be preserved without first using imaging and extraction techniques, those additional steps are not recoverable.
- If a vendor works on a large volume of documents before culling to produce only a subset, awarded costs must be confined to the subset actually produced.
- Costs incurred in *preparing* to copy are generally not recoverable. For example, keyword searching, reviewing documents for responsiveness and privilege, and training to use review software are not recoverable. Rather, they are part of "the large body of discovery obligations, mostly related to the document-review process, that Congress has not included in section 1920(4)."
- Deduplication and decryption costs are not recoverable.
- The creation of "load files" is covered to the extent those files contain information required by the requested production.
- The costs of slip sheets are recoverable.
- The costs of copying responsive documents to production media are recoverable.

PRIVACY

Privacy Groups Try to Stop Facebook's Purchase of WhatsApp

Facebook's recent announcement that it was purchasing the instant messaging app WhatsApp met with mixed responses. Privacy advocates promptly petitioned the Federal Trade Commission (FTC) to stop the $19 billion sale until it was clear how Facebook would use the personal data of WhatsApp's 450 million users. The app has long been committed to not collecting personal data for advertising purposes. The question is: Will Facebook (which does collect personal data for advertising purposes) honor that commitment?

Facebook responded that "WhatsApp will operate as a separate company and will honor its commitments to privacy and security."

Despite such assurances, Reuters reported, the privacy groups behind the FTC filing noted that Facebook has in the past amended an acquired company's privacy policies, such as the Instagram photo-sharing service that Facebook acquired in 2012. The groups asked regulators to require Facebook to "insulate" WhatsApp user information from access by Facebook's data collection practices.

CLOUD

What NOT to Do When Adopting the Cloud

Before deciding to make the leap to the cloud, you may want to read Mike Kavis's new book, *Architecting the Cloud: Design Decisions for Cloud Computing Service Models*, which explores the key steps IT and business leaders need to first consider.

Joe Kendrick previewed the book in a recent *Forbes.com* article, summarizing the nine "worst practices" Kavis has observed that have derailed cloud deployment.

- *Worst Practice #1: Migrating applications to the cloud solely to drive down costs.* Kavis says companies that want the cloud to reduce the costs of managing current applications should consider moving their applications to a managed hosting provider.
- *Worst Practice #2: Having inflated expectations of suddenly becoming a digital enterprise.* Kavis advises that companies should use the cloud for smaller deliverables that can provide business value sooner and in smaller increments.
- *Worst Practice #3: Not fully understanding cloud security.* The lack of standards and enterprise experience with the cloud make it vulnerable to abuse. Cloud security understanding needs to be a top priority for architects, product teams, and other IT professional, says Kavis.
- *Worst Practice #4: Selecting a favorite vendor, not an appropriate one.* Kavis advises to select a vendor who is experienced in cloud and understands the different business circumstances it may present. He also advises IT professionals to learn about the three cloud service models.
- *Worst Practice #5: Failing to plan for outages.* He says organizations must understand the providers' service level agreements and data ownership policies and must thoroughly examine all legal binding documents and agreements.
- *Worst Practice #6: Not understanding the impacts of organizational change.* Starting with smaller, less risky initiatives can help minimize or diffuse resistance to change, Kavis believes. He also recommends bringing a change leader into the process.
- *Worst Practice #7: Not bringing in enough of the right skills.* Operating in the cloud often requires new or different skills. Kavis suggests organizations help employees get the experience they need to manage in the cloud.
- *Worst Practice #8: Misunderstanding customer requirements.* Kavis advises creating a list of frequently asked questions to help customers navigate the cloud.
- *Worst Practice #9: Not preparing for unexpected costs.* Kavis notes that "the most expensive part of cloud computing usually has nothing to do with the cloud at all. Often companies underestimate the effort it takes to build software in the cloud."

INFO TECHNOLOGY

Predictive Coding: Not Just for E-Discovery

Relying on employees to appropriately label and manage records is a flawed approach, according to experts who spoke at the recent LegalTech New York. *Law Technology News* reported that one of the experts, Warwick Sharp, vice president of marketing and business development at Equivio, equated this approach to a game of telephone in which the retention officer "is responsible for sending a company's record policy all the way down the chain to a company's last user employee (who is ostensibly responsible for labeling files in his own email with up to 300 categories)."

The impracticality of this approach is obvious, especially when a company has thousands of employees and hundreds of policies, Sharp said. In his opinion, predictive coding could be a much better solution considering that a records retention expert can train software to label documents with categories. The goal: an automated process that is consistent, and defensible.

Panelist Laura Kibbe, managing director of expert and professional services at Epiq, related a case study that demonstrated the usefulness of predictive coding to one of Epiq's clients. Kibbe said they were able to clean up the company's e-mail repository by categorizing 40% of 1.4 million stored documents as simply junk e-mails, with 80% accuracy – a rate that has been accepted as legally defensible in court, according to the panelists. This approach yielded substantial savings in storage and e-discovery costs for that material alone, persuading the company to further analyze and categorize the not-junk category.

The experts were quick to remind their audience that the goal of predictive coding isn't perfection, but that perfection wasn't possible in the days of paper either. It is, however, a more defensible process than relying on 20,000 employees to follow a detailed schedule.

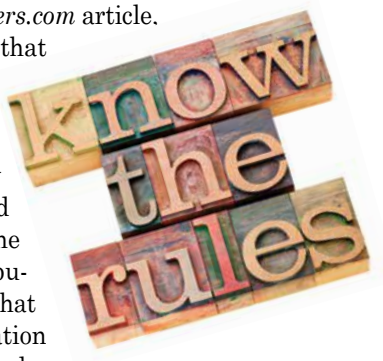
E-DISCOVERY

FRCP Comments Under Review

The proposed changes to the Federal Rules of Civil Procedure would require a party seeking discovery to establish that the requests are justified by the value and "importance" of the case; and they would limit the number of depositions, interrogatories, and requests for admissions.

A brief review of the comments received via hearings and written submissions didn't uncover any surprises. According to Alison Frankel in a *Reuters.com* posting, the comments revealed that defense lawyers and business groups praise the Judicial Conference (which presented the amendments) for attempting to reduce the burdens of discovery in civil litigation in the federal courts, while plaintiffs' lawyers expressed serious concern that proposed limits on depositions, interrogatories, and other discovery tools will exacerbate the challenge of acquiring legitimate information from defendants who don't want to surrender it.

In a Jan. 13 letter to the Committee on Rules of Practice and Procedures, U.S. District Judge Shira Scheindlin of the Southern District of New York questioned the need for and impact of some of the proposed changes. She wrote that a change to Proposed Rule 26(b)(1) adds a proportionality assessment that "invites producing parties to withhold information based on a unilateral determination…. This could become a common practice, requiring requesting parties to routinely move to compel the production of the withheld materials. This, in turn, will increase costs and engender delay."



In the *Reuters.com* article, Frankel wrote that Scheindlin, who is a noted authority on e-discovery sanctions and the author of the influential Zubulake decisions that are the foundation for the current rules, has expressed opposition to the proposed new rule for e-discovery sanctions, particularly the rule's "willful or in bad faith" language. Frankel reported that Scheindlin "is of the view that requiring a showing of bad faith to impose sanctions will encourage parties to handle their e-discovery preservation sloppily."

INFO TECHNOLOGY

New Study: Are State and Local Agencies Ready to Deploy the 'Big Five' IT Initiatives?

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

U.S. government agencies are looking to the "Big Five of IT" to help them respond to increasing responsibilities and decreasing funding, according to the new study "Big Five in Overdrive: Are State and Local Networks Ready?" by MeriTalk. In fact, most of the agencies said they plan to deploy over the next three years the "big five" IT initiatives:

1. Data center consolidation
2. Mobility
3. Security
4. Big data
5. Cloud computing

However, 94% also said their agency's IT network is not fully prepared for the resulting demands.

Government IT professionals generally buy into the promise of these initiatives to improve performance, productivity, and service, yet two-thirds (63%) admitted they would face moderate to significant network bottleneck risks, and 89% said they would need additional network capacity just to maintain current service levels.

These aren't the only likely ramifications of the infrastructure imbalance created by unsynchronized adoption of these technologies, according to the report. Additionally, the IT professionals said their agencies will face security risks (59%), bandwidth limitations (55%), storage limitations (44%), and network latency (40%).

Surprisingly, the respondents aren't asking for new budget or policy changes to overcome these challenges. They want better coordination, which they believe would result in increased efficiencies (72%), shared best practices (59%), and better decision making (58%). Only two of five agencies reported they are currently coordinating efforts across these initiatives.

As always, executive support is critical. More than half (52%) believe their organization's senior leaders do not understand the combined impact of these five initiatives on IT. When asked what they most need from their senior leaders, 54% of respondents said clear prioritization from leadership, 47% asked for regular coordination across all initiatives, and 44% cited the need for standardized documentation of infrastructure requirements.

"If agencies don't align their plans to the major IT trends driving our industry, both cost and risk will increase," said Anthony Robbins, vice president public sector for Brocade, which underwrote the study. "The Big Five will fundamentally reshape how state and local governments can deliver services to citizens – better services at a lower total cost. Agencies can't afford to wait, but without coordination and planning, network capacity will choke off any chance at delivering benefits."

The good news is that some agencies are laying the groundwork now. Almost half (45%) reported they have already taken steps to improve security measures. Many have also taken steps to improve network policies, reduce network latency, improve scalability, and add bandwidth.

CLOUD

U.S. Agencies Embrace the Cloud

Four years ago the U.S. government took a major step toward modernizing its IT system by issuing a cloud-first mandate and identifying funds to support the effort. Agencies were directed to adopt cloud computing in some capacity and were advised on how to select services appropriate for migration to the cloud, such as e-mail systems. Some agencies have moved beyond the cloud-first mandate and are looking at using the cloud strategically to support their missions.

Executives from the Interior and Treasury Departments recently described some of the more strategic cloud initiatives they've deployed; their comments came during a forum sponsored by the University of Maryland's Center for Digital Innovation, Technology and Strategy. Those initiatives include cloud platforms that support the geospatial community, develop-and-test-as-a-service, and extranet services, reported *InformationWeek*.

Regardless of how they embrace the cloud, many agencies are not adequately considering the electronic recordkeeping requirements, which could lead to legal problems, warn former and current officials at the National Archives and Records Administration (NARA).

"It doesn't surprise me that the issue of recordkeeping doesn't come up much in discussions about going to the cloud," Jason R. Baron, a lawyer at the Washington law firm Drinker Biddle and former director of litigation at NARA, recently told *InformationWeek*. "When people think about the cloud, the first issues that come to mind are security and privacy. Of course, those are extremely important, but from an information governance perspective, one needs a more holistic picture."

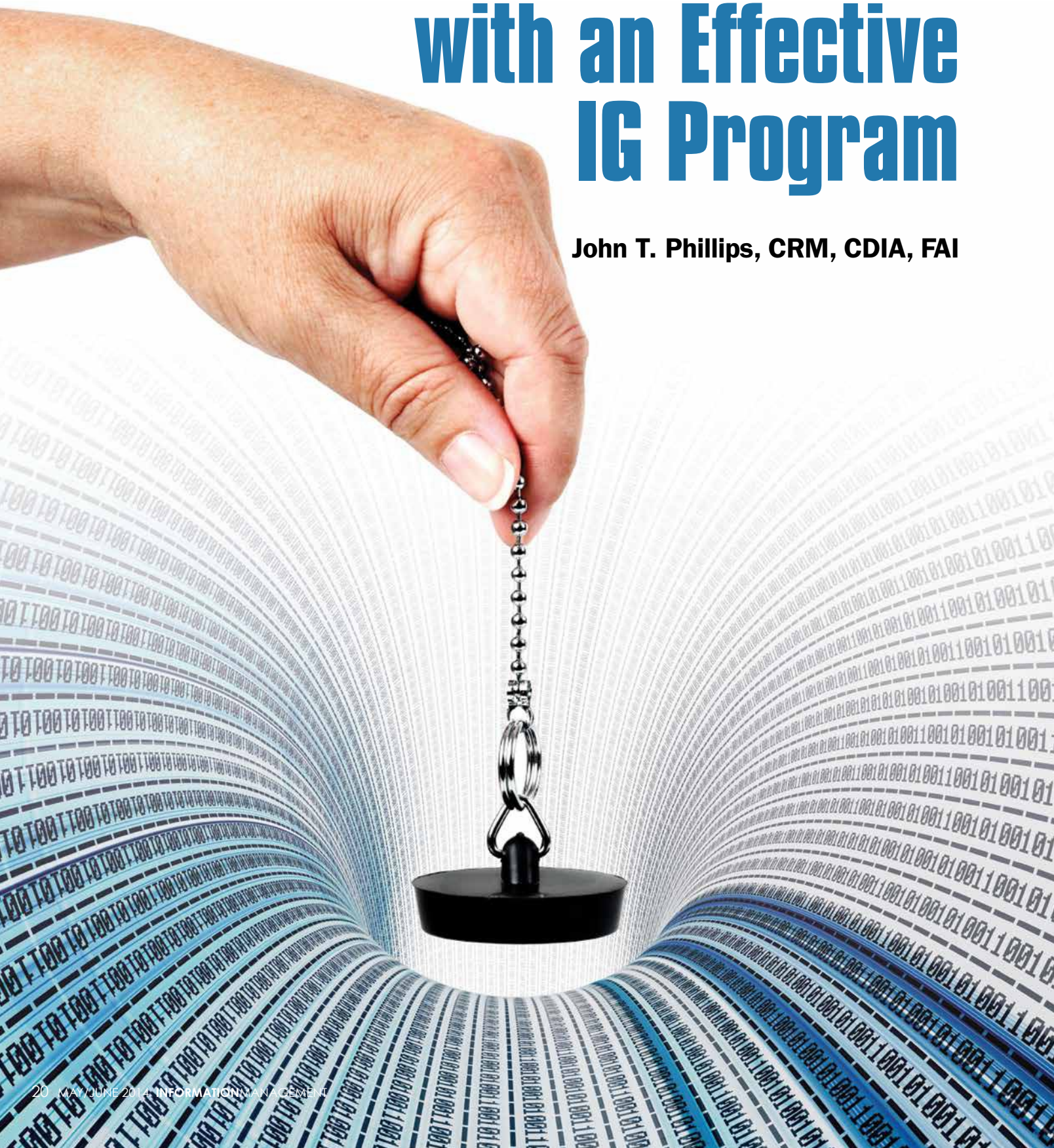
NARA launched the Capstone Project to help agencies better manage their e-mail by automation so the agencies can meet some of the key deadlines. For example, agencies must be managing their permanent and temporary e-mail records in an electronic format by the end of 2016 and all permanent records by December 31, 2019.

These deadlines will be especially difficult for those agencies that aren't spending enough time on electronic records management requirements at the beginning of the migration process. Explained Baron: "Otherwise you're building what amounts to a slow-motion train wreck, where you've got this cloud and you've got a million e-mails somewhere in there and that's all very good. But at the end of the day, when the agency wants [to forward e-mail records] to NARA, it may not have deleted any email or differentiated between what's permanent and what's temporary."

Agencies can look to NARA as a best-practices model for integrating electronic records requirements into a cloud-based e-mail migration. Last year NARA successfully moved more than 3,000 of its e-mail users to the cloud. The migration took only six months, but officials had spent several years carefully planning it. **END**

Plug Internal Data Leaks with an Effective IG Program

John T. Phillips, CRM, CDIA, FAI



Increasingly, employees are selling the "crown jewels" of their organization's proprietary information for a pittance. Organizations are scrambling for ways to reduce, if not eliminate, these internal threats. An effective information governance program can help.

Today's information security dangers while "surfing the Internet," downloading applications to smartphones, and opening e-mail are well-known. Organizations expect network hackers, data thieves, scam artists, and phishers to act from external sources. But, the unsettling truth is that data breaches often originate from individuals who operate from within.

New Technologies Not Always the Solution

Because organizations have used IT-based systems for more than 30 years, it would seem that common data protection mechanisms would protect them from data breaches. Although technical solutions like increasing network firewall capability or implementing better user access control systems might have addressed security risks in the past, today's environment is more challenging. Trends like employees using social media and their own devices for business produce evolving risks, making it more and more difficult for IT to address them.

Buying sophisticated new technologies is not necessarily the answer, either. Buying a new solution to control every new technology that enters the market or respond to information trends will break almost any IT department's budget. And many, if not most, security technology solutions today focus on external threats rather than risks that are embedded in every organization that has employees.

Unfortunately, such measures as data archiving, log-on procedures, disaster planning, and data encryption are not sufficient safeguards if employees fail to rigorously and properly practice them. Indeed, in *Information Week's* "2013 Strategic Security Survey" report published last June, 42% of respondents said "enforcing security policies" was their biggest information security challenge. (See Figure 1.)

One respondent said, "Shops doing security right have moved away from gimmicks to analyzing the core of every other business discipline: people." Further, 54% of respondents said that end-user security awareness training was their "most valuable security practice." (See Figure 2.)

Insider Threats Are Difficult Challenges

It was once possible for IT to focus most of its data security activities on the detection of inappropriate intrusions into computer networks based on external Internet protocol (IP) addresses or inappropriate data traffic on computer networks at certain times of the day. Today's mobile workforce and 24x7 workdays have made those parameters of network security less relevant.

IT departments dealing with huge volumes of data traffic must differentiate risks that occur from outside an organization from those that occur from within because internal breaches can pose much larger threats. Two recent high-profile cases illustrate this enormous change in attention.

WikiLeaks

Australian journalist Julian Assange and the WikiLeaks website he co-founded cannot publish secret information without it coming illegally from sources within other organizations. In the largest release of classified government information in the history of the United States, WikiLeaks was aided by U.S. Army soldier Pfc. Bradley Manning. Manning, who downloaded nearly 500,000 war documents to a compact disc, later copied the files to his laptop, and then transferred them to an SD card for a camera to transport them, provides a prime example of the risks of insider data theft and mobile technologies. In addition, the fact that an organization like WikiLeaks exists and has some public support for posting confidential insider information should give IT system administrators pause.

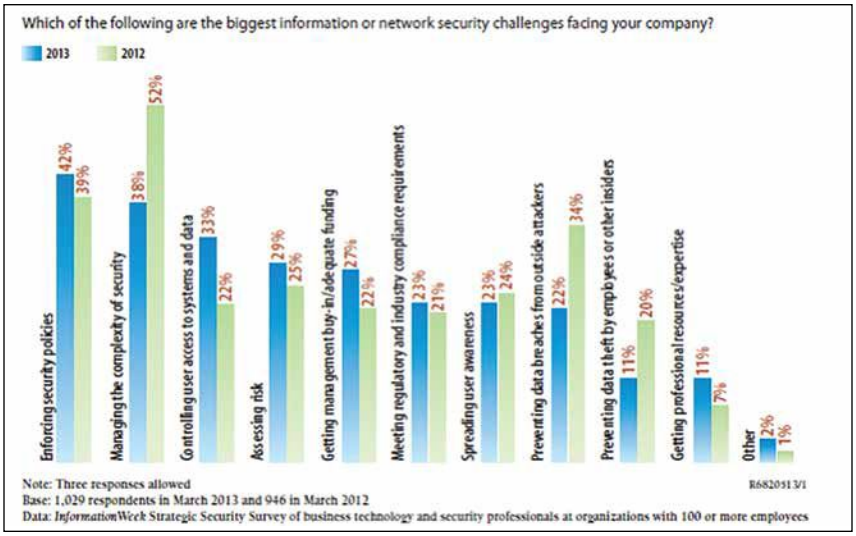


Figure 1: Biggest IT Security Challenges

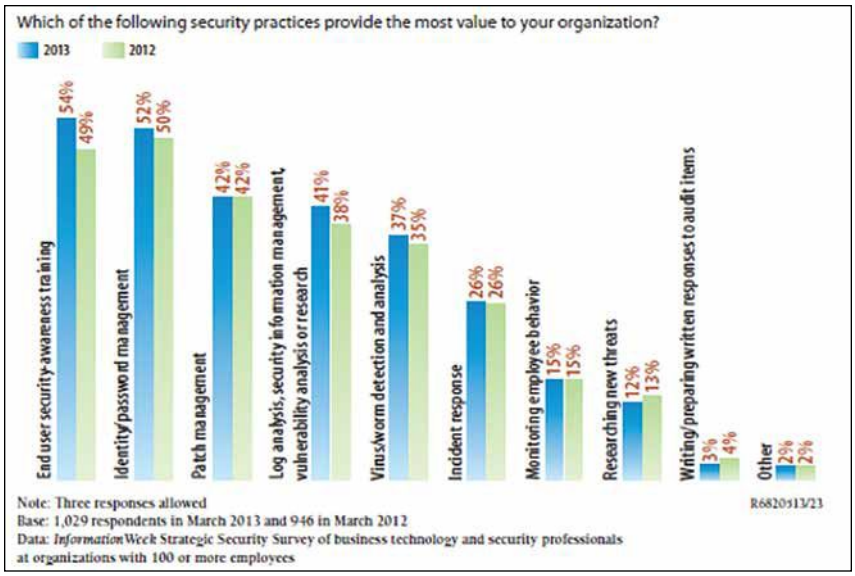


Figure 2: Most Valuable Security Practices

NSA Files Theft

More recently, U.S. National Security Agency (NSA) contractor Edward Snowden released approximately 1.7 million internal intelligence files, starting an enormous debate about the role of the NSA and other organizations in collecting information on private citizens and foreign leaders. This case makes it obvious that internal data breaches can have far-reaching organizational and social impacts.

Responses to insider threats can be difficult to incorporate into IT department strategic plans. How does an organization develop metrics for the frequency with which employees store company data on personal devices, for example?

Information Volume Overwhelms Tools

The tools that do focus on internal threats have only limited success. These tools often use technology that monitors external access threats to internal data and are designed also to monitor internal information being transmitted to external recipients by e-mail or by accessing external websites.

By monitoring large data transmissions, IP addresses for internal/external communications, and user system security parameters, IT system administrators can see if unusual data transmissions are occurring. Unfortunately, this approach is often overwhelmed by the sheer volume of information to analyze and results in reports without sufficient specificity to initiate meaningful security interventions before a compromise begins.

Focusing on Users, Content Can Help

So, how can IT departments increase the effectiveness of their internal security measures and internal system monitoring?

One method is to increase the specificity of the risk assessment by associating risks with data classification and users' access attributes. For instance, because it is possible to know that large data transmissions are atypical for some users, IT professionals can apply additional security measures to their user accounts.

They should apply these same measures to the user accounts of resigning or soon-to-be-terminated employees, who may be disgruntled and engage in data theft or sabotage before, during, or after their departure. With appropriate human resource procedures in place for data security, these breaches could be reduced in volume and severity.

Security monitoring is most effective, though, when the security measures can focus on the actual content of the data stream, discerning the increased risk when very sensitive information is crossing a network boundary, as opposed to monitoring large volumes of undifferentiated data. If, for instance, an e-mail contains certain text or metadata known to be business sensitive, additional attention must be focused on that data to effectively monitor the increased risk.

IG Program Is Best Solution

The best solution, though, is a comprehensive information governance (IG) program, which ensures that increased security measures and user training become part of an organization's daily operations. It is not difficult to develop an IG plan with strong information security awareness components that can be implemented by all employees and will enable them to intervene early in potential data breaches and minimize their consequences. Typical IG program components that can impact data security are listed below.

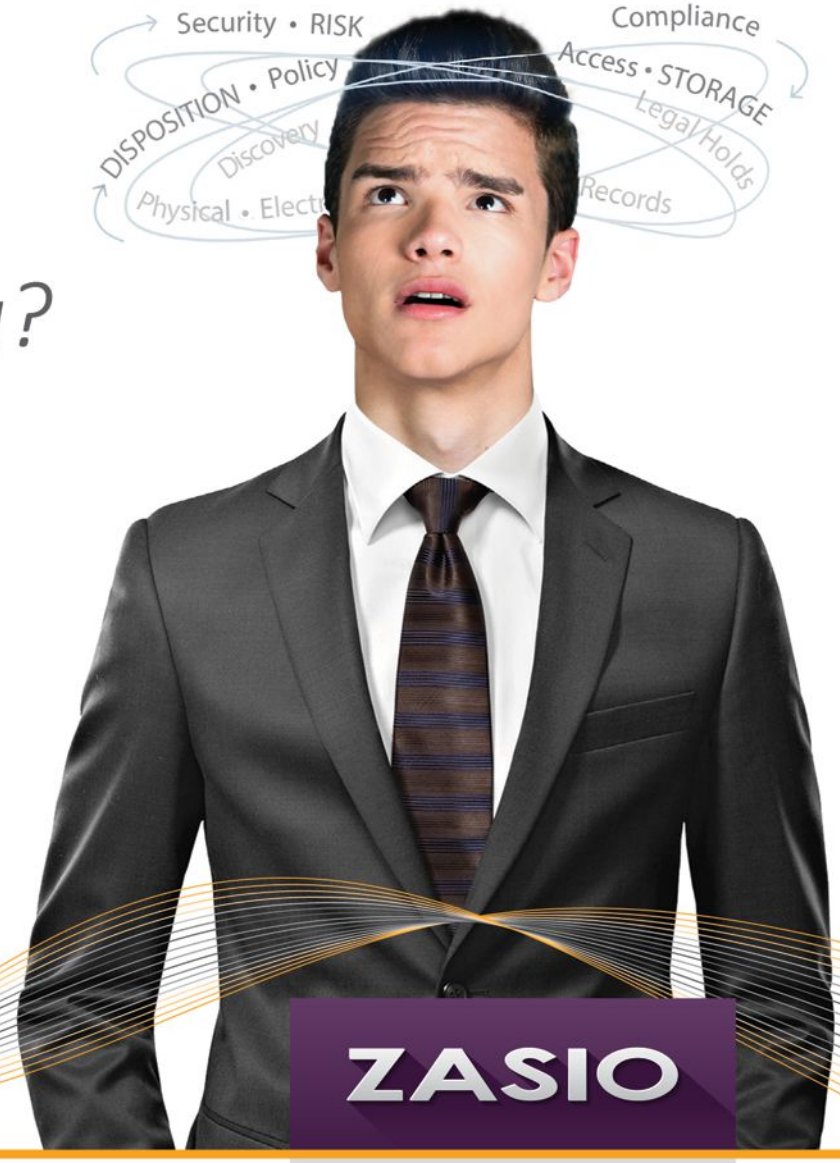
Data Management Policies and Procedures

Data management policies and procedures that address the enterprise-wide use of information represent the first step in embedding secure actions into systems and in helping ensure that employees are handling information securely. They are the umbrella that keeps data breach attacks from raining on an organization.

No single employee or department alone can intervene in every possible breach event. By cooperatively designing organizational IG standard operating procedures to address all types of information, it is possible to encompass most, if not all, attacks that could occur.

Don't be one of the many organizations that only partially implements its data management policies and

Information Governance have your head spinning?



ZASIO

RECORDS & DOCUMENT MANAGEMENT EXPERTS

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

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

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

800 513 1000 | www.zasio.com

Connect with us:

www.facebook.com/ZasioEnterprises

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

procedures, though; this increases litigation risk, not only because of the gap it leaves in the IG program, but because it implies to a court that the organization is not properly concerned with conducting business ethically and effectively.

IT System Inventories, Data Maps

Without knowing the informational content of technology systems, it is impossible to appropriately apply security procedures and retention rules. The locations of data, data types, and applications used for data creation and management must be clearly defined and documented for IG policies and data security measures to be implementable. An organization cannot manage and secure data it does not know exists.

Information Classification, Retention Rules

The data's value and risk must be classified before proper security measures can be applied. Business sensitivity, regulatory compliance requirements, legal hold obligations, privacy mandates, and other retention rules demand that data and IT systems be assigned content descriptors and metadata so appropriate procedures can be applied.

Organizational file plans, retention schedules, IT systems inventories, and application metadata can serve to create initial data security taxonomies to describe and classify information. In many cases, due to the huge volume of data that an IG program must encompass, automated tools that employ sophisticated search algorithms can enhance the specificity of classification processes across large data repositories and reduce the time needed to identify and respond to data breaches.

Enabling Technologies

In some cases, additional technology tools can be used to direct the application of security procedures to appropriate data and systems. Software already in use to detect viruses, malware, and other intrusive threats can often be applied internally to e-mail systems, database servers, file shares, and applications. In addition, more sophisticated search software can categorize data and system content for increased scrutiny once the information in those systems has been classified or the data can be accessed directly.

Many organizations are using enabling technologies to reduce human involvement in information processing. When content management systems were implemented many years ago, it was soon discovered that end users were not properly classifying content because of time constraints, system limitations, and confusing terminology.

Many applications now have content search, retrieval, and classification capabilities that allow at least an initial assessment of the value and appropriate rules to be associated with information types. These can save time, create data management metrics, and improve auditing of processes for classifying information and applying targeted data security measures. In addition, technology-based solutions can often identify data breaches that may not be evident to human eyes.

Training

Because systems are created for people and operated by people, employee training is extremely important for all information management system implementations.

Even "automated" technology solutions must be developed by people after targeting the business requirements, configured by people to be focused on their specific work process needs, and then operated by those individuals to accomplish their objectives. Training is a cornerstone of any IG program because humans are still involved in some way with all data creation, storage, and preservation or disposal.

Because systems are created for people and operated by people, employee training is extremely important for all information management system implementations.

The means and mechanisms of employee training across an enterprise might include direct-to-employee e-mail announcements, company-wide web seminars, social media site postings, and online testing programs with auditable accountability. Without a firm understanding of the importance of data security policies and the consequences of data breaches, many employees may not be aware they are contributing to increased risks.

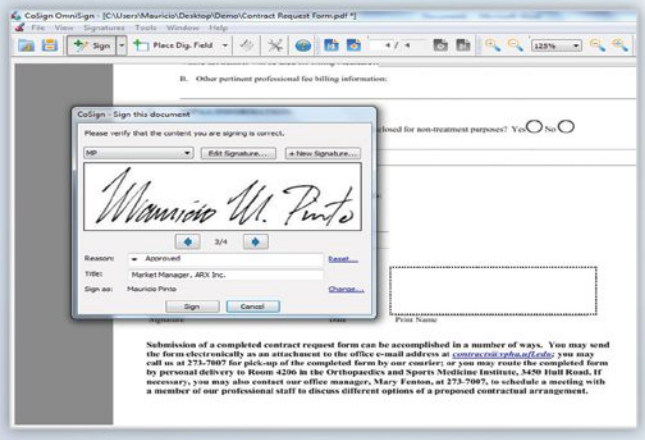
IT Must Leverage IG

Data breaches will continue to plague organizations that do not have comprehensive IG programs with accompanying integration of data security policies, procedures, and consequences for non-compliance. Considering that IG programs can reach across organizations to impact and train all employees, IT departments must take advantage of these enterprise-wide programs. **END**

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

Top Ten Tips for Selecting the Digital Signature Solution that is Right for Your Organization

As the traditional paper-based world gives way to global digital businesses, documents often require signatures to be collected from people across the world including employees, external partners or customers.



While document and content management systems are commonly used, the final step of signing documents breaks otherwise fully-automated workflows by requiring users to print and sign manually. Digital signatures enable companies to eliminate unnecessary delays and expenses and fully benefit from their automation investments with truly paperless processes.

Digital signatures provide numerous benefits to organizations, regardless of location, industry and size:

- Reduce paper-related costs, including printing, scanning and couriering
- Improve efficiency by speeding up all signature-related processes
- Enable everyone to sign anytime, anywhere and from any device
- Ensure trust, security, integrity, and control across the ecosystem
- Comply with industry and country-specific laws, regulations and audits

The best signature automation system should enable you to:

1. Easily add digital signatures to the types of documents and data you typically use
2. Sign using your existing content, document or workflow systems
3. Digitally sign whether you're using a PC, a web browser or any mobile device
4. Save your sensitive documents only inside your enterprise IT domain
5. Fully control its implementation and flexible integration with other systems
6. Continue using the management policies you already have in place
7. Comply with the regulations that are relevant to your organization
8. Allow anyone to validate the signatures even without access to the signing app
9. Implement it according to your preference: on-premises or in the cloud
10. Cost-effectively and efficiently manage the system for both IT and end-users

CoSign by ARX

The Digital Signature Company

CoSign, the most widely used digital signature solution in the world, has been recognized by Forrester Research* as "the strongest digital signature solution."

CoSign easily integrates with SharePoint, OpenText, HP, Alfresco, Oracle, K2, Nintex, and many other document-related systems.

To learn more, watch our ARMA webinar:
www.arx.com/go/arma2014
For a free 30-day trial, please visit www.arx.com.

* The Forrester Wave™ — E-Signatures, Q2 2013

New!

Save Thousands on Retention Requirements Research

Legal Requirements for Electronic Records Retention in Western Europe (PDF)

This PDF surveys national laws and regulations that specify retention requirements for commonly encountered records that are likely to be maintained in electronic form in 18 Western European countries where multi-national and transnational organizations have a significant presence. The types of records discussed include: corporate, accounting, tax, customs, legal, employment, workplace health and safety, intellectual property, and surveillance. It also discusses retention requirements for dissolved and bankrupt companies, data protection, and transborder records storage. (Much of the retention guidance is also applicable to paper records.)

$395.00 For Professional Members: **$295.00**

Also available for individual countries:

- Austria
- Belgium
- Denmark
- Finland
- France
- Germany
- Iceland
- Ireland
- Italy
- Liechtenstein
- Luxembourg
- The Netherlands
- Norway
- Portugal
- Spain
- Sweden
- Switzerland
- United Kingdom

$65.00 For Professional Members: **$50.00**

Order your copy online today!

ARMA INTERNATIONAL BOOKSTORE

www.arma.org/bookstore

Proposing a Charter of Personal Data Rights

Our personal data is being created, collected, mined, analyzed, monitored, shared, sold, stored, and used for diverse reasons beyond most of our knowledge or control, let alone our willing consent or endorsement. A charter of personal data rights is needed to temper this datafication of people's lives, which compromises personal privacy, confidentiality, trust, and security.

Marc Kosciejew, Ph.D.

In this data-saturated world, many important political, economic, and social activities increasingly provide opportunities for access to and use of *personal data* – that is, information relating to an individual as an identified or an identifiable person. It is being harnessed and exploited by powerful institutions and interests for diverse purposes.

Every day, personal data is given to these institutions and interests or, increasingly, simply taken by them to permit participation in the information ecosystem upon which many aspects of public and private life now depend. Those who want to participate, it is argued, must be willing to hand over their personal data.

It is no wonder why the World Economic Forum declared personal data as a new economic asset class or why analysts and officials were led to describe it as the 21st century's version of oil and the new currency of the digital world.

Types of Data Collected

The kinds, quantities, and values of personal data being given, or taken, are enormous and varied: employment histories, educational backgrounds, familial ties, social connections, professional networks, financial records, medical profiles, personal propensities, daily routines, and other everyday engagements, some of which people may

be unaware, are being collected and analyzed.

Personal data regarding who people are, who they know, who they are connected to, where they are, where they have been, and even where they may be going is being aggregated. It is consequently under threat by those who are able to harness and exploit it for their own benefit, usually to the detriment of those whose personal data it is.

For example, personal data is being created or collected

Personal data fundamentally belongs to the person it identifies, stands in for, and represents; it should not be treated as the property of powerful institutions or interests, governmental, corporate, or otherwise.

by powerful commercial enterprises for their own financial profit of which people tend not to receive any share. It also is being monitored by government agencies for their own Big Brother-esque surveillance and security activities, regardless of whether those being watched have ever been suspected of criminal activity.

The Threat of Datafication

These threats to personal data are, in fact, threats to people's physical selves. It is not simply a collection of meaningless bytes about random information abstracted from their lives. It is integral to their very personhoods, an informational extension or a kind of personal appendage that extends their lives into the informational (which increasingly means "digital") realm. This means that it is people – not just data – being exploited.

Personal data fundamentally belongs to the person it identifies, stands in for, and represents; it should not be treated as the property of powerful institutions or interests, governmental, corporate, or otherwise. As such, people have certain rights to their personal data. Indeed, personal data rights are basic human rights that must be recognized, respected, and protected.

There is particular urgency for the recognition of and respect for personal data as human rights because, as many aspects of people's lives continue to migrate online, they are, in turn, being datafied. Every transaction, interaction, connection, and contribution are being transformed into distinct data points to be aggregated with so-called big data sets in order to more effectively surveil individuals for diverse purposes.

Even those individuals who are not connected online are caught up in this digital panopticon as many mundane activities, from walking down a street to riding a bus or making a commercial purchase, are captured and datafied by various information communication technologies (ICTs). This datafication of people's lives seriously compromises personal privacy, confidentiality, trust, prospects, and security.

Balance Needed

Admittedly, there must be an appropriate balance between personal data rights and the legitimate and legal interests of those who may collect and use this information. There are some political and economic interests that are of societal and individual import, such as the refinement and delivery of particular social services, programs, or products.

But, as Aleecia M. McDonald from Stanford Law School's Center for Internet and Society reminds us, "We have learned the hard way that we cannot trust companies or governments to exercise basic decency and restraint in collecting [and managing, storing, using, etc.] our data."

For example, Edward J. Snowden's revelations of the U.S. National Security Agency's widespread surveillance practices, coupled with the complicity by many important players in the ICT and Internet industry, have serious (worldwide) political and economic implications for governments and corporations alike.

A March 21 *New York Times* article, "Revelations of N.S.A. Spying Cost U.S. Tech Companies," examined how these practices and their resulting violations of personal rights have negatively affected the bottom lines of many ICT and Internet companies and eroded much public and commercial trust in them. Indeed, there are substantive political and economic risks for governments, corporations, and other powerful institutions and interests that violate personal data rights.

A Call to Action

There is growing momentum for the recognition of personal data rights. Brazil recently approved the draft bill Marco Civil da Internet, heralded as a Constitution for the Internet that will enshrine individuals' rights to access and use the World Wide Web.

The European Union also recently approved new rules strengthening net neutrality to help ensure equal access to the Internet, and it is working on revised digital privacy regulations.

Tim Berners-Lee, the creator of the World Wide Web, recently called for a Magna Carta bill of rights for the Internet that should be considered on the same level as human rights. In a March 12 *BBC.com* article, "Tim Bern-

A Charter of Personal Data Rights

In response to the datafication of people's lives, which seriously compromises personal privacy, confidentiality, trust, prospects, and security, this charter of personal data rights is proposed.

Everyone has the following personal data rights:

- The right to own their personal data.
- The right to control and use their personal data.
- The right to privacy regarding their personal data.
- The right to anonymity regarding their personal data.

ers Lee: World wide web needs bill of rights," he challenges us "to make a big communal decision. In front of us are two roads: which way are we going to go? Are we going to continue on the road and just allow the governments [and corporations] to do more and more and more control; more and more surveillance? Or are we going to set up a bunch of values? Are we going to set up something like a Magna Carta for the World Wide Web and say, actually, now it's so important, so much part of our lives that it becomes on a level with human rights?"

He argues that we "have to be constantly aware, constantly looking out for [increasing encroachment on these rights] – constantly making sure through action, protest, that it doesn't happen." At the center of this call to action is personal data. When Internet rights are respected, so are personal data rights, and vice versa.

A Charter of Personal Data Rights

This article responds to Berners-Lee's call to action by proposing a Charter of Personal Data Rights. The aim is to increase awareness and contribute to the momentum towards ensuring that personal data rights are recognized and treated as human rights. This charter proposes four personal data rights, as explained below.

1. Everyone has the right to own their personal data.

As Ann Cavoukian, the Information and Privacy Commissioner of Ontario, Canada, noted in "Personal Data Ecosystem (PDE) – A *Privacy by Design* Approach to an Individual's Pursuit of Radical Control," "When individuals "When individuals go about their daily activities online, it is said that they also release, on average, 700 pieces of personal information a day. It is this stream of data that organizations profit from [that many of which] believe they have the right to control [and ultimately own] this information so that they can extract its value."

Governments and corporations increasingly treat personal data as their proprietary assets that they can collect, store, use, and reuse indefinitely and for whatever purposes they want; indeed, they regard personal data in a similar way to how the energy industry sees untapped reserves of oil and gas. It is theirs to use, distribute, and charge for as they please.

There is a saying that if you are not paying for the product or service, you *are* the product or service. Many online apps, services, and products are, seemingly, free of charge. But as MIT scholar Alex Pentland argues, "You have a right to *possess* your data." In "Reality Mining of Mobile Communications: Toward a New Deal on Data" from the *Global Information Technology Report 2008-2009,* he explains that third parties "should adopt the role of a Swiss bank account for your data. You open an account (anonymously, if possible), and you can remove your data whenever you'd like."

This charter supports this perspective, arguing that while individuals may consent to *share* some kinds of personal data, in limited and specific ways and for limited and specific reasons or functions, this consent does not mean that they have handed over ownership of their personal data. They have the right to both possess and determine how it will be used.

2. Everyone has the right to control and use their personal data.

By virtue of their right to ownership, individuals consequently have the right to determine how their personal data is created, collected, managed, stored, shared, and otherwise manipulated.

Pentland suggests that "if you're not happy with the way a company [or some other third party] uses your data, you can remove it. All of it. Everything must be opt-in, and not only clearly explained in plain language, but with regular reminders that you have the option to opt-out."

Further, individuals have the right to be informed about the processing of their personal data, which must comply with the original specific and limited reasons for which it was created or collected, as well as the right to correct it in cases of mistakes or misinformation.

This right to control and use personal data supports Cavoukian's call for "radical control" of personal data, which she describes as "the level of personal control necessary for an individual to exercise 'informational self-determination.'"

She explains that radical control should be enabled and protected by data protection policies and procedures adopted, and it should be designed and embedded within

ICTs and Internet services. ICTs, for example, should be formatted to enable individuals' control over their personal data when navigating, participating, and interacting within the digital realm.

Personal privacy, in many cases, is becoming a luxury good in this data-saturated world. Privacy comes at a literal and figurative price: those who want privacy have to pay for it through a company or service that claims to protect and ensure it …

3. Everyone has the right to privacy regarding their personal data.

People's personal data privacy is being continually encroached by many parties, from government agencies to ICT and Internet companies, who regard this information as theirs. Many powerful institutions and interests have growing desires for personal data resulting in their disregard for many basic privacy protections. People's privacy is compromised when they lack ownership, control, and use over their personal data.

Personal privacy, in many cases, is becoming a luxury good in this data-saturated world. Privacy comes at a literal and figurative price: those who want privacy have to pay for it through a company or service that claims to protect and ensure it; further, those who want to be connected have to give up some of their privacy. Thus, instead of privacy being the default, access to an individual's private life is, indeed, a matter of course.

But the right to privacy is a human right and a core principle of any free society. The right to privacy must be applied to personal data since it is an information extension of individuals.

Cavoukian, for example, proposes the idea of "privacy by design" built within ICTs, digital services and products, and other informational technologies and settings. Privacy by design would ensure that privacy is the default for all such systems and services instead of it being an afterthought or ignored altogether.

When privacy itself is the default, individuals will be able to better exercise their rights to own, control, use, and, of course, keep private their personal data. Privacy should not have any kind of price tag, literal or figurative.

4. Everyone has the right to anonymity regarding their personal data.

Anonymity through obscurity can no longer be assumed. This data-saturated world is achieving a level of surveillance over people's lives through their personal data that would have been the envy of the former East Germany.

As a scholar on digital security, Ron Deibert writes in *Black Code: Inside the Battle for Cyberspace*, "We no longer move about our lives as self-contained beings, but as nodes of information production in a dense network of digital relations involving other nodes of information production. All of the data about us as individuals…is owned, operated, managed, and manipulated by third parties beyond our control."

With personal data being increasingly collected, analyzed, and used, individuals lose their anonymity. Individuals' right to their personal data being and remaining anonymous requires them to be able to: have any or all of it either removed or erased by the party storing or using it; withdraw consent for or opt out of it being collected; and demand abstention from any further dissemination or use.

Applying the Charter

How can this charter be implemented? In a recent *Foreign Affairs* article, "Privacy Pragmatism: Focus on Data Use, Not Data Collection," Craig Mundie, the senior advisor to the CEO of Microsoft, offers five main recommendations that he refers to as "privacy pragmatism" that governments, companies, and individuals can take to protect their personal data.

1. Use metadata for access control.

The first step Mundie proposes is to annotate, or wrap, personal data in metadata at its point of origin. He asserts that this metadata wrapping "would describe the rules governing the use of the data it held [and] any programs that wanted to use the data would have to get approval to 'unwrap' it first."

2. Impose auditing requirements.

Robust legal and industry regulations should be established to "impose a mandatory auditing requirement on all applications that used personal data, allowing authorities to follow and observe applications that collected personal information to make sure that no one misused it and to penalize those who did," Mundie writes.

3. Encrypt data rights.

ICTs, software, etc. can use encryption and further metadata to embed personal data rights within their services, programs, and products, providing "individuals and organizations a simple and manageable way to protect confidential or sensitive information."

4. Connect data with verified identities.

Governments and the appropriate regulators must create and employ systems connecting legally recognized personal data to individuals. If an individual's preferences for his or her personal data are to be respected and enforced, the personal data must be verified to be that person's authoritative and correct information.

Mundie notes, moreover, that even with proper ways "to more rigorously connect individuals with verifiable online identities, three additional kinds of validated 'identities' would need to be created: for applications, for the computers that run them, and for each particular role that people play when they use an application on a computer." Thus, "only specific combinations of identities would be able to access any given piece of personal data."

5. Punish violators.

The final recommendation is to establish substantive penalties for the violation of personal data rights like privacy. Mundie writes that the violation of personal data rights should "be considered serious criminal offenses, akin to fraud and embezzlement – not like the mere 'parking tickets,' which would not deter rogue operators and companies."

Thus, if people believe their personal data has been violated, they could contact the appropriate regulator who, in turn, "would investigate and prosecute the abuse, treating it as a crime like any other."

Momentum for Charter of Personal Data Rights

As illustrated by Berners-Lee's Internet privacy campaign and the national legislation mentioned in this article, there is growing momentum for the right of people to control their personal data to be recognized as a human right.

There may be resistance and ridicule regarding the recognition of such a charter, particularly because it disrupts the current information practices of many government and corporate parties with vested interests in the status quo. Nevertheless, remembering that no one is exempted from the continuing and increasing expropriation of personal data, it is crucial that these rights be recognized and respected. **END**

Editor's Note: This is the first in an occasional series of editorial/opinion articles meant to provoke reader feedback, including comments and counter-point articles. Send your comments or completed article proposal forms (available at *http://archive.arma.org/imm/IM%20Mag%20Proposal%20Form.doc)* to *editor@armaintl.org*.

Marc Kosciejew, Ph.D., *can be contacted at* mkosciej@gmail.com. *See his bio on page 47.*

Leveraging the Principles in Mergers, Acquisitions, and Divestitures

Despite the upheaval that comes with merger, acquisition, and divestiture activities, they provide great opportunities for organizations to assess and improve their information governance practices.

Julie Gable, CRM, FAI

Industries as diverse as hospitals, pharmaceuticals, airlines, law firms, utilities, and non-profits have all experienced high levels of merger and acquisition activity in recent years. According to the Institute of Mergers, Acquisitions and Alliances, a non-profit think tank that researches the subject, there were more than 130,000 such transactions from 2000 to 2010.

At best, mergers and acquisitions are the melding of two cultures to produce a single, stronger entity. At worst, they are politically fueled wars about which processes and systems will dominate once the dust settles. Records and information management (RIM) programs are often caught in the fray because information assets play a pivotal role in mergers and acquisitions. Most often, the acquirer or the larger firm in the merger assumes its information governance program is superior, when that may or may not be true.

In merger and acquisition scenarios, the Generally Accepted Recordkeeping Principles® (the Principles) and the Information Governance Maturity Model (IGMM) provide standards-based, objective ways to coolly assess where the strengths

and weaknesses of each party's RIM program lie, removing the competitive "Our program is better than your program" atmosphere and focusing instead on the opportunity to combine the programs with an eye to overall improvement.

Conversely, changes in regulatory climate and new technologies in industries such as energy and communications have made it profitable to spin off or divest certain subsidiaries into stand-alone companies. Newly divested companies may find themselves with gaping holes in information policy and practices that were once supplied by the parent company. How to plug the gaps becomes an important priority for the new company.

For divested companies, the Principles and the IGMM can be used to identify what needs to be done to shore up and supplement RIM programs that lack the features and focus of their more established parent company's programs.

The case studies of fictional companies below illustrate how the Principles can be used in acquisition and divestiture settings.

Case Study 1: Arix Acquires Nemestan

Arix, established in 2001, is a pharmaceutical company that has grown chiefly through acquisition. Each acquired company produced a specific product at one or more locations globally.

Previous Acquisition Practices

Upon acquisition, records were left in place at the acquired company. Paper records may have been stored at one or more offsite storage facilities, and electronic records occupied the expected mix of document management systems, specialized quality systems, file shares, and storage devices.

Many of the previously acquired companies had some components of RIM, but there was never any formal study of which company had which elements. Each company did its own thing with regard to regulatory compliance, retention schedules, policies, procedures, and tools such as records management software. So far, regulatory audits have gone smoothly, and Arix has never had a serious lawsuit.

Newly divested companies may find themselves with gaping holes in information policy and practices that were once supplied by the parent company. How to plug the gaps becomes an important priority for the new company.

Corporate RIM Established

About a year ago, Arix established a formal RIM department at the corporate level. The new RIM function is working on global policies and retention schedules that can be disseminated to all locations. It is hoped that these will serve as a uniform framework that can be adapted for managing records locally. The RIM department is also developing policies to protect records that are considered private, confidential, or privileged, as well as standardized metadata for all records.

Arix is also evaluating records management software as part of an effort to unify records management practices throughout all companies. The software will require standardized classification and metadata for managing paper and electronic records. Most of the line managers at Arix's various locations welcome the chance to shed inconsistent indexing procedures in the hope that better metadata will mean better search results.

The records software will allow legal, tax, and other holds to be placed on paper and electronic records, but this hold functionality may not matter because there have never been formal retention schedules, and Arix has never disposed of anything, living by the credo "storage is cheap."

The Arix records program is staffed by one manager, one analyst, and various contractors hired to produce specific pieces of the records program such as procedures and training materials. Arix's RIM department reports through the IT department.

A New Acquisition

Last year, Arix announced that it would acquire Nemestan, a maker of vaccines. Though relatively small compared to Arix, Nemestan has had a formal RIM program almost from its inception, with a centralized management structure for mostly paper and some electronic records – usually images of paper documents.

Nemestan takes an archival approach to its business records, preferring to err on the side of preserving more than is needed, rather than aggressively disposing of records the moment full retention is reached. There are approved policies, procedures, and retention schedules that apply to U.S. locations, and Nemestan is developing audit criteria for judging records management compliance and effectiveness. The company also wants to extend the program to its non-U.S. locations.

The company has invested in software for maintaining records inventory, and there are many metadata fields to aid in searching. Indexing is done at the box level, the folder level, and in the case of electronic records, at the document level.

Nemestan's program is staffed by four full-time people, including a manager, an assistant manager, and two records analysts. The records group reports to the law group. Because it has no way to reliably attach legal holds, Nemestan has never destroyed anything.

After the initial period of non-communication, the manager of Arix is ready to meet with his counterparts at

Principle	Level 3 (Essential) Elements	Arix Score	Nemestan Score
Accountability	The company includes electronic records in RIM program.	3	2
Transparency	It has written policy regarding transparency.	3	1
	Employees are educated.	2	1
	Business & RIM processes are documented.	2	3
	It can handle most requests for information, e.g., discovery, regulatory response, FOI.	2	3
Integrity	A formal process to ensure authenticity and chain of custody can be applied to systems and processes.	1	1
Protection	It has a formal written policy on protection.	3	1
	RIM audits are conducted only in regulated business areas.	3	1
Compliance	A hold process is integrated into information management and discovery processes for critical systems, and it is effective.	1	1
Availability	A standard for where and how records are stored, protected, and made is available.	2	3
	It has clear policies for information handling.	2	3
	Retrieval methods are consistent.	2	3
	It is easy to determine where to find the authentic and final version of information.	2	3
	Legal discovery and information request processes are well-defined and systematic.	1	1
	Systems and infrastructure contribute to records availability.	2	2
Retention	A retention schedule tied to regulations is consistently applied.	2	3
Disposition	Official procedures for records transfer and disposition exist.	1	1
	Official policy and procedures for suspending disposition have been developed.	1	1
Totals		**35**	**34**

Figure 1: Comparing Tangibles – Arix & Nemestan

Nemestan to find out what they have in the way of information governance and how it fits with Arix's plans. Arix does not want this acquisition to be like the others with yet another silo of records managed without corporate supervision.

A New Way Forward

To systematically determine the companies' similarities and differences, the Arix records manager has prepared a chart based on the Principles and the IGMM Level 3 (Essential) descriptions of information governance program elements that are indicators of basic good practices. For his comparison, the Arix records manager concentrates only on information governance program aspects that are tangible and transferable, focusing on what is measurable and what would be useful going forward as the two programs merge.

As a first step, he honestly rates the aspects of Arix's program, with a score of 1 if the element does not exist, 2 if the element is being worked on, or 3 if the element is a delivered part of the information governance program. Following conversations with his counterpart at Nemestan, he also rates each aspect of the Nemestan program using the same scale, producing Figure 1: "Comparing Tangibles – Arix & Nemestan" above.

Not the Most Points, the Most Value

Adding up the points, Arix "wins," but that isn't the objective of the exercise. A careful look at the chart shows that Nemestan has potential value to offer in regard to the Principles of Availability, Transparency, and Retention, where it has already achieved at least the Essential Level 3 in the areas of storage standards, policies for information handling, consistent retrieval, and retention schedules.

These are worth further investigation to see where synergies may exist and how Arix could possibly raise its own levels in these areas by capitalizing on work done by Nemestan. It

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

CRM

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

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

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

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

ICRM®
Institute of Certified Records Managers

Principle	Essential Aspects Required for Stream
Accountability	• Hire a records manager at the right level to have strategic impact on the company. • Make senior management aware of the records program and ask for their support. Find a senior manager to be the records champion. • Establish an information governance steering committee. • Define goals related to accountability and a timeline for their accomplishment.
Compliance	• Formulate the company's overall code of business conduct. • Document a rudimentary hold policy and process and ensure they can be complied with now and in the future.
Transparency	• Update business and records policies inherited from Mega. Are these usable and practical at Stream? Define goals related to information governance transparency.
Availability	• Establish best practices for responding to requests for information by customers, regulators, auditors, and others. • Consider prioritizing projects that have the objectives of consistent indexing, records classification, and retention codes.
Retention	• Revise the inherited retention schedules so they are applicable to Stream's legal, fiscal, operational, and historic requirements. • Make records training mandatory for all employees.
Disposition	• Establish uniform procedures for disposition–for example, describe what approvals are needed to dispose of records. • Establish procedures for suspending disposition.
Integrity	• Lay the groundwork for a project to ensure that some standardized metadata elements are captured for all of the company's electronic records.
Protection	• Examine how physical records will be kept while they are active, as well as when they are inactive. For example, are there locked rooms onsite? Who may retrieve boxes from offsite storage? • Work with information technology to ensure that systems containing sensitive or private information have adequate safeguards in place.

Figure 2: Divested Stream Energy's Priorities

is important to remember, though, that work developed for a U.S.-based company may not have specific applicability outside U.S. borders.

On the other hand, areas of the chart showing a Level 1 for both companies indicate aspects that need work. In this case, the formal processes to ensure authenticity under the Principle of Integrity, the hold process under Compliance, the legal discovery process under Availability, and procedures governing Disposition are weak for both companies. These can form the basis for a RIM strategic plan for the merged companies going forward.

Case Study 2: Mega Power Divests Stream Energy

Mega Power is an energy conglomerate that wanted to raise cash to finance its newly developed shale exploration division. With competition increasing in the electric power marketplace, Mega has changed its strategic direction to focus on future technologies and revenue sources. Mega decided to divest Stream Energy, its electric power division. Stream will be a free-standing entity, with stock sold through an initial public offering.

Mega's RIM Program

As part of Mega, Stream had the benefit of using records management

services supplied by Mega's corporate services group. RIM at Mega is a mature program that covers both paper and electronic records. Mega has its own paper archives, its own software for managing them, and a competent staff who easily handles their storage and retrieval.

In addition, Mega has in-house, centralized services for document imaging. Mega also has invested in document management technology for its unstructured records, and progress is being made in applying retention to electronic records in these systems.

The RIM program staff consists of a corporate records manager, six analysts, and several liaisons who are responsible for records management within each division. Several of the records liaisons for Stream have opted not to go to the divested company, so some records management knowledge has been lost.

Stream's RIM Program

Stream has appointed an attorney to be responsible for records management for the divested company. He has received a report of the records inventory, and asset transfers from various systems will be made where possible. Some data, such as that for accounting, human resources, and finance, will be outsourced to third-party organizations. Stream has Mega's retention schedule and copies of Mega's policy and procedures. Much more is needed to ensure that the new company can manage its information needs.

Of the many challenges facing Stream, one of the greatest is how to structure a records and information governance program that can serve the present and future needs of the new entity.

Using the Principles in Divestiture

Stream's acting records manager knows he needs to establish a program as robust as the one everyone knew at Mega. However, this can't happen overnight. Each element of a sound RIM program takes time to develop. Determining where to start, what to work on, and in what order are important.

…organizations that participate in merger, acquisition, and divestiture activities have great opportunities to take a critical look at RIM policies and practices with an eye to improvement.

The immediate need is to make sure that Stream has received all of its records and information from Mega per the terms of the divestiture. The next is to make sure that there are adequate systems and storage for information needed to conduct daily business.

As an attorney, Stream's acting records manager is highly aware that managing information is crucial. While he has plenty of comprehensive documentation about how to do RIM processes from Mega, what he doesn't have is a way to structure the RIM culture. Without this structure, policies, procedures, schedules, and training are just words on paper. Furthermore, what worked as policy infrastructure for a large records program may not be appropriate for an entity that does not yet have the resources to support it.

The attorney decides to look through the IGMM as a way to understand what needs to be done, to set goals for Stream's RIM program, and to measure progress. Looking at the column for Level 3 – Essential, he formulates Figure 2: "Divested Stream Energy's Priorities" (on page 36) as the initial path toward setting up a RIM program to meet Stream's needs.

Note that he has put the Principles in a different order to indicate priorities. While everything on the chart is essential, the Principle of Accountability will take first priority. If the new company's culture can grow to be information governance aware, it must start at the very beginning with executive sponsorship and recognition of the RIM function. Looking at the remainder of the chart, the attorney realizes what a tall order it is, but he also knows he has a sound plan to follow going forward.

Change Provides Challenges, Opportunities

Those who have been through mergers, acquisitions, and divestitures often cite change management and culture change as some of the greatest challenges in moving forward. This is because people become used to doing things in certain ways, and they don't want to change.

Time is also a factor; many RIM initiatives require the participation and commitment of those who know the business processes. These are often the same people charged with keeping the business moving forward. They can be overwhelmed, particularly in cases where new technology comes with the new situation.

Despite the upheaval, organizations that participate in merger, acquisition, and divestiture activities have great opportunities to take a critical look at RIM policies and practices with an eye to improvement. Used well in merger and acquisition, the Principles and the IGMM can provide a framework for objectively assessing RIM programs to take advantage of the strengths of all parties and to identify where more work will be needed. For divestitures, the Principles and the IGMM are like girders in construction projects, providing a foundation on which the next levels can be built from the ground up. **END**

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

How to Conduct a Records Survey

Ann Bennick, Ed.D., CRM, and Judy Vasek Sitton, CRM

The *records survey*, a high-level assessment tool, focuses on identifying the various records categories that are created, processed, or received by the organization or a department within a larger organization. Use a records survey form or at least a standardized list of questions (with blanks for recording comments) to guide your interview.

If you are conducting the project alone at this stage, gather the information in a manner that conforms to your work style. If you are managing a team of analysts, standardize the information-gathering format. See Figure 1: Sample Blank Records Survey Form on page 43.

The purpose of the survey is to determine major records series or categories that end users create, receive, process, or maintain in their ongoing work. The survey is most effective when an individual trained in records survey techniques conducts interviews of key employees who use the records. A skilled records analyst can anticipate the record types usually created or maintained by a certain function and ask leading questions to trigger information about those records.

Questionnaire vs. Interview

Another method, called the *questionnaire method*, is sometimes used instead of or in advance of having a trained analyst conduct interviews. As indicated by the process name, a questionnaire or form is sent directly to the user. If your users understand the objectives of the survey, know how to calculate file volume and capacity, understand retention schedules and records management benefits, you might get reasonably good results. If you narrow the focus and train the users in completing the questionnaire, your results will be more reliable.

However, the authors do not advise solely using the questionnaire method or using the questionnaire without training the users. The analyst brings away from user interviews much more than the checked boxes and brief notes on a form. Impressions and awareness of the department's records needs and interactions with other groups, when interpreted in light of the analyst's knowledge and experience, cannot be replaced.

Interview Questions

When conducting the survey by the interview method, have explanatory comments and other forms of the questions in mind in case the end user does not understand the initial question. The additional questions and comments are intended to help you better understand the objectives of and the results desired from the survey. Use these questions as explanatory or follow-up information to ensure that you get comprehensive responses.

Who is being interviewed? List the organization name, name of the person interviewed, office location, telephone number, or other location information. If you know ahead of time that the individual being interviewed works with many records categories, look up the location information in the company directory, enter it on one form, and copy that form for additional categories.

Another method is to number and compile each end user's survey forms (1 of 15, 2 of 15, etc.) and complete the location information only on the first page. Put enough information on each page to ensure that you can trace it back to the right person.

Is the individual being interviewed representing a larger group of employees? If so, make a notation indicating which work group. In very large organizations, one or two individuals may be designated to provide information for a larger group of employees with the same general responsibilities.

What is the major activity or function of the organization or subgroup within the organization? This information helps you understand the relationship of the records and their contribution to the workflow of the organization. Get a comprehensive description – "processes accounts payable invoices, customer complaints; interfaces with vendors and company personnel regarding accounts payables" – is a much better response than "accounting."

What is the records category name? *Remember to use a separate form for each major group of records created, received, maintained, and processed by the individual.* Ask the user to describe the record category. By knowing what users call the records, you are collecting key retrieval terms for incorporation into the file classification/taxonomy and/or retention schedule. Verify that the user is describing only one records series.

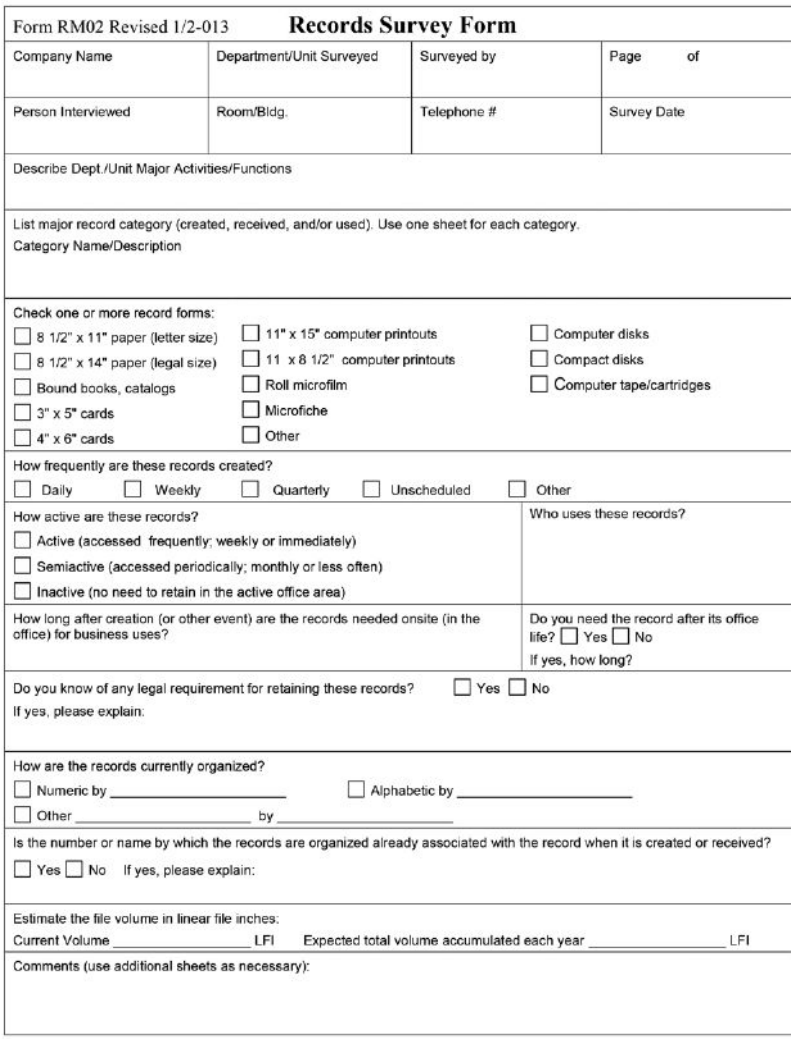
For example, "accounting records" is too broad. Ask for specific examples, such as "accounts payable invoices" or "customer complaints," and complete a records survey form for each series.

What is the usual records format? Check one or more formats on the survey form. Modify the survey form provided [with this article] if it does not include the record formats, choices, and questions appropriate to your organization.

Ask whether the record format is satisfactory. Has the user experienced any problems with using the records that can be attributed to its format? If so, determine the cause. For example, *microfiche files* (4" x 6" film containing an eye-readable header and reduced images, usually arranged in a grid pattern) that are difficult to find could be attributed to:

- An inadequate indexing system for the microfiche
- An inadequate eye-readable header
- The absence of controls for removal of a microfiche from its normal location
- A format that impedes access to documents

When the format indicated is electronic or digital, ask for specific system and application names, which will assist in ESI **data mapping**. (See Chapter 5 [of *Managing Active Business Records]* for more on data mapping.)



Form RM02 Revised 1/2-013 **Records Survey Form**

Company Name	Department/Unit Surveyed	Surveyed by	Page of
Person Interviewed	Room/Bldg.	Telephone #	Survey Date

Describe Dept./Unit Major Activities/Functions

List major record category (created, received, and/or used). Use one sheet for each category.
Category Name/Description

Check one or more record forms:

- ☐ 8 1/2" x 11" paper (letter size)
- ☐ 8 1/2" x 14" paper (legal size)
- ☐ Bound books, catalogs
- ☐ 3" x 5" cards
- ☐ 4" x 6" cards
- ☐ 11" x 15" computer printouts
- ☐ 11 x 8 1/2" computer printouts
- ☐ Roll microfilm
- ☐ Microfiche
- ☐ Other
- ☐ Computer disks
- ☐ Compact disks
- ☐ Computer tape/cartridges

How frequently are these records created?
☐ Daily ☐ Weekly ☐ Quarterly ☐ Unscheduled ☐ Other

How active are these records?
☐ Active (accessed frequently; weekly or immediately)
☐ Semiactive (accessed periodically; monthly or less often)
☐ Inactive (no need to retain in the active office area)

Who uses these records?

How long after creation (or other event) are the records needed onsite (in the office) for business uses?

Do you need the record after its office life? ☐ Yes ☐ No
If yes, how long?

Do you know of any legal requirement for retaining these records? ☐ Yes ☐ No
If yes, please explain:

How are the records currently organized?
☐ Numeric by _____ ☐ Alphabetic by _____
☐ Other _____ by _____

Is the number or name by which the records are organized already associated with the record when it is created or received?
☐ Yes ☐ No If yes, please explain:

Estimate the file volume in linear file inches:
Current Volume _____ LFI Expected total volume accumulated each year _____ LFI

Comments (use additional sheets as necessary):

Figure 1: Sample Blank Records Survey Form

How frequently are the records created? Are records created daily, weekly, or on no set schedule? High-volume records may be candidates for an image or online application, particularly if they also have high reference requirements and/or are accessed by many people in remote locations.

How active are the records? How often is a record referenced or recalled after its creation or receipt by the organization? The survey form gives three choices:

- *Active* (accessed frequently such as weekly or immediately)

- *Semiactive* (accessed periodically such as monthly or less often)
- *Inactive* (no need to retain records in the active office area or server)

Who uses the records? Do only one or two individuals use the records, or are records shared throughout the department or company? Do other departments also use the records? Answers to these questions can provide support for formal charge-out systems and can help determine the appropriate level of centralization of physical records. These answers may also highlight an opportunity for changing the record format from paper to image (microform or electronic image) or online application.

How long after creation (or other significant event) are the records needed in the office or in an active server environment for business use? This period of time identifies a preliminary office retention period for the records. Significant events that signal the beginning of a records retention "countdown" include events such as termination of an employee, expiration of a contract, or completion of a project.

Record the event that triggers retention as well as the time that the record is required in the office after that event has occurred. Even if the documents are needed in the office only a relatively short time, if reference volume is high, dispersed, and immediate need exists, changing the format of the record should be investigated.

Are the records ever needed after their initial use (office life) has expired? If so, how frequently and over how long a period? This information indicates whether the organization may need offsite or offline storage of the records.

Does the user know of any legal requirements for retaining these records? Users, especially in regulated industries, are often aware of current laws or regulations.

Knowing legal requirements early in the process can save research time and facilitate development (or verification) of the retention schedule. Verification and review by a company attorney, however, is important before establishing or changing official retention periods.

How are the physical records currently organized? Are they in alphabetic, numeric, or alphanumeric order? By what data element are they organized (such as alphabetic by customer name, etc.)?

Is the current organization of records effective, and are the records easy to find? If users can easily find information, recommend continuing this organizational method. As the old saying goes, "If it isn't broken, don't fix it." However, you will need to compare your interview subject's perception against the perception of others who use the same records. Determine whether a user who is new to the department would also find it an "easy-to-locate" records series.

Is the name by which the records are organized (sequence key) already associated with the record at the time it is created or received? Using an existing key – its natural order – as the document's normal sequence is often the best way for users to find it. If a natural order of the record is identified and the current filing order is different, consider changing to the natural order.

However, if customer files are currently arranged alphabetically by name, but every document filed includes a printed customer number, customer number may be a better filing order, especially if the customer records series is very large. Do not just assume that the natural order should always be used.

Can retention schedules be used in lieu of a records survey? If the company or organization has a retention schedule, this schedule may serve as a validation tool, negating the need for conducting a formal records survey. This validation should demonstrate that the retention schedule is comprehensive, includes full descriptions, and identifies any regulatory citations that identify legal requirements for length of retention for the series. Propose, as additions to the retention schedule, any records series not listed on the schedule but discovered during earlier stages of the project.

Even if you have a retention schedule, you need to conduct a records survey if the retention schedule has not been recently reviewed.

Analyze the information gathered from the records survey or validated retention schedule. Records survey results can provide preliminary file classification/taxonomy and retention information and can assist in mapping digital records systems. **END**

Ann Bennick, Ed.D., CRM, can be reached at abennick@pineneedlelodge.com. *Judy Vasek Sitton, CRM, can be reached at* info@pacotech.com. *Their bios are on page 47.*

Editor's Note: *Managing Active Business Records*, from which this article was excerpted, is available for purchase from the ARMA online bookstore at *www.arma.org/bookstore.*

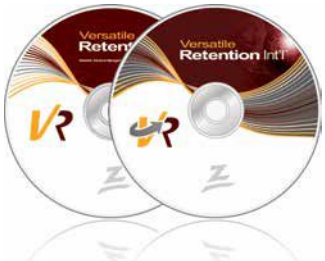
BULLETIN BOARD

Privacy+ is an international certification program open to all companies providing outsourced storage and protection of hard-copy records and off-line removable computer media. Participation in Privacy+ is voluntary and allows companies to publicly demonstrate their commitment to protecting the privacy of information entrusted to them by their clients. Privacy+ certification is owned and administered by PRISM International (Professional Records & Information Services Management), the not-for-profit trade association for the commercial information management industry. Look for the Privacy+ logo, ask for it in your RFPs, and expect your records and information management partners to have it. For more information, please visit ***www.prismintl.org.***

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

ZASIO

Zasio Enterprises, Inc.
Versatile Retention™
Versatile Retention Int'l™



Get your hands on Zasio's latest version of Versatile Retention. With over 40,000 legal citations containing records retention requirements, this intuitive software will help you keep your retention schedule — whether domestic and/or international — up-to-date, easily accessible, and legally compliant.

To learn more about the latest release of our retention management software solutions, visit: ***www.zasio.com/company-news-releases.asp.***

RSD announced RSD GLASS 3.2, the latest version of its patent-pending platform used to power global corporate information governance programs for electronic and physical content. Key enhancements and additional features within its Policy Manager, Governance Manager and Governance Dashboard modules further broaden the functionality of this proven platform. Create and enforce corporate policies across organizational and jurisdictional boundaries, IT systems, content repositories, cloud-based applications and paper archives. Learn more at ***www.rsd.com/en/products/rsd-glass***.

Recall Holdings Limited (ASX: REC), a global leader in information management, announced that it was awarded ISO/IEC 27001:2005 Management System certification by SRI Quality System Registrar on December 19, 2013. Recall is the first information management company to achieve ISO27001 Certification for all global operation centers. ISO/IEC 27001:2005 is a process-based certification recognizing organizations that can link business objectives with operating effectiveness. Recall's Global ISO27001 Certification demonstrates excellence in Information Security Management System (ISMS) planning, deployment, and provisioning services that support IT infrastructure to protect information and enable the associated secure service delivery processes to Recall employees and customers.

XACT DATA DISCOVERY (XDD) is an international discovery and data management company providing streamlined forensics, processing, hosting, document review, project management, and paper discovery services for corporations, law firms, and government agencies. XDD has offices throughout the U.S. and two locations in India, and recently added a domestic review option to its managed document review services. Visit ***www.xactdatadiscovery.com*** for more information.

Balancing the Risks and Rewards of Cloud-Based Healthcare Information

Rebecca N. Shwayri, J.D.

We are in the early stages of the electronic health record (EHR) era. And while EHRs offer many benefits, their proliferation is presenting challenges that some healthcare organizations are not equipped to handle.

For example, storing, harvesting, and accessing EHRs on a regular basis require significant investments in technology and personnel. To mitigate these costs, many healthcare organizations use cloud vendors for these services, which has some inherent risks. Storing EHRs in the cloud is still a good option, though, if organizations take the appropriate steps to mitigate these risks.

Cloud Benefits and Risks

The benefits and risks of outsourcing EHRs to the cloud are both quantitative and qualitative.

Benefits

On the benefit side, using a cloud vendor can dramatically reduce costs and enhance patient outcomes.

First, by deploying a cloud solution, the organization need not pay for hardware or the IT personnel that would be required to maintain EHRs onsite. In addition, a cloud option can be deployed to address an exponential increase in EHRs more quickly and cost-effectively than an onsite solution can be.

Second, deploying a cloud solution has the potential to enhance patient outcomes. When informa-

tion is stored in the cloud, physicians can access it at any time and can collaborate with hospitals and other physicians regarding a patient's care.

Risks

On the risk side of the equation, using a cloud solution could increase liability if the cloud vendor is not compliant with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the 2013 HIPAA Omnibus Final Rule, which provides a more expansive definition of "business associates" that likely encompasses most cloud vendors.

According to the January 25, 2013, issue of the *Federal Register* (available at *www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf*), "…a data storage company that has access to protected health information (whether digital or hard copy) qualifies as a business associate, even if the entity does not view the information or only does so on a random or infrequent basis. Thus, document storage companies maintaining protected health information on behalf of covered entities are considered business associates, regardless of whether they actually view the information they hold."

While the Omnibus Final Rule imposes direct liability for security breaches on business associates, covered entities (like healthcare providers) are also liable.

While deploying a cloud solution can enhance patient outcomes, it can also detrimentally impact a patient in an emergency situation if vital health information stored there is not available. In addition, a security breach of that cloud-based information might expose additional patient information such as financial data, name, and address, which can be used to wreak havoc on an unsuspecting victim.

There is also the potential for violating international data privacy laws if EHRs are held on cloud servers located outside the United States.

Further, data stored in the cloud must be accessible and produced if it is relevant to litigation. Properly implementing a litigation hold and producing data stored with a cloud vendor can be difficult, and failure could subject the organization to sanctions for spoliation of evidence.

Security Issues in the Cloud

Records managers working within the healthcare industry need to be intimately familiar with HIPAA's Security Rule in order to mitigate the risks and liabilities from using a cloud vendor to hold electronic records. The Security Rule applies to health plans, healthcare clearinghouses, healthcare providers, and business associates.

Records managers working within the healthcare industry need to be intimately familiar with HIPAA's Security Rule …

Pursuant to the HIPAA Omnibus Final Rule referenced above, subcontractors that create, receive, maintain, or transmit protected health information (PHI) on behalf of business associates are now also business associates and must comply with the Security Rule. This more expansive definition of subcontractors encompasses most cloud vendors. Thus, a healthcare organization should ensure that the cloud vendor operates within the parameters of the Security Rule.

The Security Rule explains certain steps a covered entity must take to:

- Ensure the confidentiality and integrity of PHI
- Protect electronic PHI against any reasonably anticipated security threat or hazard
- Protect against any reasonably anticipated uses or disclosures of electronic PHI
- Ensure the covered entity workforce's compliance with the Security Rule

The Security Rule delineates several types of safeguards that are administrative, physical, and technical in nature.

Safeguards

Administrative safeguards are policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic PHI. They may include such measures as conducting risk assessments to evaluate whether electronic PHI is vulnerable, developing an incident response plan to deal with a security breach, and creating policies for establishing access to sensitive systems that permit access to electronic PHI.

Physical safeguards encompass physical measures, policies, and procedures to protect a covered entity's electronic information systems and equipment from natural and environmental hazards and unauthorized intrusions.

Technical safeguards are the technologies, policies, and procedures for electronic PHI's use that protect and control access to it. Technical safeguards include audit controls to monitor activity in sensitive IT systems and encryption of data transfers.

Mitigating Security Risks

Utilizing a healthcare cloud storage solution can result in significant cost savings. Often, the cost savings can outweigh the risks if an organization takes appropri-

ate steps to mitigate them.

First, a healthcare organization should assess the cloud vendor's compliance with HIPAA. Do not take the cloud vendor's word at face value. Ask to examine its audit reports and its administrative, technical, and physical safeguards.

Explore the possibility of procuring cyber risk insurance to cover privacy-related risks. The cloud vendor could buy this insurance and name the healthcare organization as an insured or beneficiary under the policy. Cyber risk insurance can provide coverage for a data breach. While many companies carry commercial general liability insurance policies, such policies may not always cover the expenses of a data breach.

Third, there are litigation risks a healthcare organization could face if it uses a cloud vendor. For example, vendor-held information may be the subject of litigation, and the organization may need quick access to produce it for the court.

To appropriately address litigation risks, the contract should state that the healthcare organization owns the data in the cloud. The contract should also delineate what would happen in case of litigation and the steps to be taken when a hold is implemented. Before engaging a cloud vendor, carefully evaluate the vendor to ensure it has the capabilities to respond to large-scale litigation or regulatory requests.

Editor's Note: The Cloud Vendor Questionnaire on page 45, which was excerpted from ARMA International's *Guideline for Outsourcing Records Storage to the Cloud,* addresses a number of other issues an organization should investigate when considering a cloud services vendor. This guideline includes a broader discussion about retention, disposition, legal, privacy, technology, and security issues related to cloud-based storage and other tools for evaluating cloud vendors.

Balancing Benefits, Risks

Using a cloud vendor can have considerable benefits for a healthcare organization, including dramatic cost reductions, easy access to data from any location, and the facilitation of better healthcare outcomes. On the negative side, using a cloud vendor may result in additional privacy, security, litigation, and regulatory risks. These risks can result in major expenses, damage to reputation, and loss of market share in case of a data breach.

Determining whether to use a cloud vendor requires a balancing of quantitative and qualitative benefits and risks. Within your organization, determine the cost of additional hardware, software, and IT personnel if your organization were to store all of its data in-house. The technology-related cost savings represent one of the most significant quantitative benefits.

The risk of a privacy breach is most noteworthy, with the potential costs running into the millions of dollars. However, these risks can be mitigated with appropriate auditing procedures and cyber risk insurance.

In most cases, the quantitative and qualitative benefits of the cloud outweigh the risks as long as appropriate quality control metrics are put in place. **END**

Rebecca Shwayri, J.D., can be reached at rebecca.shwayri@akerman.com, *See her bio on page 47.*

Cloud Vendor Questionnaire

1. Are vendor terms and conditions consistent with the organization's goals and objectives?
2. Under what conditions, if any, will the vendor allow independent audits of systems and processes?
3. Where are the vendor's physical servers located?
4. Can the vendor provide international diversification with hubs in various geographic locations?
5. How long has the vendor been in business?
6. How long has the vendor been providing cloud-based services?
7. Who are some current clients of that vendor?
8. Can the vendor provide public, private, or hybrid cloud environments? (Circle all that apply.)
9. Can the vendor separate data depending on the data type?
10. Does the vendor have a firewall that will adequately address security-related needs?
11. Are data encrypted when using a public cloud environment?
12. What does the disclosure policy say about data on the vendor's systems?
13. Does the vendor offer redundant systems?
14. Does the vendor offer guaranteed uptime?
15. Does the vendor have redundant Internet connections?
16. Does the data center have adequate environmental control features?
17. Is the data center conveniently located (geographically)?
18. Is the perimeter of the data center protected?
19. Does the data center have a visible security presence such as a guard or monitoring cameras?
20. Is the data center location secured with systems to provide authorized access?
21. Is the data center located in a country where geopolitical instability may be problematic?
22. Identify the geographic locations the virtual environment spans.
23. Is the data center located near known or potential hazards?
24. Are applications and information distributed across systems?
25. Will data be stored so that it is segregated from (rather than commingled with) other organizations' data? If yes, specify how, i.e., what hardware and software are used?
26. Has the vendor's backup strategy been reviewed?
27. Is a backup done using disk to disk or tapes or other methods? (Circle all that apply.) Describe other methods.
28. Where are backup media located?
29. What types of drives are used for backups and are replacements available? Are they replacements?
30. How often are backup media rotated?
31. What types of redundant network links are available?
32. Can the vendor demonstrate a business continuity plan?
33. Are business-critical applications being hosted?
34. Is the data center designed around a virtualized environment?
35. Are the data on virtualized servers?
36. How is retention managed in a virtualized environment?
37. Is access to system configuration and/or administrative functions tightly controlled? Who can make changes to settings?
38. Are encryption and control lists in place to reduce the risk of inappropriate access?

Source: *Guideline for Outsourcing Records Storage to the Cloud* © 2010 ARMA International. (This publication is available for purchase at *www.arma.org/bookstore*.)

ARMA INTERNATIONAL®

Introducing the official

Information Governance Assessment

Based on a large body of generally accepted practices, international- and national-level standards, and legal and regulatory requirements, the **Information Governance Assessment** provides an authoritative and objective means of measuring your organization's information governance (IG) program's maturity.

The **IG Assessment** can be used to:

- Identify your organization's IG maturity
- Track deficiencies by principle and overall score
- Monitor the progress of risk mitigation efforts
- Assess the sufficiency of IG training and documentation

Find out how the **IG Assessment** can work for you!

Visit ***www.arma.org/assessment***

Contact: **Elizabeth Zlitni**
+1 888.279.7378 (U.S., Canada)
+1 913.217.6015 (international)

Contact Information

AUTHOR INFO


BENNICK


GABLE


KOSCIEJEW


PHILLIPS


SHWAYRI


VASEK SITTON

Plug Internal Data Leaks with an Effective IG Program Page 20

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

Point of View Proposing a Charter of Personal Data Rights Page 27

Marc Kosciejew, Ph.D., is a lecturer of library, information, and archives sciences within the Faculty of Media and Knowledge Science at the University of Malta. His current research interests include the intersections of society and technology, records and information management, concepts and practices of information, and the histories of libraries and information. Kosciejew received his master's degree and Ph.D. in library and information science from Western University (formerly the University of Western Ontario) in London, Ontario, Canada. He also holds certificates in web search strategies, records management, and freedom of information and protection of privacy from the University of Toronto. He can be contacted at mkosciej@gmail.com.

The Generally Accepted Recordkeeping Principles® Leveraging the Principles in Mergers, Acquisitions, and Divestitures Page 32

Julie Gable, CRM, 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*.

How to Conduct a Records Survey Page 38

Ann Bennick, Ed.D., CRM, operates a Texas-based records and information management (RIM) consulting business. She is a Certified Records Manager with more than 30 years of experience, including as an in-house consultant for a multinational energy company that received the prestigious Olsten Award for the outstanding large company RIM program; a tenured business professor at a Texas community college; and a frequent speaker and writer for educational and professional organizations. Bennick received her doctorate and prior degrees from the University of Houston in Houston, Texas. She can be reached at *abennick@pineneedlelodge.com*.

Judy Vasek Sitton, CRM, is director of information governance – consultant for PacoTech, Inc., a full-service information management consulting and outsourcing solution provider. A Certified Records Manager for more than 25 years, she previously designed, implemented, and managed records systems for oil and gas companies, a high-tech manufacturing industry leader, and a world-class healthcare institution. Vasek Sitton has authored several articles for national publications and is a frequent speaker for university classes and professional association meetings. She received a bachelor of arts degree from Our Lady of The Lake University in San Antonio, Texas. She can be reached at *info@pacotech.com*.

Balancing the Risks and Rewards of Cloud-Based Healthcare Information Page 42

Rebecca Shwayri, J.D., is an attorney, author, and educator on e-discovery, privacy, and technology topics. She has published numerous articles on these topics in national publications, has presented educational programs to the corporate law departments of Fortune 500 companies, and is a regular monthly blogger on e-discovery and privacy issues on *i-sight.com*. Shwayri has a decade of experience advising global organizations on information management and e-discovery problems. She can be contacted at *rebecca.shwayri@akerman.com*.

AD INDEX

recall™
Your Information. Securely Managed.

"Your Passport to Information Management Freedom"

As organizations face increasing complexity with managing the expanding volume of physical and digital information and complying with industry and government regulations, they need a trusted partner that can help them. At Recall, we can help your business gain a competitive edge through the strategic, compliant, and economic use of information. Now that is Information Management Freedom!

Contact us at 1.888.RECALL6 (732.2556) or info@recall.com