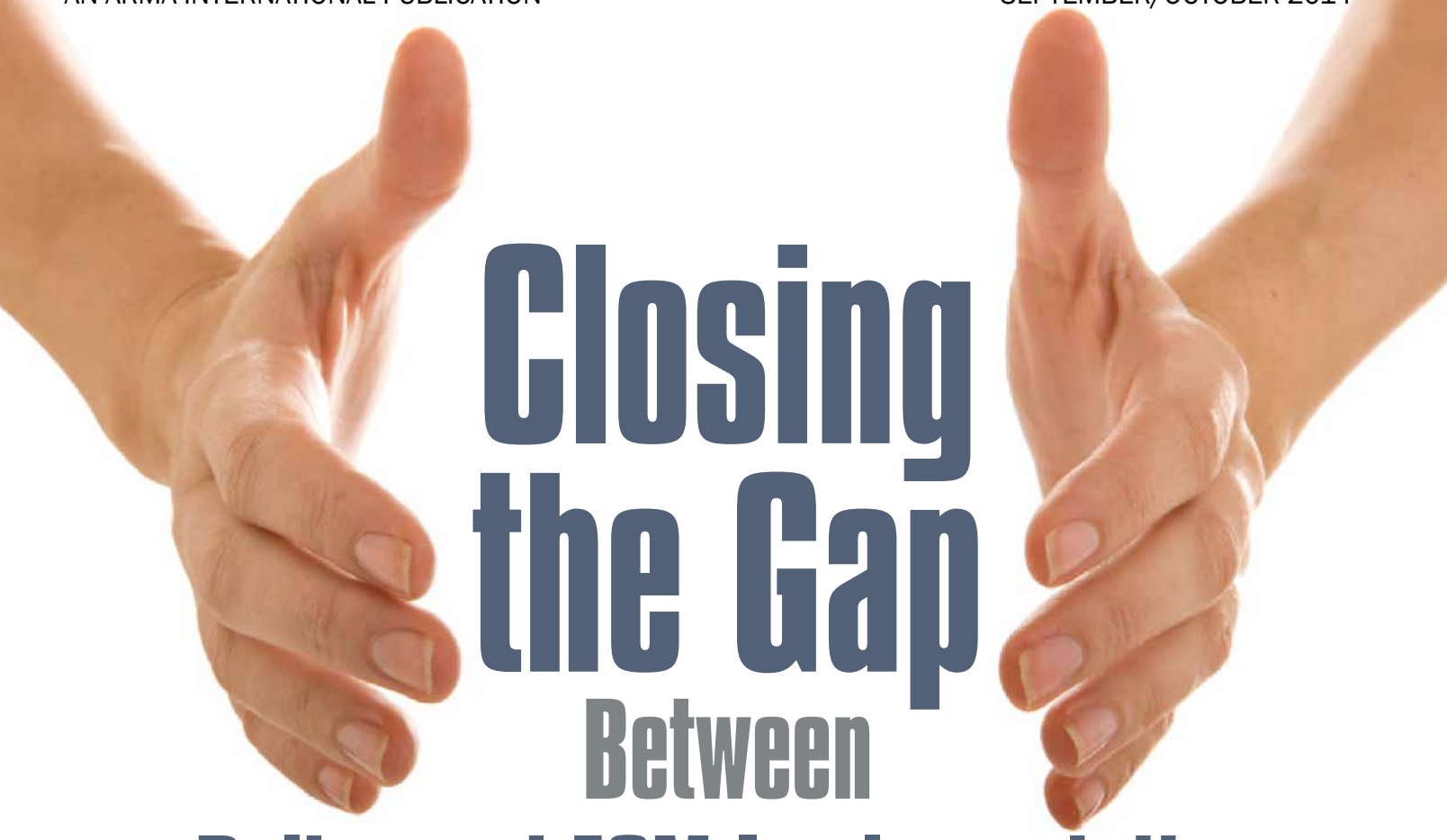
INFORMATION MANAGEMENT

AN ARMA INTERNATIONAL PUBLICATION

SEPTEMBER/OCTOBER 2014



Closing the Gap Between Policy and ECM Implementation Using Privacy by Design

Page 20

Six Steps for Creating a 'Super Data Map'

Page 28

Tossing the Tape?

Implications of Making the Switch to Disk-Based Backups

Page 33

rsd Your Information. Governed.

SMART INFORMATION GOVERNANCE

SIMPLE.
MEASURABLE.
ACHIEVABLE.
Repeatable.
TRANSFORMATIONAL.

2014 IGA
THE YEAR OF INFORMATION GOVERNANCE ACHIEVEMENT

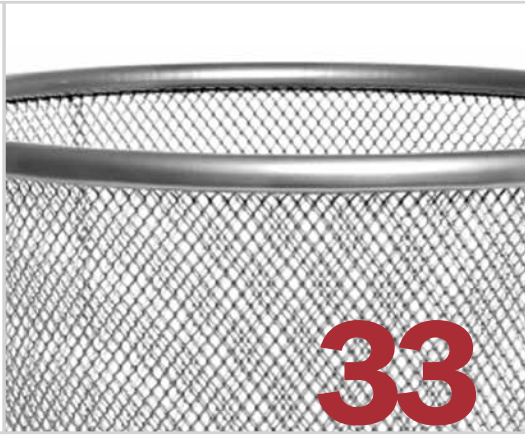
Learn More: rsd.com/arma2014

ARMA Conference 2014 | San Diego, CA | **BOOTH 1419** | October 26 - 28

INFORMATION MANAGEMENT

SEPTEMBER/OCTOBER 2014 **VOLUME 48 NUMBER 5**

DEPARTMENTS



FEATURES

SPOTLIGHTS

CREDITS

INFORMATION MANAGEMENT

AN ARMA INTERNATIONAL PUBLICATION

Publisher: Michael Avery

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.

Visit us at the 59th ARMA Annual Conference & Expo in Booth #1639 for a demo of our newest Prep-Reducing Scanner:

Falcon™

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

OPEX® CORPORATION

Investing in Privacy and Your Career – by Design

Flipping through the "Up Front" section of most issues of *Information Management* reveals the extent to which privacy is a growing concern for governments, businesses, and consumers around the world.

In this issue, for example, you can read several privacy-related news items, including how Google is on the hot seat with the EU and the state of California for its privacy policy; Europe and Canada have embraced their citizens' "right to be forgotten" by forcing Google and other Internet companies to take down certain personal information upon citizens' requests; and Florida has strengthened accountability requirements for the security of personal information.

At the same time, cyber criminals are working overtime to attack this vulnerable information, resulting in the exponentially growing need for skilled cybersecurity specialists. This is good news for records and information management (RIM) professionals who want to expand their information governance (IG) skills to meet this challenge.

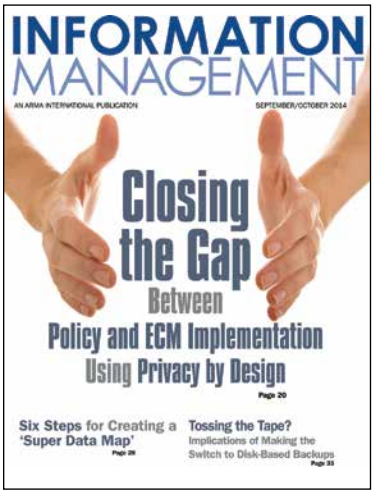
"We do see a lack of capability and capacity in skilled professionals, and that's partly due to massive demand across the world that stretches an already small, existing pool of people," Bryce Boland, Asia Pacific chief technology officer at California-based cybersecurity firm FireEye Inc., said in a recent *Bloomberg Businessweek* interview.

"In the short term, many large organizations have found innovative ways of meeting the demand for cybersecurity professionals through internal recruitment and training," the Rand Corporation reported in "Hackers Wanted: An Examination of the Cybersecurity Labor Market."

This issue of *Information Management* includes several articles meant to help you expand your privacy- and security-related IG skills to meet your organization's needs. The cover article by Norman Mooradian, Ph.D., for example, uses the Privacy by Design concept to provide a framework for converting legal requirements for protecting personal information into functional requirements for electronic content management solutions.

Mark Diamond writes about how to create a single, super data map that integrates privacy, legal, compliance, and IT requirements with the organization's records retention schedule. This type of map can help your organization identify and track personally identifiable information, protected healthcare information, and privacy data flows.

Switching from backup tape to disk-based backups has a number of implications for discovery, but also has an impact on privacy protection, according to a technology consulting team of authors in "Tossing the Tape?" Disk-based backups are not bulky like tapes and are generally stored in house, which means organizations using this method don't have to entrust their sensitive information to third-party service providers.



In the Generally Accepted Recordkeeping Principles® (Principles) series article, Julie Gable writes about two sets of "Principles for Protecting Information Privacy" that offer a starting point for making sense of what organizations are required to do and in what order.

Finally, in the RIM Fundamentals series article, John Isaza writes about "10 Things Organizations Should Do to Protect Against Hacking."

We hope these articles will encourage you to step up to the challenge of ensuring that your organization stays out of the headlines. We'd like to hear about other ways we can help you expand your skills; e-mail us at *editor@armaintl.org*.

Vicki Wiler
Editor in Chief

Oh, Dear! They're not supporting my scanners anymore — WHO DO I CALL???

Unlike our competitors, who *end-of-life* their products once they roll out their new lines, OPEX document imaging and material handling equipment is ***PRACTICALLY IMMORTAL!***

Knowledge, support, and a dedication to customer satisfaction, **(available 24 hours/7 days)** make the comprehensive OPEX Service Organization the ***SUPERPOWER*** in the industry! Does that make us heros? Why, yes it does.

OPEX WORLD HEADQUARTERS ■ OPEX FRANCE

OPEX® CORPORATION

OPEX GERMANY ■ OPEX UNITED KINGDOM

WWW.OPEX.COM

SOCIAL MEDIA

U.S. and European Lawmakers Scrutinize Facebook

Facebook continues to draw fire from its users, privacy groups, and some lawmakers in both the United States and Europe. The uproar this time is over the recent disclosure of a blind research study the social network site conducted one week in January 2012, unbeknownst to its subscribers. Essentially, Facebook manipulated the content of news feeds being sent to 700,000 users to see if negative emotions were contagious. The researchers' published the study's findings in the *Proceedings of the National Academy of Science (PNAS)* and stated that "the actual impact on people in the experiment was the minimal amount to statistically detect it." The reaction to the survey after the fact was anything but minimal.

Several European data protection agencieshave expressed their concern that the survey constituted a breach of users' privacy. Similarly, at least one U.S. privacy group registered a complaint with the Federal Trade Commission (FTC), and Senator Mark Warner (D-Va.) asked the FTC to "explore the potential ramifications" of the study.

"As the collection and analysis of 'big data' continues to increase, and as it assumes a larger role in the business plans of Internet-based companies, it is appropriate that we consider questions about what, if any, oversight might be appropriate, and whether best practices should be developed and implemented by the industry or by the FTC," wrote Warner.

Warner acknowledged that "companies like Facebook may have to perform research on a broad scale in order to improve their products. However, because of the constantly evolving nature of social media, big data, and the Internet, many of these issues currently fall into unchartered territory."

INFO SECURITY

Congress Asked to Help Protect Consumers' Data

The Federal Trade Commission (FTC) recently asked Congress to do more to protect consumers against the unchecked collection and sharing of their digital data by providing them with tools to view, suppress, and change their information. The agency also asked Congress to rein in data brokers, the companies that analyze and sell huge amounts of information for marketing purposes.

The FTC took aim at the data brokerage industry in its recent report to Congress, "Data Brokers: A Call for Transparency and Accountability." There is a fundamental lack of transparency about data brokers' practices, the agency noted in the exhaustive report. Unbeknownst to most consumers, data brokers work behind the scenes to gather information about them from commercial, government, and other publicly available sources both online and offline. From this, they can create a composite of the consumer that can infer race, gender, or sexual orientation, among other things – a composite that could, in actuality, be flawed. Storing this type of data indefinitely, the FTC pointed out, also poses a security risk.

An earlier report released by the White House raised similar flags regarding the immense aggregation of personal information. According to an article in *The New York Times*, the report's most significant findings focused on "the recognition that data can be used in subtle ways to create forms of discrimination and to make judgments – sometimes in error – about who is likely to show up at work, pay their mortgage on time, or require expensive medical treatment."

PRIVACY

Florida Passes Far-Reaching Data Security Law

The state of Florida has enacted a new law that increases security accountability for all business, healthcare, and governmental entities that reside or do business in the state. The new Florida Information Protection Act of 2014 (FIPA) specifically requires organizations to take reasonable measures to protect personal information, the definition of which has been broadened to include an individual's first name, first initial and last name, or any middle name and last name, in combination with a Social Security, driver's license, account, credit card, or debit card number.

Healthcare organizations take note: the law also expands the definition to include health insurance policy or subscriber number or any unique identifier used by a health insurer to identify the individual; information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis; or financial information. Further, it encompasses third-party agents that collect, maintain, store, or use personal information of Florida residents.

Healthcare organizations that operate in Florida will need to abide by both the Health Insurance Portability and Accountability Act (HIPAA) and the state's stringent data privacy laws, Jennifer Christianson, a partner at the law firm Carlton Fields Jorden Burt, told *InformationWeek*. One notable variance is in the number of days organizations have to notify affected individuals and the Florida attorney general. If a third-party service provider experiences the breach, the healthcare organization – not the third-party organization – is responsible for notification.

Christianson stressed that healthcare organizations must ensure that their business associates and other partners comply with privacy rules, and that all organizations must review their insurance policies to ensure breaches are covered. Failure to comply would be risky and potentially very expensive.

CYBERSECURITY

Apple to Team with IBM

And they said it would never happen. Apple recently announced that it was teaming with its former nemesis to bring IBM's big data and analytics capabilities to iPhone® and iPad®. Together they will develop more than 100 industry-specific applications, developed from the ground up, for the two devices.

Apple said the partnership will redefine the way work will get done, address key industry mobility challenges, and spark true mobile-led business change. Specifically, the two companies intend to deliver the essential elements of enterprise mobile solutions:

- Mobile solutions that transform business – The companies will collaborate to build IBM MobileFirst for iOS Solutions – a new class of "made-for-business apps" targeting specific industry issues or opportunities in retail, health care, banking, travel and transportation, telecommunications, and insurance, among others. The apps will become available starting this fall.
- Mobile platform – The IBM MobileFirst Platform for iOS will deliver the services required for an end-to-end enterprise capability, from analytics, workflow, and cloud storage, to fleet-scale device management, security and integration.
- Mobile service and support – AppleCare for Enterprise will provide 24/7 customer support to IT departments and end users while IBM will deliver onsite service.
- Packaged service offerings – IBM is introducing IBM MobileFirst Supply and Management for device supply, activation, and management services for iPhone and iPad, with leasing options.

CLOUD

EU Issues Cloud Guidelines

The European Commission (EC) has released guidelines intended to increase professional users' trust in cloud technology and to standardize service level agreements (SLAs). The guidelines were developed by the Cloud Select Industry Group (C-SIG) as part of the Commission's European Cloud Strategy. Contributors included ATOS, Cloud Security Alliance, ENISA, IBM, Microsoft, SAP, and Telecom Italia.

According to the EC, the guidelines are the first step toward standardizing SLA terminology and metrics. They will help business cloud users ensure that the key elements regarding technical and legal aspects of the services provided are included in plain language in their contracts with cloud providers. Examples of the essential items that need to be included are:

- The availability and reliability of the cloud service
- The quality of support services the user will receive from the cloud provider
- Security levels
- How to better manage the data stored in the cloud

The next step is to test the guidelines with users, particularly small and mid-size businesses. C-SIG is also working with the ISO Cloud Computing Working Group "to present a European position of SLA standardizations."

PRIVACY

Europe Turns Up the Heat on Google's Privacy Policy

It's taken more than two years and two appeals, but a privacy class action suit filed against Google in 2012 will be moving ahead, at least in part. The suit was filed in response to Google's adoption of a single, unified policy that allowed it to commingle Android users' data across all accounts and to provide that data to third-party advertisers.

After evaluating each claim of each sub-class in the suit, a California court allowed two claims, which include U.S. users who acquired an Android device and downloaded at least one application through the Android Market or Google Play between August 19, 2004, and the present, to proceed. Claims filed by users who acquired an Android device between May 1, 2010, and February 29, 2012, but switched to a non-Android device on or after March 1, 2012, were dismissed.

According to *IDG News*, the claims allowed include one that alleges Google breached its contract with the users by disclosing data to third parties following every download or app purchase. A second claim is filed under California's Unfair Competition Law.

European Union member countries also have taken Google to task over the 2012 policy change. Although Google has made changes to the offending policy, European data protection regulators are not satisfied. Italy is the latest country to join the fray. In late July, Italy's data protection commissioner, who has reportedly been coordinating with his counterparts across the EU, announced that Google had 18 months to comply with the European data protection law. Specifically, Google must make the following changes or, according to IT news service Gigaom, face possible criminal charges and fines of €1 million ($1.35 million U.S.):

- Make it clear to users that their data is mixed and matched across Google services for marketing purposes, both by cookies and by more advanced behavioral "fingerprinting" technologies.
- Get explicit opt-in permission from users before using their data in this way.
- Define how long it retains users' data.
- Delete users' data when asked, within two months for data stored on "active" systems and within six months for backed-up data.

By the end of September, Google must submit a plan outlining the steps it will take to comply.

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.

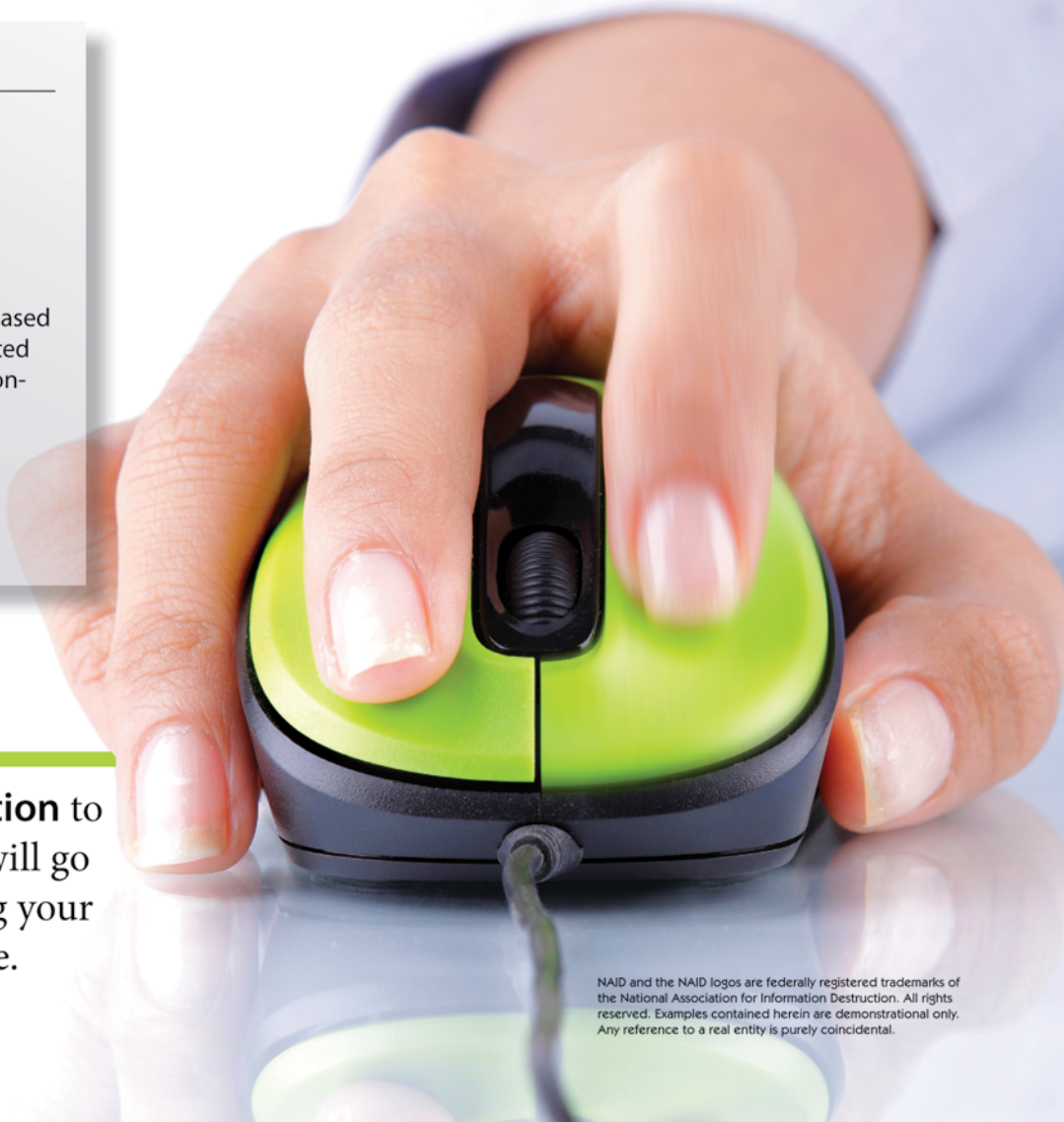
Data Destruction Co.

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.

CYBERSECURITY

Cyber Crime Costs More Than $400B Annually

A new McAfee-sponsored report from the Center for Strategic and International Studies (CSIS) revealed that cyber crime is having a significant impact on economies around the world. More specifically, it has cost businesses worldwide between $375 billion and $575 billion, more than the national income of most countries. Governments and companies underestimate how much risk cyber crime poses and how quickly that risk can grow, asserted CSIS.

The full impact of cyber crime, of course, goes beyond the dollar figure. It is also being felt in the job market. CSIS estimated that the losses from cyber crime could cost as many as 200,000 jobs in the United States and 150,000 jobs in the European Union.

The most important cost, however, is the damage to company performance and national economies, the report asserted. It damages trade, competitiveness, innovation, and global economic growth. Specifically:

- The cost of cyber crime will continue to increase as more business functions move online and as more companies and consumers around the world connect to the Internet.
- Losses from the theft of intellectual property will also increase as acquiring countries improve their ability to make use of it to manufacture competing goods.
- Cyber crime is a tax on innovation and slows the pace of global innovation by reducing the rate of return to innovators and investors.
- Governments need to begin serious, systematic effort to collect and publish data on cyber crime to help countries and companies make better choices about risk and policy.

It's imperative, therefore, that companies do more to protect their networks and countries strengthen their cyber defenses. What is needed, CSIS contended, is better technology and stronger defenses, as well as agreement and application of standards and best practices.

"Making progress on these changes will require governments to do a better job accounting for loss and companies to do a better job assessing risk," the report concluded.

BYOD

BYOD May Relieve Some E-discovery Headaches

Employers are realizing that they aren't always able to prevent their employees from using their personal devices for work purposes while on the job. A global survey by Fortinet found that 70% of personal account holders have used their personal cloud storage accounts for work purposes. This can present a problem when a lawsuit involves e-discovery of company documents, more and more of which are being created on personal devices or stored in personal Internet spaces.

One solution that some companies are exploring is mandatory BYOD. Yes, in the very near future you may be required to provide your own smartphone, tablet, or computer. Gartner has predicted that 50% of employers will require employees to supply their own devices for work purposes by 2017.

Gigaom's Geoffrey Goetz pointed out in a recent article that such a move would necessitate adjusting the company's privacy policy. Employees would also have to surrender their personal devices when it is legally in the company's best interest to do so if the goal of the mandatory BYOD policy includes helping to manage the risk associated with complying with e-discovery requests when the data resides on an employee's personal device.

Clearly, mandatory BYOD needs to be a carefully thought-out step for any organization.

CLOUD

Study: Mobile Users Shape the Cloud Computing Landscape

Thanks in lareg part to the increasing use of mibile devices for business purposes,the majority of the companies in the United States and Europe have made the move to the cloud, according to a new study by Frost & Sullivan. Although U.S. organizations lead Europeans in the rate of cloud adoption, companies in both regions are clearly becoming more aware of the benefits of the cloud.

More than half the businesses surveyed have already moved 50% or more of their enterprise communications solutions – particularly e-mail servers and collaborative applications – to the cloud. A quarter of those companies expect that percentage to increase to more than 75% over the next three years.

The study determined that 57% of U.S. and European cloud users are "cloud reliant." Furthermore, 70% of U.S. and 56% of European respondents currently using cloud technologies find them to be highly effective, indicating that increased exposure to cloud technologies could lead to wider adoption. The majority of cloud-reliant users are in the United States, particularly in manufacturing and in businesses of 20-500 employees and businesses of more than 10,000, according to Frost & Sullivan Research Analyst Karolina Olszewska. In the future, the largest growth areas will likely be the government sector and small businesses.

"The share of remote and mobile workers is expected to increase over the next three years and change business technology requirements," concluded Olszewska. "The cost impact of supporting these new business needs will be felt more intensely by IT decision-makers in the United States than those in Europe."

PRIVACY

Data Privacy Becomes an HR Issue

Until lately, data privacy has been regarded as primarily an IT issue. Some – particularly in the legal community – contend it is also becoming a human resources issue as hackers are starting to take aim at employee personal information as well as customer information. Take the monstrous Target breach as an example. The hackers attacked both customer and employee personal data.

In the Connecticut Employment Law Blog, publisher Daniel Schwartz, a partner at Shipman and Goodwin LLP, also noted an article in *The New York Times* that reported hackers recently tried to access government employee files that included in-depth personal information required for security clearances. Four months later, the administration says there is no indication that the breach was successful.

The motivations for the attacks may be different, but both instances drive home Schwartz's point that HR departments have some skin in the game of data privacy. He recommended that HR develop a data privacy policy to cover security concerns; continually train and educate all employees – including senior executives – on the steps they need to take to protect confidential information; conduct regular audits of information in all formats, including paper; and insert clauses into employment contracts that clearly prohibit employees from accessing confidential data during their employment with the company and after they leave.

PRIVACY

Europe and Canada Embrace Right to Be Forgotten

The right to be forgotten (RTBF) is gaining ground. Both Europe and Canada have implemented RTBF regulations and are looking at extending it beyond national boundaries.

Europe's RTBF regulations went into effect May 30, and by July 3 Google already had received nearly 70,000 requests to remove links to content on some of the world's largest news sites. The European Court of Justice, the highest court in the European Union, ruled in June that European users should have the right to be forgotten on the Internet. It decided there were certain cases in which Google and other Internet companies should allow online users to be "forgotten" after a certain time by erasing links to web pages "unless there are particular reasons, such as the role played by the data subject in public life, justifying a preponderant interest of the public."

Thus, Google and other Internet companies would have to remove web pages if requested, even if the original "publication in itself on those pages is lawful." If the provider doesn't remove the link to the "offending" information, the user can take the matter to the appropriate authorities to obtain, under certain conditions, the removal at the Internet company's expense. The officials will then weigh "legitimate interest of Internet users potentially interested in having access to that information" and the individual's fundamental right to privacy and to the protection of personal data. The decision to remove links, according to the court, would depend on the "nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life."

BBC News Business Economics Editor Richard Preston announced to readers on July 2 that BBC had received notice from the search giant that it would no longer be able to show a blog Preston wrote in 2007 in response to certain searches on European versions of Google. There was no additional information provided, including why the link was no longer going to be available via the search engine. Had the individual who was the main subject of the news item requested its removal? After some sleuthing, Preston discovered that the removal was prompted by a request from a reader who chose to comment on the article. For whatever reason, he no longer wanted his comment to be visible under the provisions of the new RTBF regulation.

BBC News isn't the only news site already affected by the new regulations. World news agency AFP (Agence France-Presse) reported that the UK's *The Guardian* also had received notices that six of its articles would no longer be included in European search results. A few days later some of the links were restored, a clear indicator that Google is refining its processes as it goes.

In the meantime, European users conducting Internet searches using Google and other search engines may not receive a complete list of references. That doesn't mean the content no longer exists or is unavailable, however. It still exists on the news sites – complete with comments. Apparently, the restrictions also relate only to certain search terms. The removed links also continue to show up in search results on the U.S. version of Google.

European news agencies are predictably extremely unhappy with Google's actions, which the search company contends are necessary for compliance with the court's order. *Mail Online* publisher Martin Clarke says the instances to date show what a nonsense the right to be forgotten is. "It is the equivalent of going into libraries and burning books you don't like," he contended. He told AFP that *Mail Online* would regularly publish lists of articles removed from Google's European search results. The BBC and *The Guardian* also published links to the restricted stories.

A Google spokesperson told AFP that it individually examines each request to be forgotten to determine whether it meets the court ruling's criteria. "This is a new and evolving process for us," she said. "We'll continue to listen to feedback and will also work with data protection authorities and others as we comply with the ruling."

shaping tomorrow with you

FUJITSU

Clear your desk faster

You'll find government compliant Fujitsu scanning solutions in some high places. From the world's fastest high-volume document scanners to versatile, easy-to-use scanners for desktops, Fujitsu has one you should consider. Include the ability to integrate with dozens of leading software providers and you have a strong and reliable solution that lasts. Get started today by visiting **ez.com/infoarma**

See the New FUJITSU Document Scanner fi-7160

epeat SILVER

LEARN MORE AT energystar.gov

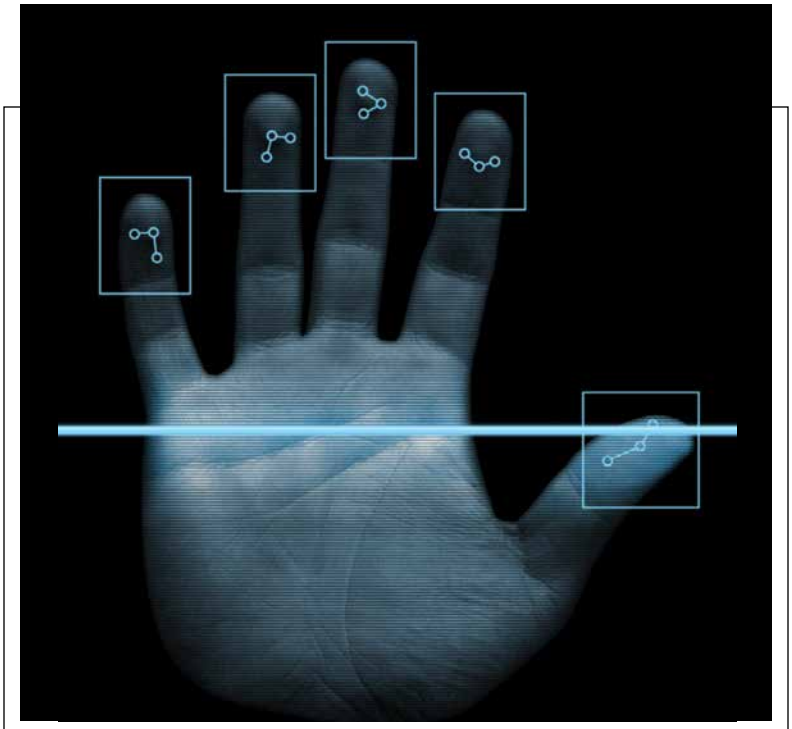
INFO SECURITY

The Sedona Conference® Adds Data Security Working Group

The Sedona Conference® has established Working Group 11 (WG11) to focus on data security and privacy liability. The group's mission is to identify and comment on trends in data security and privacy law so that organizations may better prepare for and respond to data breaches. It will also provide guidance regarding data security and privacy class-action developments, including liability, damages, and class certification issues.

WG11 will be guided by a steering committee composed of representatives of the various stakeholders involved in the data security and privacy liability area. Anyone interested in this subject is welcome to join the full group, which will meet virtually, with limited face-to-face meetings throughout the year, the first of which is scheduled for November 5-7 in New Orleans.

The Sedona Conference® describes itself as a nonprofit research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights. It is known for bringing together some of the brightest minds to create practical solutions and recommendations of immediate benefit to the civil justice system. It has 11 working groups that use an extended peer-review process to develop content that is widely published in conjunction with legal and professional educational programs.



CLOUD

NIST Drafts Cloud Forensic Standard

The increased use of cloud computing brings new and bigger challenges for those involved in digital forensics. As the National Institute of Standards and Technology (NIST) recently pointed out, "The characteristics that make this new technology so attractive also create challenges for forensic investigators who must track down evidence in the ever-changing, elastic, on-demand, self-provisioning cloud computing environments. Even if they seize a tablet or laptop computer at a crime scene, digital crime fighters could come up empty handed if these devices are linked to pooled resources in the cloud."

NIST's Cloud Computing Forensic Science Working Group, an international body of cloud and digital forensic experts from industry, government, and academia, set out to identify the challenges that cloud computing poses to forensics investigators who uncover, gather, examine, and interpret digital evidence to help solve crimes. The group's recent report, "NIST Cloud Computing Forensic Science Challenges," identified 65 such challenges. While the report focuses on the technical challenges, almost all intersect with legal and organizational issues. The group divided the 65 challenges among nine categories, including architecture, data collection, analysis, standards, training, and "anti-forensics" (such as data hiding and malware).

"The long-term goal of this effort is to build a deeper understanding of, and consensus on, the high-priority challenges so that the public and private sectors can collaborate on effective responses," said Martin Herman, co-chairman of NIST's Cloud Computing Forensic Working Group.

NIST believes there is a pressing need to develop forensic protocols that major cloud providers eventually would adopt. "These protocols must adequately address the needs of the first responders and court systems while assuring the cloud providers no disruption or minimal disruption to their services," the report stated.

INFO SECURITY

Too Small for a Cyber Attack?

Small businesses don't need to worry about cyber attacks, right? After all, you only hear about large enterprises and some mid-size businesses being hacked.

While the latter statement is true enough, that doesn't mean small businesses aren't at risk, particulary given their reliance on mobile devices for storing critical business information. According to the UK Federation of Small Business, 41% of small firms were victims of cybercrime – including online fraud and computer viruses – in 2013. One in 10 of micro firms (10 or fewer employees) surveyed by Kaspersky Labs admitted that an IT security breach would probably cost them their business.

"While it is encouraging to see the extent to which micro firms are embracing the latest technologies, this must go hand in hand with a strong approach to internet security," said Kirill Slavin, UK managing director at Kaspersky Lab. "Micro firms don't have to become IT security experts. Most of the time it's the IT equivalent of remembering to lock all the doors and windows when you go out, make sure you have some additional protection and not to leave valuables where others can easily see and get to them."

A survey by Barclays Bank revealed one in eight small businesses are victims of cyber-fraud each year. "Typical scams include opportunities to acquire new customers who you supply but never receive payment from, or to purchase items from new suppliers that never deliver after having been paid. Fraud can happen to any type of business in many different ways, impacting their revenue, reputation and the long-term health of the business, with no business being too small to be targeted," said Alex Grant, Barclays managing director of fraud prevention.

Kaspersky Labs and Barclays Bank suggested that small and micro firms spend just five minutes a day checking the following five things to help keep their businesses safe:

1. Passwords – All Internet-enabled devices that carry your business data should be protected by strong passwords, whether the equipment is company- or employee-owned.
2. Attachment awareness – Understand the dangers that can lurk in e-mails, web links, USB sticks, CDs, etc., and onsider introducing extra software that will filter out or contain suspicious-looking items.
3. Educate all employees – Make sure everyone knows how to stay safe online, including how to use strong passwords, spot suspect e-mails or sites, and protect company information.
4. Back-up – Every day make sure the information you store on computers is backed-up and secure.
5. Security systems – Take full advantage of any user-friendly Internet security software that has been specially created for small firms to secure devices such as smartphones, laptops, tablets, computers, WiFi, and networks. Also remember to keep things out of sight and the site locked up.

PRIVACY

Consumers: Access to EHR Trumps Privacy

The ability to access electronic health records (EHR) outweighs concerns of privacy invasion for U.S. consumers with chronic conditions, according to a report from Accenture. The research study of 2,011 individuals, a little more than half of whom had a chronic condition, revealed that 69% of those with a chronic condition believe they should have the right to access all of their healthcare information, and 51% believe that accessing their medical records online outweighs the privacy risks.

The biggest barrier to accessing those records online for 55% of those with chronic conditions is not knowing how to do it. For the largest majority (87%), access isn't enough; they want to control their health data. Only a little more than half, however, believe they have much or any control over their medical information.

The U.S. Centers for Disease Control estimates that 47% of Americans have at least one chronic disease, but they account for 76% of all physician visits. They are also actively engaged at most stages of patient care, which means health care needs to adapt to a new generation of consumers who expect to have transparency and therefore demand more access to their personal data online, said Kaveh Safavi, M.D., J.D., the leader of Accenture's global health business.

Privacy Concerns Among U.S. Consumers with Chronic Conditions

Individuals are slightly less concerned about the privacy of their electronic medical data (65%) than other personal information that is stored electronically, such as online banking (70%), in-store credit card use (69%), and online shopping (68%), according to an Accenture survery.

Source: Accenture Patient Engagement Survey, 2014

COPYRIGHT

Europeans Call for a Single Copyright

The European Commission (EC) received an earful when it asked for public comment on the EU copyright rules earlier this year. It seems many European consumers want a single EU copyright. They are frustrated with being denied cross-border access to online content, especially when attempting to view or listen to content from their home country when they are in another EU country. In other words, they want a single market in which they can access all content from any online stores whether directed to the member state in which they reside or not. Those that called for a common copyright believe that it would do away with territorial restrictions and allow users to freely access, purchase, and transfer content across the entire EU market.

Libraries expressed sentiments similar to those of consumers. University libraries especially pointed to problems students face in trying to access online educational resources from sources – including other universities – outside the country in which they are searching.

Those generating and publishing the content, however, laid the blame on the service providers. EU-wide cross-border licenses are available; it's the digital providers who limit the access, they contended. Film producers and broadcasters see territoriality as less of an issue, in large part because of language differences.

The EC reviewed more than 2,000 responses in composing a white paper that examines whether further action on the current EU copyright system is needed. That paper is expected this fall.

New Risk Maturity Index Emerges from Study

A recent PricewaterhouseCoopers (PwC) study found that most organizations (almost 60%) in Europe and North America are aware of the importance of their information and its role in gaining competitive advantage. The challenge is protecting it from internal and external threats without sacrificing its access and value within the organization.

"The repeated emphasis from regulators, advisors, and risk-managers on data protection and information safeguarding has become the holy grail of data management," observed PwC analysts in the report. "Unfortunately, this company-wide focus on security has kept organizations and their boards from sharing and distributing data and information within the organization to maximize its value."

The study, commissioned by Iron Mountain, is in its third year, but this is the first year it presented the results in a risk maturity index. The index gauges the extent to which businesses implement and monitor a set of 34 measures to manage and protect information assets. These measures fall into four groupings: strategy, people, communications, and security. To receive a high individual index score, an organization must not only implement the measure but also monitor its effectiveness. The four levels of risk maturity are:

- Unprepared for Risk – Organization is severely exposed to information risk. It likely does not have an information risk strategy in place, and senior management is unaware of the potential impact to its business. (Score: 49 or under)
- Aware of Risk – Organization realizes it needs to manage risk but is uncertain about what to do or remains ill-equipped to tackle the threat. (Score: 50-79)
- Approaching Maturity – Organization has established some measure and senior leaders are more aware. It has reduced its exposure but has not yet implemented a robust strategy. (Score: 80-99)

- Equipped for Risk – Organization has implemented a responsible approach that encompasses strategy, people, communications, and security from top to bottom. It monitors, evaluates, and improves its approach to effectively manage its exposure to risk. (Score: 100)

Larger organizations (2,500+ employees) are outperforming mid-size organizations (250-2,500 employees) in this effort, with Europe leading the United States. Businesses in Norway stand out from the other countries (United States, Canada, France, United Kingdom, Germany, Spain, the Netherlands, and Hungary), followed by France and Canada. According to the report, businesses in these countries stand apart from the others because they understand the importance of monitoring the effectiveness of their strategies and making the necessary changes to keep ahead of the risk. At the sector level, energy and pharmaceutical businesses lead the way in information risk strategy in both Europe and North America.

Those organizations that are leading the pack and approaching maturity are focused on monitoring the success of their policies and programs and adapting to the evolving landscape. They are more likely to have prioritized leadership, communications, and analytic skills in future growth plans. Further, they protect their data well but also use that data to drive growth through innovation.

"The key to the success of information risk initiatives is to build both the policy and the evaluation into the day-to-day processes," PwC concluded. For some organizations, this may require a significant cultural shift.

CYBERSECURITY

Needed: Cybersecurity Professionals

The need for skilled cybersecurity specialists has grown exponentially as governments and businesses have raced to protect their networks from cyber attacks from all directions. Unfortunately, the supply doesn't begin to meet the demand, which some believe could become a national security issue.

"We do see a lack of capability and capacity in skilled professionals, and that's partly due to massive demand across the world that stretches an already small, existing pool of people," Bryce Boland, Asia Pacific chief technology officer at California-based FireEye Inc., a cybersecurity firm, said in a recent *Bloomberg Businessweek* interview.

Unfortunately, addressing this gap between supply and demand takes time. Rand Corp. explored the state of the cybersecurity labor market in its research report "Hackers Wanted: An Examination of the Cybersecurity Labor Market." It concluded that there has already been a large increase in education, particularly government-supported education, and an increase in the number of computer science majors in response to early indications of a growing demand for cybersecurity professionals.

"It's normal for the labor market to lag demand and education initiatives," Rand said in its report. "Theory suggests and experience confirms that the market may take a long time to respond to unexpected increases in demand. In the short term, many large organizations have found innovative ways of meeting the demand for cybersecurity professionals through internal recruitment and training."

The Rand report suggested the best steps may already have been taken for addressing the shortage. "The difficulty in finding qualified cybersecurity candidates is likely to solve itself, as the supply of cyberprofessionals currently in the educational pipeline increases, and the market reaches a stable, long-run equilibrium," it concluded.

A new cybersecurity report released by the Pell Center at Salve Regina University in Rhode Island took the discussion a step further by charting a path to professionalizing the field. The key element of the proposal is the creation of a professional association for the cybersecurity industry.

"There is a widening gap between the supply and demand of qualified cybersecurity professionals," said Pell Center fellow Francesca Spidalieri, one of the authors of the report. "As schools and training institutes proliferate to meet that need, basic standards are needed to assure that someone claiming special skills actually has them." She noted that there are already excellent models – such as the American Medical Association and the American Bar Association – for professionalizing the cybersecurity workforce.

"Achieving cybersecurity is far more than a technical problem: it is fundamentally a people problem," said the report's co-author, Lt. Colonel Sean Kern, USAF. "And since cybersecurity is a people problem, there must be a people solution. This requires developing an overarching organizational framework to develop, manage, and oversee the training, education, certification, and continuous professional development of a qualified cybersecurity workforce along a career continuum, and to guide leaders across society in harnessing the right people with the right knowledge, skills, and abilities to the right challenges in a rapidly-evolving environment."

Spidalieri noted that the cybersecurity industry in the United States is "highly fragmented." She and Kerns believe that a national professional association would change that and "solidify the field as a profession." They hope their study will be a catalyst for more research and efforts to unify the industry. **END**

XACT DATA DISCOVERY

Fact: The world is digital.

Fact: Paper hasn't disappeared.

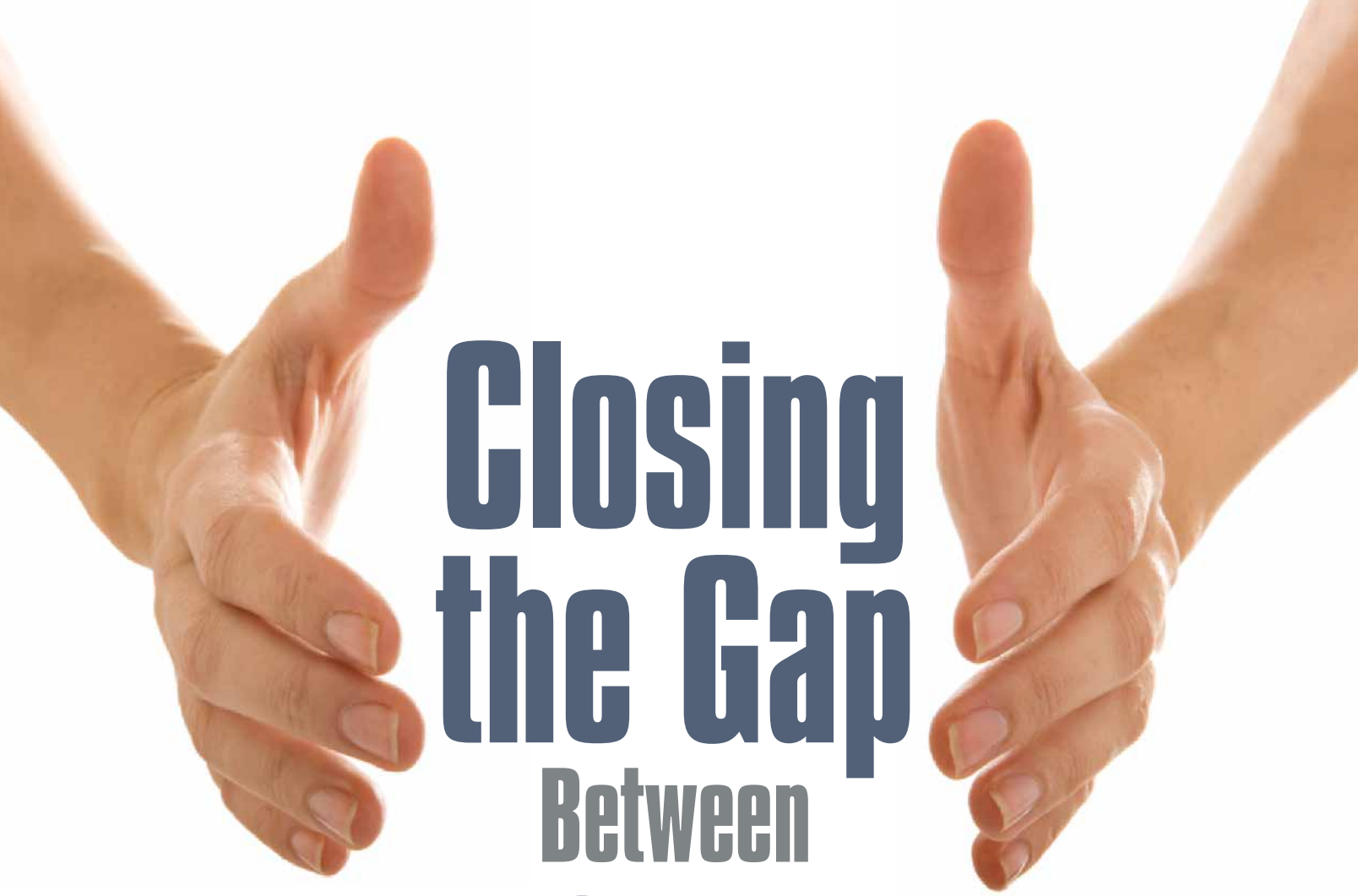
Xact Data Discovery is both

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



Closing the Gap Between Policy and ECM Implementation Using Privacy by Design

Norman Mooradian, Ph.D.

This article provides a framework for converting legal requirements for personal information into functional requirements for procuring or implementing an electronic content management (ECM) solution.

The core idea of the Privacy by Design (PbD) software engineering approach is that privacy controls should be built into information systems that capture and manage personal information. Its focus is on consumer-facing applications and platforms, such as social media and interactive websites, as well as on big data applications that process masses of personal information.

PbD concepts are especially important to enterprise content management (ECM) because ECM systems often capture personal information. This includes *unstructured* content, such as word processing documents and e-mail, which makes their privacy requirements much less predictable than for systems that capture *structured* content, such as the data fields in a financial system's database.

Because records and information management (RIM) professionals are key stakeholders in the procurement, configuration, and management of ECM solutions – typically shaping system requirements, creating and implementing policies, and overseeing daily operations – they can use PbD as an interface between the policy creation and ECM implementation processes.

Identifying Relevant PbD Principles

The PbD approach is articulated by seven principles (see Sidebar 1), the full text of which is published on the website of the Information and Privacy Commissioner of Ontario, Canada, a long-time champion of PbD. Three of these are especially relevant to RIM professionals.

Privacy Embedded into Design

The third principle of PbD, "Privacy Embedded into Design," sums up the approach by calling on developers to build privacy features into the product. It applies well to ECM solutions because their focus on capturing records requires privacy-relevant features, such as robust audit trails and fine-grained security controls. Also, ECM solutions tend to be configurable, which means that many functional components can be implemented through the selection of settings and the creation of system objects.

For RIM professionals, this means that ECM systems can be evaluated on how they address privacy concerns through their inherent features and how they can be configured to provide compliance with policies and regulations.

Positive Sum

The fourth principle, "Positive Sum," contains the idea that information privacy is a *feature* of a system, not a *constraint* on it. It sets an expectation that good engineering can avert tradeoffs, and it has backing from developers and regulators. This is important for RIM professionals because they can invoke it if there is push back from the IT or vendor side.

Full Lifecycle Protection

The fifth principle, "Full Lifecycle Protection," reflects a core competence of RIM professionals: managing records throughout their lifecycle.

Foundational Principles of Privacy by Design

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality — Positive-Sum, not Zero-Sum
5. End-to-End Security — Full Lifecycle Protection
6. Visibility and Transparency — Keep it Open
7. Respect for User Privacy — Keep it User-Centric

Sidebar 1: Privacy by Design: The 7 Foundational Principles
Source: Information and Privacy Commissioner of Ontario, Canada, *www.ipc.on.ca*

Understanding the Solution Development Cycle

To use PbD as a bridge between organizational policy and the development of information solutions, RIM professionals must be familiar with the software development cycle. As described below, RIM professionals will contribute heavily during the first stages of the development cycle, but they need visibility into the *entire* process to be better able to specify what they need and to advocate for it with confidence. (See Diagram 1.)

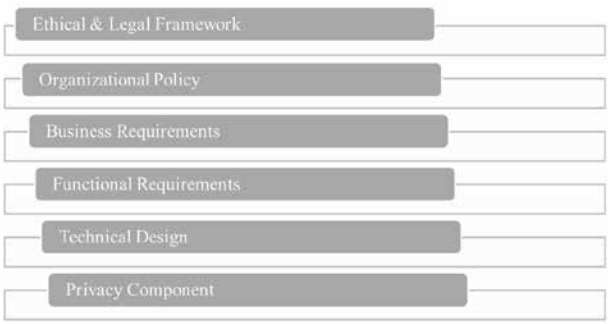


Diagram 1: Solution Development Cycle
Source: Adapted from *Privacy Engineer's Manifesto: Getting from Policy to Code to wQA to Value.©2014 Apress.*

RIM-Shared Responsibilities

Within the privacy context, the first steps of the cycle are developing policy based on ethical norms and legal requirements. RIM professionals, who presumably do legal research in retention and confidentiality, should certainly be at the policy creation table when information privacy is at issue.

The next step is to develop the ECM solution's privacy-related *business requirements*, which state at a fairly high level the capabilities the system needs to have. They should take into account what is a programmed, or built-in, feature of the solution and what can be configured with the system's tools.

At the procurement stage, the business requirements are used to evaluate the system; they include security controls, audit trails, reporting, workflow capabilities, and other such features.

Functional requirements, which are more specific and come into play once the ECM platform has been chosen, state exactly how the system should be set up and what the system should do relative to all the processes that will be covered in the implementation.

IT Responsibilities

The last stages of the cycle belong to the developers. They take the functional requirements from the business analyst and articulate them further into the system's technical design. This means, for example, taking the steps of a workflow and specifying what programming or configuration is needed to accomplish them within the ECM system.

Identifying Private Information

Developing privacy requirements for ECM solutions requires looking at the ECM solution architecture from both a data perspective and a functional perspective.

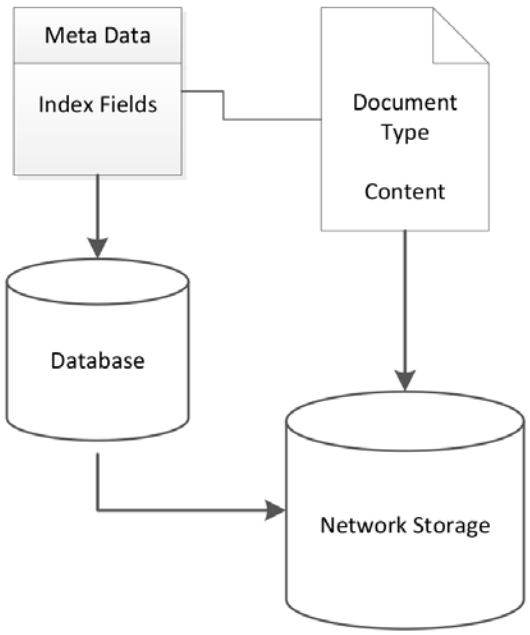


Diagram 2: Personal Information Stored in Content and its Metadata

ECM Data Structures

As mentioned earlier, there are two things that make an ECM solution unique from a privacy perspective: ECM solutions are quite variable in their scope and purposes when compared to data systems and, as represented in Diagram 2, they contain both structured and unstructured data.

The structured data is *metadata,* which is defined by ARMA International as "information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage information resources"; it is used to manage the content.

The implication is that there are two areas of the application that can have personal information: the content itself and the metadata. This means that when a privacy inventory or privacy impact assessment is performed, the same methods used for any data system can be used for the metadata.

When assessing the data attributes, consider:

- Whether they constitute personal information singly or in combination with the other attributes in the metadata set
- The level of sensitivity of the attributes singly or as a set

When assessing document types (or record series) managed by the system, you will need to consider both the document type and the content that the document type might contain. This is because some document types – such as medical records – are considered as a category to be of a personal and sensitive nature. However, personal information may also be found in document types that are in categories not considered to be personal and sensitive, such as departmental correspondence.

Diagram 3 indicates the levels of analysis for reviewing existing or proposed systems from a data model perspective. The red font indicates that the data attributes, the document class, or the content contain or *potentially* contain personal information. (Note that the diagram could be elaborated further to indicate levels of risk.)

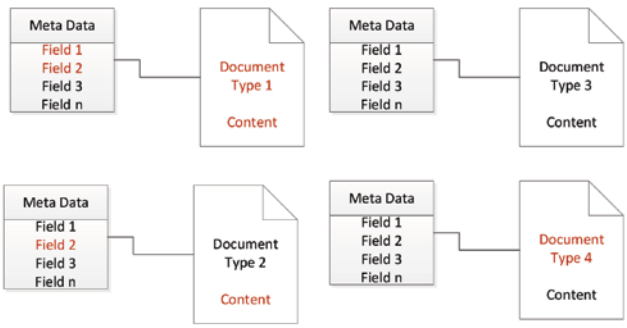


Diagram 3: Analyze Data Attributes, Document Class, and Content to Identify Personal Information

Canon

imageFORMULA

Document Scanners

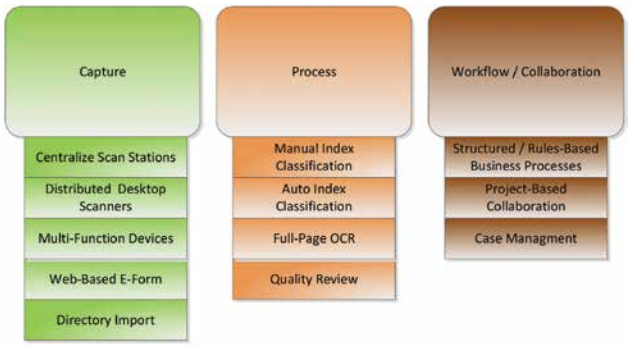
The imageFORMULA Document Scanner Line Just Got More Powerful!

Stop by Booth #915
at the *ARMA Live! Conference*
for more information and enter for a chance to win a P-215II Mobile Document Scanner

www.usa.canon.com/scanners

Defining ECM Functional Areas

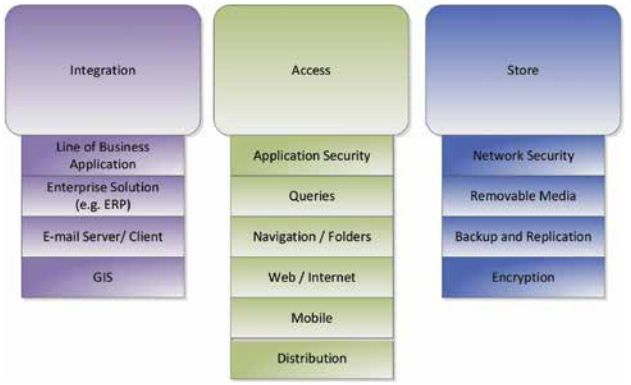
Having looked from a high level at the data structures of ECM solutions, we need to look at the functional areas. Diagram 4 presents a graphical overview of those areas:



Capture is the process of ingesting documents and data into the system.

Process represents steps taken to prepare the documents for storage and retrieval. Here we would find auto classification, auto-indexing, and quality control.

Workflow and ***Collaboration*** represent processes and methods that allow users to work together to use documents and information in structured and unstructured ways.



Integration concerns interaction with other systems. Important here is the two-way transfer of information between systems.

Access concerns the methods for retrieving and using information. This includes search tools and mobile access.

Store concerns the actual storage of documents and data on file shares and in database tables.

Diagram 4: Graphical Overview of ECM Functional Areas
Note: The top-level categories are adapted from Hyland Software's six pillars.

Applying Privacy to Functional Areas

You can apply any privacy framework concepts to these ECM functional areas to create a conceptual design and functional requirements. You can also use the categories to evaluate a system. And very importantly, you can use these areas to formulate policy around your practices and system users.

Table 1 provides an example of how you might associate the American Institute of Certified Public Accountants' (AICPA) Generally Accepted Privacy Principles with different areas of a solution, create policies, or formulate functional requirements. You can see full guidance about the AICPA principles at *www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/DownloadableDocuments/GAPP_BUS_%200909.pdf*. (The other leading privacy frameworks are the Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data at *http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf* and The Code of Fair Information Practices, which directly shaped the U.S. Privacy Act of 1974, at *www.justice.gov/sites/default/files/opcl/docs/rec-com-rights.pdf.)*

Each functional area and its subcomponents introduce areas of risk that need to be assessed. For example, the capture area covers the way documents enter the system. From a policy perspective, this is where you would determine which document types can be captured and from what source and set controls that restrict capture to those types.

Capture is also the area that represents interaction between people and the ECM system. Subcomponent differences are relevant to privacy concerns. For example, centralized scanning (a subcomponent of capture) provides more controls for restricting users from seeing the documents being scanned. It also provides a direct channel into the ECM system.

Converting Legal Requirements into Functional Ones

The rest of this article walks through how to convert a legal requirement into a policy statement, a policy into business requirements, and business requirements into functional requirements.

Legal Requirement to Policy Statement

One of the U.S. Privacy Act of 1974 (Privacy Act) provisions for recordkeeping (5 U.S.C.A. § 552ad) concerns capturing records of the disclosure of qualifying personal information:

> c) **Accounting of certain disclosures.** – Each agency, with respect to each system of records under its control, shall –
> (1) except for disclosures made under subsections (b)(1) or (b)(2) of this section, keep an accurate accounting of –
> (A) the date, nature, and purpose of each disclosure of a record to any person or to another agency

American Institute of Certified Public Accountants' Generally Accepted Privacy Principles

ECM Functional Areas	Notice	Consent	Collection	Uswe/Retention	Access	Disclosure	Security	Quality
Capture	x	x	x				x	x
Process	x	x		x		x	x	x
Workflow	x	x		x	x	x	x	x
Integration	x	x	x	x	x	x	x	x
Access	x	x		x	x	x	x	
Store				x			x	x

Table 1: Evaluating ECM System Against AICPA Principles

made under subsection (b) of this section; and

(B) the name and address of the person or agency to whom the disclosure is made;

An organization within the jurisdiction of the Privacy Act would translate the legal requirements into its information privacy policy, abstracting the statutory language to make it more flexible, broadly applicable, and easier to understand. For example, it might read:

ECM System Policy – Capture Record of Disclosure

Maintaining a record of disclosures not covered under normal business purposes of personal information and records maintained within the organization's ECM/EDM or ERM system.

- For any disclosure not covered under the definition of routine business purposes,
  - The organization will create a record of the disclosure that contains at a minimum:
    - A description of the purpose of the disclosure
    - A description of the documents disclosed
    - The name of the person(s) proving the disclosure
    - The date of the disclosure
    - The name, address, and contact information of the party receiving the disclosure
    - A history of any steps taken in approving the disclosure (which steps are defined in the relevant section of this policy)

Policy to Business Requirement

The next step is to use the policy to lay out the business requirements, in this case for procuring an ECM system. Note that these requirements are high level, as they are meant to provide general privacy-relevant functionality that can be used in different ways.

ECM Business Requirements – Capture Record of Disclosure

The ECM solution will include functionality to manage the disclosure of personal information.

- It will allow authorized users receiving a request for personal information to create a request for disclosure of a personal record by invoking an electronic form and filling in predefined data fields.
- The electronic form will allow capture of all metadata specified in the policy in such a way that it can used for reporting purposes, such as providing: a specific accounting of a particular disclosure; a complete report of all disclosures for a given data subject; and aggregate reports for statistical purposes.
- The system will be able to provide workflow automation that supports policy-based decision rules for approving requests for personal information.
- The electronic form will be linked to the record.

Business Requirement to Functional Requirement

The next step is to create functional requirements. These will need to be more specific and detailed than the business requirements, as they address how the functionality that is acquired or developed needs to be implemented.

Often they are expressed using a convention called a "use case," which covers specific user interactions or transactions in the system. The use case or other functional

requirements document is given to the developer or IT specialist who will configure or develop the solution. In the example below, the functional requirements specify what has to be built.

Use Case: Records Specialist Creates Request for Personal Information

- The records specialist receives a request by e-mail, phone, or walk-in.
- He/she will be able to invoke an electronic form via a menu command. The form will have an identifying name appropriate to the request type (e.g., Non-Exempt) Disclosure Request.
- The form will have the following fields:
  - Requestor First Name
  - Requestor Last Name
  - Date of Request
  - Organization
  - Address
  - Purpose of Request (Drop-Down List)
  - Request Description
  - Comments
  - Records Specialist First Name
  - Records Specialist Last Name
  - Date Information Provided
  - The form fields will map to database fields.
- The form will be saved by clicking a submit button.
- Security will be applied to the form when submitted, limiting viewing and editing to records staff while in processing.
- The form will enter an approval workflow when submitted.
- If approvals are required, the form will be routed to the required approvers and security will be reset.

Stepping up to the Challenge

RIM professionals can be key participants in the ECM system procurement or development process. Their research skills and knowledge of ECM structures and the development cycle position them to translate legal requirements into policy that can then be used to identify business requirements and implemented as functional requirements for an ECM system. **END**

Norman Mooradian, Ph.D., can be contacted at nmooradian@kmbs.konicaminolta.us. *His bio is on page 47.*

You asked, we listened.

At Zasio, we're committed to listening to our customers and delivering the best records management software in the industry. Introducing **Versatile Enterprise 8**—*manage your records better than ever!*

To learn more about Zasio and its records management software and consulting services, please stop by ***booth #1314*** *at the* ***ARMA Live! 59th Annual Conference & Expo****.*

ZASIO

800 513 8000 | www.zasio.com

Six Steps for Creating a 'Super Data Map'

Creating a "super data map" that not only captures metadata about where and in what media information resides, how it is used, and who owns and has access to it, but also integrates legal, compliance, privacy, and IT attributes along with a record retention schedule, can lower risks, reduce costs, and be easier to maintain than separate, single-purpose databases.

Mark Diamond

Do you know where your records actually live – in which systems and on what media? How about your privacy information? Do you know what content is where when you need to place a legal hold?

Multiple groups in an organization need to know what information lives where for a number of purposes. These groups, including legal, IT, and records and information management (RIM) professionals, often take disparate approaches to identifying and classifying the same information, multiplying the work and producing a variety of results.

Organizations that want to link retention schedules and policies to repositories have an even more difficult task. Extending a records retention schedule to capture other types of metadata, such as privacy and security fields or pointers to systems of records, quickly can become overwhelming and unmanageable. What's needed is a better approach. It's time to create a data map.

Defining 'Data Map'

A *data map* is a database that captures an inventory of what you have, where it is, and who is responsible for managing it. It can track record types, personal and confidential data classifications, documents and other types of paper and electronically stored information (ESI), and key metadata, such as how it's used, for what purposes, and who has access to it.

Data maps can track information across a variety of media, systems, and locations. Because information and data are continually created, deleted, and moved, an effective data map is dynamic and updated regularly. Maintaining it is a great challenge, but good map design can make it much easier.

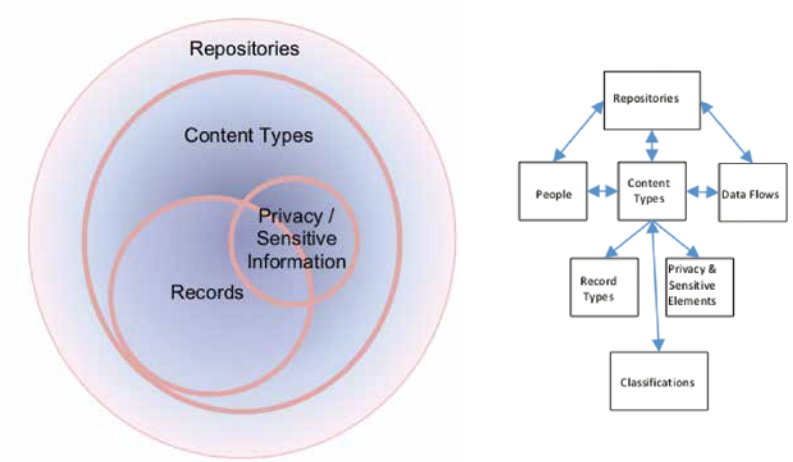


Figure 1: Super Data Map: Fitting the Pieces Together

Identifying Users

A number of business functions need to track the location of documents and data. These include the following:

Application and Infrastructure Management

IT groups need to catalog enterprise applications, repositories, and systems across the organization. Such information helps guide backup and archival strategies, disaster recovery plans, and capital spending.

RIM

RIM professionals need to know which records reside in which repositories, track systems of record, identify what records are convenience copies, and manage retention requirements. They also need to identify and defensibly dispose of expired, duplicative, and low-value data and documents.

Legal and Compliance

Litigators and investigators need to know the location of ESI and hardcopy content that may be relevant in a legal proceeding or investigation. This knowledge enables them to issue narrower legal holds, thereby reducing the costs of discovery and increasing defensibility.

Legal and compliance teams need to track trade secrets, intellectual property, and other kinds of private and confidential data. They also have to ensure that employees, customers, and other legitimate stakeholders have access to data, while unauthorized or non-legitimate users don't.

Auditors need to track financial and compliance information that is relevant to one or more specific regulations, including the Sarbanes-Oxley Act of 2002, the Foreign Corrupt Practices Act of 1977, and others.

Privacy

Privacy professionals have regulatory and statutory requirements to identify and track personally identifiable information (PII), protected health information (PHI), and other privacy data. This may also include privacy data flows.

While the needs for mapping vary across functions, the mapping process is very similar. Creating a single, "super" data map that combines records, privacy, discovery, and other drivers and serves multiple masters is easier, more efficient, and costs less than building and maintaining multiple maps.

Defining 'Super' Data Map

As shown in Figure 1, a *super data map* identifies the repositories, applications, and storage locations where information can live. Within the repositories are *content types*, which are discrete documents, databases, images, and other content that must be managed for retention or security. Important subsets of the various content types are business *records*, which carry a mandated retention period. Private and sensitive information may be regarded as content types or records, depending on the level of detail to which they must be managed.

Creating a Super Data Map

At minimum, the map includes descriptions of applications and systems; types of *unstructured content* (e.g., documents and images) and *structured data* (e.g., database elements) included in each; the sources and locations of data; and the involved personnel (business and IT custodians). If created in a relational database, super data maps also can incorporate record retention schedules and data security classification policies, providing one place to track data and repositories and linking this information to relevant policies.

Sample Fields for System Information in Data Map

System Name	The system, application, or repository where data is stored
Description	A brief description of the specified system/repository, which may include information about the primary users and the type of data stored there
Hosted	Indicates whether the application is hosted internally or outside the organization
Status	The status of the specified system/repository as of the "Last Update" date. A drop-down menu provides "Current" or "Retired" options.
Roll-Out Date	The first date on which the specified system/repository was available to store data
Retirement Date	For inactive or legacy systems/applications/ data storage locations, the last date on which the specified system/repository was actively accepting new data
Data Structure	Identifies the type of information housed in the specified system/repository. Standard descriptions include unstructured (e.g., flat files saved on the network), semi-structured (e.g., MS Outlook e-mail), and structured (e.g., database records from applications such as PeopleSoft or Oracle).
System of Record	Identifies whether the repository is considered a system of record or a secondary or reference source
Information Classes	Lists any information, content, or record classes that may be contained within the system/repository (used as a single point of collection to aid in more granular linking of records/information classes to systems/repositories)
PPI Sensitive Info	Indicates through a "Yes," "No," "Maybe" drop-down menu whether personal protected information (PPI) or other sensitive information exists in the repository (used to flag repositories with PPI or sensitive data to allow for more granular linking or classification as appropriate)
Custodians	Lists the name(s) of key business, legal, and IT contacts or business unit subject matter experts with ownership, responsibility, or knowledge of the system/repository
Retention	**Retention Backup** – Describes the current back-up system for the repository, including frequency, media type, location(s) of backup media, etc. **Retention Policy** – Indicates how long information should be retained in the repository

Table 1: Sample Fields for System Information in Data Map. You will want to customize the fields to your needs.

Following are six steps for creating and maintaining a super data map.

1. Form a Cross-Functional Committee

An important success factor for a data mapping project is the formation of a cross-functional team to oversee the effort. The team should include key stakeholders from legal, RIM, and IT, as well as end-users from business units, who have the best understanding of how information flows through and outside the organization. Once the stakeholder groups understand the challenges at hand and the "win" in it for them, they'll be willing to participate, ensuring a map that is usable across the organization.

2. Gather Input from Stakeholders

A super data map will succeed – and scale to meet future needs – if the business requirements are well-defined and agreed-to across the organization early-on. Ask committee members:

Which constituencies will use the data map, and how will they populate and consume the information? Including two or three functions can meet the needs of many.

Will the map serve just one or many purposes? The trick is to make the map useful for any given function without getting too detailed and overwhelming the structure. When it doubt, keep it simple.

What data elements will be collected and maintained for these repositories (e.g., application names,

record types, custodians, server locations, backup methods, storage size, format)? Use the answers to create an in-depth database table for each repository that contains detailed content types, as well as additional reporting capabilities to allow production by content type. This allows users to search on specific content types to find the associated repositories. Don't get too detailed, though. For example, a data map may identify that purchasing records live in a specific place, but it should not be so detailed that it shows where contract negotiations from Customer ABC live.

Will the map track privacy information at the object level (typical files or database records) or at the element level (fields within an object)?

How many repositories will the map address? While an enterprise may have hundreds of repositories, 80% of the relevant information may live in just 20; start with these first.

Are there limitations as to the accessibility of information? Inaccessible repositories might include those created or used by electronic media no longer in use, redundant electronic storage media such as backup tapes, or those from which retrieval involves substantial cost.

Each stakeholder group has a unique perspective and a list of what it wants to be included in the map. But, including too many fields and discrete data points will lengthen the collection process and make it difficult to maintain the map.

Conversely, if the scope is too narrow, important data points could be missed, resulting in an ineffective map and the need to re-collect data. The key to good data map design is balance and tolerance of the imperfect; it will be a trade-off among comprehensive data collection, maintainability, and ease of use.

Start with a pilot or trial version of the data map, populating only a sub-section before collecting data on a large scale. Build and improve the map through iteration, as the requirements of multiple groups and the significance of additional repositories and content types are identified. This process will test the structure, allowing early assessment and adjustments to be made and resulting in the proper balance for the data map design.

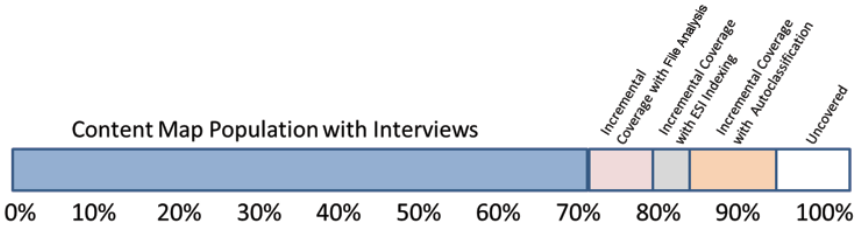


Figure 2: Average Percentage of Data Collected by Collection Method

Table 1 provides an example of the types of attributes that might be tracked within a data map. The actual fields to be included, though, will be dependent on the organization.

3. Choose the Right Structure

Picking the right tool to house your data map is important. There are three options:

MS Word or Excel. These programs may be suitable for retention schedules or very small data maps, but quickly become overwhelmed due to the many-to-many interelationships between the data elements.

MS Access or SQL Server. A simple-to-use but fully functional relational database can be ideal. When designed well, they are capable of mapping significant amounts of data.

Commerial Software. Some very large organizations may wish to keep their data maps maintained through direct links from other applications, such as the HR module from an enterprise resource planning (ERP) system. In these specialized cases, organizations may want to consider purchasing a commercial software tool to hold the data map. The drawback, however, is that these tools may be difficult to customize for specific use cases and environments.

4. Collect Data to Populate the Map

Populating the data map means creating for each repository an in-depth database table entry that contains content type details and creates capabilities for reporting by content type. This framework allows stakeholders to search on specific types of content relevant to their respective use-case and find the associated repositories and other important data elements.

But before the data map can be populated, information must be collected. Following are three of the best approaches for collecting information.

Interviews. Interviewing a cross-section of employees is surprisingly effective. They provide useful guidance when the data to be collected is well-structured (i.e., are of a specified format and can be easily described) and when stakeholder behavior can be categorized (i.e., the expectations of individual groups can be clearly articulated).

Surveys typically miss nuance, such as the pain people may feel when dealing with particular systems and kinds of information. Individual and small-group interviews can uncover real issues and challenges that simple, form-oriented surveys often miss. In practice, surveys followed up with interviews provide excellent guidance and insight.

ESI Scanning and Keyword Index Tools. Automated tools can sort through and index huge volumes of information, making it easier to inventory and classify data. Rules-based approaches use keywords and synonyms along with Boolean logic that

…no automated technology can, by itself, point at a collection of information and then define and populate a data map in a way that is defensible and comprehensive.

is often associated with search engines to confirm objectively a category match with a content item. The precision and completeness of rules-based systems are good when the information to be classified contains sufficient metadata and/or keywords.

Predictive coding goes farther than rules-based systems. This machine learning approach uses established statistical models and a set of keyword-rich "exemplar" documents to train the software about the context and meaning of information. With predictive coding, relevant information can be identified for each concept in the category scheme. This is especially useful when there is not enough metadata available or when large collections of information are spread across multiple data sources, such as e-mail, SharePoint, and file shares (i.e., content "in the wild").

Autoclassification. Originally intended to improve the consistency and accuracy of records categorization, autoclassification software can be suitable for locating many types of documents and files – especially when such items are already housed in supported document management systems and repositories – and can make information easier to search and retrieve. As with predictive coding, autoclassification software requires considerable up-front manual effort and system training.

Automated tools have become sufficiently trustworthy to assist humans in their decisions or, in some cases, to supplant human intervention. The suitability of a particular technology depends on the volume of information to be reviewed, the desired accuracy of the results, and the amount of manual effort and expense that an organization is willing to invest. See figure 2.

At this time, no automated technology can, by itself, point at a collection of information and then define and populate a data map in a way that is defensible and comprehensive. And, none of these tools can establish how the information got to where it is or how to remediate problems. Manual effort is also required.

5. Integrate Retention, Security

The same relational database used to house your data map can also hold your records retention schedule. Furthermore, since repositories are managed as separate elements in the map, creating linkages between record types and their respective repositories is straightforward.

This also applies to data security classification for privacy and other sensitive information. Mapping security levels to elements within a repository allows for easier execution of security policies and provides a convenient view of what sensitive information lives in each repository.

The complexity of the data map increases through embedding schedules and policies, so keep in mind the importance of keeping it simple. Well-thought-out and well-designed map taxonomies – with a preference for simpler – yield benefits.

6. Maintain the Map

As new applications, repositories, and tools are introduced, the information contained in the map can become obsolete; on average, a well-designed map will experience about 20% data "drift" per year. Accountability for ongoing maintenance should be spelled out from the beginning of the project. Identify the responsible parties and the appropriate procedures to be used (e.g., interviews and surveys), and train staff on processes and maintenance. Those responsible for maintaining the map must do the following.

Incorporate IT system change management procedures. Every time IT commissions or decommissions a system or repository, part of the IT system change management process should be to update the data map. Doing so will often address the majority of the changes in the environment.

Leverage discovery to feed the map. New and ongoing litigation will uncover unexpected sources of information that are subject to discovery. Feed information gleaned from the discovery process to update the map.

Develop a regular refresh process. Beyond depending on IT system change management and e-discovery, organizations may want to refresh their maps every 12 to 18 months through the same processes used to initially populate the map. Map maintenance is typically less difficult and much faster than the initial map generation since it will be focusing only on changes.

As is true for developing the map, maintaining the map is best done as a shared process by multiple stakeholders. Many functional hands make for lighter map maintenance work.

Sharing Final Words of Advice

A good super data map can be a boon for RIM, e-discovery, privacy, compliance, and IT. It is an essential navigational tool for climbing the information governance mountain.

So, invest the time needed to design a map that matches your organization's needs. It will pay off with its ease of use and maintenance. Take a balanced approach and include multiple stakeholders. Walk before you run; build the map through iteration, tackling the most relevant repositories first, then working down the list. And don't let perfect be the enemy of good. **END**

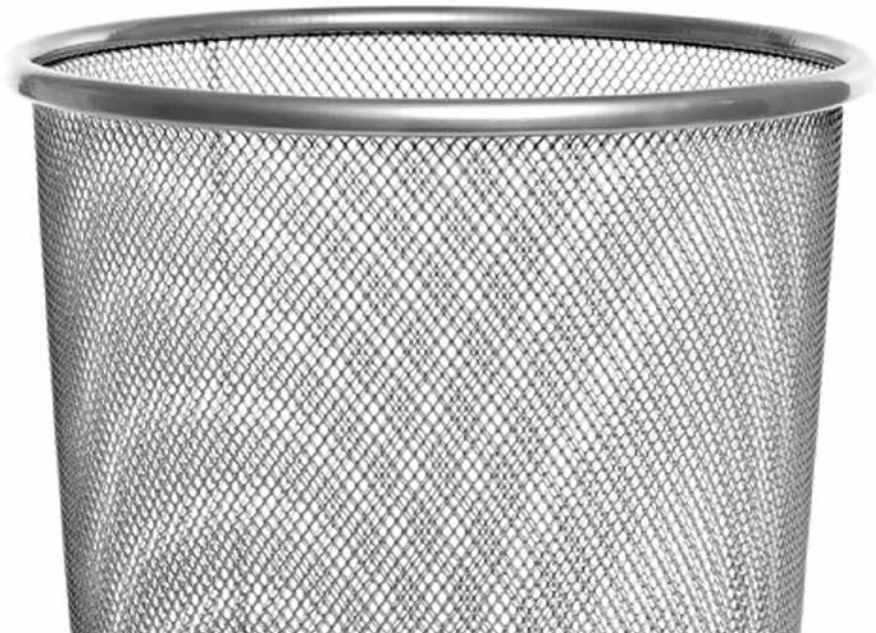
Mark Diamond can be contacted at mdiamond@contoural.com. *See his bio on page 47.*

Tossing the Tape?

Implications of Making the Switch to Disk-Based Backups

Veeral Gosalia, Antonio Rega, and Matt Shive

Backup data on tape has usually been deemed inaccessible for e-discovery, with courts ruling that it would be overly burdensome to retrieve. Now that organizations are increasingly using disks, the question of whether backup data remains inaccessible is worth examination.



In the last few years, production of electronically stored information (ESI) for business and other purposes has increased exponentially. As the amount of information that organizations maintain grows, so do the costs and risks associated with effectively managing that data.

Organizations are increasingly moving away from tape and toward disk-based formats as their primary means of backup. While disk options are more scalable, have better indexing, and offer virtual management,

they do introduce e-discovery implications that are not of concern with tape backups.

Records and information management (RIM) professionals should therefore know that when transitioning from tape to disk, more areas may be called into interest for litigation and investigations.

Case Law

In the last decade, judges have ruled that the amount of work involved in restoring tape backups is overly burdensome, and therefore data on them is considered reasonably inaccessible for e-discovery purposes.

One of the most widely noted and earliest rulings on this matter was *Laura Zubulake v. UBS Warburg*, presided by U.S. District Judge Shira Scheindlin from the Southern District of New York. *Zubulake* centered on a sexual harassment suit filed by a former employee. The employee claimed that to prove her case, she needed e-mails from UBS Warburg that had been stored on tape and later written over by backups.

This issue brought forth case law about the duty to preserve, with exceptions made for data that is retained as part of a backup. This ruling has led to widespread interpretation that if data must be retrieved from backups, the burden of cost must shift to the requesting party.

A ruling in *Kilpatrick v. Breg, Inc.* in 2009 said that backup tapes can be subject to discovery despite being identified as not reasonably accessible. In this matter, the defendant claimed that its tapes could not be produced for the purpose of finding electronic documents of relevance because they were for disaster recovery only. Ultimately, the judge ruled the tapes could be produced to the court, but at the plaintiff's effort and expense.

This issue came up again in *Johnson v. Neiman* in 2010, wherein the court ruled with the defendant that electronically stored information residing on backup tapes was not reasonably accessible. The court provided a protective order on the tapes and stated "'reasonably accessible' is best defined as whether the electronically stored information is kept in an accessible or inaccessible format (a distinction that corresponds closely to the expense of production)."

The Federal Rules of Civil Procedure (FRCP) provide further guidance on the matter of backup tapes. Rule 26(b)(2)(B) supports the court actions:

> A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery. Rule 45 (e) (1) (D) also addresses inaccessibility and echoes this guideline.

Discovery of Backups

While the cited rulings still leave some gray area about accessibility, what's clear is that retention and deletion policies are paramount when it comes to preparing for discovery of backups, regardless of whether they are stored on tape or on disk.

When legal and IT departments forget they have backup tapes from prior years, or when they change their retention policies and fail to enforce those policies on past data, problems such as the ones described below involving the authors' clients can arise.

A client was facing an inquiry that required the review of data from several years. Because the organization had a policy that all tapes would be overwritten after 30 days, the investigators initially believed there would be limited historical data. The team at corporate headquarters confirmed this policy, as did the contact at the company's satellite office where collection was to take place.

However, when the forensic examiner was leaving the satellite office after collection, he noticed stacks of tapes – many more than would have been needed for 30 days of backups. It was then revealed that these backup tapes predated the 30-day retention policy. Because the company had not disposed of the existing tapes when it implemented the 30-day retention policy, it had to spend millions of dollars to restore and review the data on them.

As another example, a client that has retained historical backup tapes for a subset of data under legal hold, dating back to 2006, now has to make a subset of its content available for review in a new litigation. Unfortunately, because these tapes weren't indexed, and many were not labeled when created, an extensive process must be undertaken to identify tapes to be indexed, restored, and their content subsequently reviewed. This effort will require an exorbitant amount of time and money to complete.

What's clear is that retention and deletion policies are paramount when it comes to pre

Benefits of Using Disk

It is important to note that when much of the case law around tape backups was established, there was little use of disk storage. Now, as disk use increases, there is more discussion of the scope of accessibility of backups on disk.

There are important differences to consider between the tape and disk-based worlds. By better understanding them, RIM, IT, and legal teams can work together to prepare for potential discovery of disk backups and to address any burden arguments.

paring for discovery of backups, regardless of whether they are stored on tape or on disk.

Among the benefits for moving from tape to disk are the following:

Reduced Risk

Most IT and records management professionals consider disk storage to markedly reduce the risk factor because it doesn't require as much physical handling, which can make tapes more error prone. Backup to tapes is also more likely to fail.

In addition, organizations typically entrust a third party to store their tapes, putting their sensitive data outside their immediate control and potentially at risk. While it's true that organizations often store more data when using disks because they are less cumbersome than tapes and because disk-based backups are often run more than once daily, the reliability of disks makes up for the risks that may come with this increased volume.

Reduced Cost

Cost is often a major factor in deciding to move to disk, but disk storage is not always cheaper. Typically, the metrics organizations use to determine cost include how long the archived data would need to be retained, how much time would be available for its recovery, and how much data loss is acceptable.

If data must be stored for more than two years, the better approaches are using a combination of tape and disk or simply using tape. Because disks require less storage space, an organization using disk storage can back up an entire data center with just two or three refrigerator-sized storage arrays and will have space for two or three years' worth of data. Using tape, the same data center would require up to eight refrigerator-sized storage racks, and the volume would grow over time.

More Efficiency

Managing tape is difficult. It should be encrypted when it's shipped to a storage facility. Further, it involves a lot of moving parts: hardware can break, and network resources must be devoted to support the backup process.

Disk storage eliminates these complications. Most disk backup solutions are built on technologies with fewer parts that can fail. Industry statistics show a strategic win for disk use in most cases due to reduced resources needed to maintain the backups.

Additionally, disk backups almost always involve deduplication. While deduplication can be done on tape, the process is less efficient. This is a key differentiator, especially when considering older backup tape methods.

Questions for Discussion

It is critical to understand how disk storage impacts records management from a compliance standpoint and how – if at all – regulations for disk use differ from tape.

As mentioned earlier, there is clear case law concerning how tape backups may be used in e-discovery. If there is a future deviation from case law, it will be governed by how readily accessible the data is and if it is too burdensome to discover. Included below are questions to help organizations determine whether disk backups can be considered reasonably inaccessible in e-discovery.

How Do Platforms Differ?

Current typical backup products do not create indices as part of the usual backup process; this is true for tape and disk. Without an index, there is a significant argument about the discoverability of that data: it needs to be restored, reviewed, and analyzed to find whatever information is being sought.

That being said, backup solutions are changing significantly and rapidly, enabling full indexing that would help limit the amount of data to be restored and addressing issues of deduplication, efficiency, and more. Some platforms include functionality that can aid in e-discovery.

As the burden discussion for disk backups evolves, these features may become more significant, setting a different precedent for this issue. As these types of technologies become available, RIM professionals should evaluate the options to ease future e-discovery burden and cost.

Can Backups Be Reasonably Restored?

With tape, hardware that can physically read the data is required, and those devices can be difficult to find for legacy data. Disk is typically easier to access than tape, but doing so does requires some effort.

With disk, the data is usually not encrypted because it does not change hands that often (though disk-based encryption is quickly becoming standard). If the backup is unencrypted, it

is possible to retrieve a single identified item or group of items without restoring the entire backup, making it far superior to tape for finding data. This is yet another reason why information management professionals and counsel must be prepared for the possibility of disk backups coming under the scope of reasonably accessible sources for discovery.

Tape restoration costs can slightly surpass those of disk. Tape requires more resources because it creates contention in the data center's bandwidth as backups are continuing to write simultaneous to the restoration process.

Further, if an organization no longer has the hardware or resources to restore legacy data, it may need to engage an outside provider. While the contention issue goes away with disk use, such restoration still requires a location for the restored data to be written to, such as a disk array or other hardware. Restoring from disk is typically faster than restoring from tape as well.

Does Switching Affect Existing Litigation Holds?

Switching from tape to disk essentially has no net impact on existing legal holds. The transition affects only the way information is stored; it does not negate any preservation commitments.

With tape or disk there must be a retention policy in place that takes into account any current litigation hold obligations. During a transition from tape to disk, IT must retain any data that is stored on tape that is under litigation hold. Further, disk use more readily allows for taking more than one backup per day, which creates more points in time to restore or recover from. If some of that data is on legal hold and therefore can't be removed, there could be an increasing cost in the disk environment because more data is being backed up.

When moving to a disk environment, policies may need adjustment to address new retention and backup approaches. As noted in the case examples, enforcing those policies can be difficult, but it must be a priority.

Be Proactive

RIM professionals can make a strategic impact on their organizations by carefully assessing the benefits and challenges of more modern, flexible options for data storage, accessibility, and governance. A thorough audit will give stakeholders the opportunity to take a hard look at how their backup policies need to change.

Legal holds are a critical focal point requiring extra attention during these discussions, as well as for and during any subsequent data migrations. RIM professionals should work with the legal team to evaluate the discovery requirements to ensure that retention and deletion policies address retention needs appropriately and that any approaches for managing backup procedures take e-discovery requirements into consideration.

Disk-based storage in particular opens a new door of what may be considered discoverable; in certain circumstances, archived data that may have since been deleted from the "live" environment can be an important consideration to an investigation.

Understanding these sensitivities and being prepared to work with counsel to respond to a discovery matter, either in making a burden argument against restoring the backups or to cooperate in a restoration process if disk backups are deemed accessible by a judge, can be a key difference-maker in the decision-making process. **END**

Veeral Gosalia can be contacted at veeral.gosalia@fticonsulting.com. *Antonio Rega can be contacted at* antonio.rega@fticonsulting.com. *Matt Shive can be contacted at* matt.shive@fticonsulting.com. *See their bios on page 47.*

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

CRM

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

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

In a business world in which new jobs are increasingly competitive, your designation as a Certified Records Manager 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

PRINCIPLES FOR PROTECTING INFORMATION PRIVACY

Julie Gable, CRM, CDIA, FAI

When it's done well, information privacy protection is part of an organization's policy and procedural infrastructure, working in the background like a silent sentinel that few realize is constantly on alert. When it's done poorly, it makes headlines and ripples through an organization from the cubicles to the board room.

Media reports tend to make privacy protection synonymous with cybersecurity, and some resources, such as the EDRM's Information Governance Reference Model, take the position that while business, legal, and records and information management (RIM) stakeholders have input, it is IT's responsibility to manage the information protection environment.

Protection, though, is as much about policy and procedural issues as it is about technology activities. Anti-hacking and anti-theft measures, for example, can exist only as the result of well-defined policies that are made in response to laws governing collection, storage, transfer, retention, and disposition of private information and the assignment of privacy protection responsibilities.

The Push for Privacy

The states of Massachusetts and Nevada have enacted tough privacy laws, and members of the U.S. Congress are moving forward with cybersecurity legislation aimed at protecting private information. Meanwhile, privacy experts are advocating that individuals have the right to control the collection and use of their personal data, an idea embodied in many European laws. Organizations, therefore, find themselves squeezed between pressures from lawmakers and customers.

Privacy breaches are expensive for business. According to the Ponemon Research Institute's "2014 Cost of Data Breach Study: Global Analysis," the average cost for each stolen or lost record containing sensitive or confidential information is $145 (U.S.). Considering that Verizon's "2012 Data Breach Investigations Report" showed that 95% of the 174 million records compromised worldwide in 2011 contained personal information, the total cost is significant. What's worse is the potentially irreparable harm to customer confidence in the breached organization and its impact on future business.

Privacy breaches can be costly for careers, too. In some cases, high-level executives have lost their jobs, and in the high-profile incidents at Wyndham Worldwide and Target, sharehold-

ers brought lawsuits against their respective boards alleging that board members failed to take reasonable steps to maintain their customers' personal and financial information in a secure manner.

But, determining what "reasonable steps" are is a mammoth task in an environment that is a complex tangle of evolving state, national, and international information privacy laws, industry regulations, human behaviors, and physical and electronic systems.

- Centralized access controls
- Well-defined confidentiality and privacy considerations
- A defined chain of custody when appropriate
- Training for employees

Level 3 of the IGMM also notes that the organization will have defined, specific goals related to records and information protection. Finally, protection notes that an organization's audit program should have a process to "ascertain whether sensitive information is being handled in accordance with the outlined policies in the principle of protection."

One complicating factor in addressing protection for private information is that it will likely involve several functions.

Privacy Protection Principles

Two well-known sets of principles offer a starting point for making sense of what is required of organizations and knowing what to do and in what order: the Generally Accepted Recordkeeping Principles® (Principles) and the Generally Accepted Privacy Principles (GAPP).

Principle of Protection

One of the eight Principles from ARMA International, the Principle of Protection, notes that an information governance (IG) program should be designed to offer "a reasonable level of protection to information that is personal or that otherwise requires protection." The context for this principle says that the program must ensure that "appropriate protection controls are applied to information from the moment it is created to the moment it undergoes final disposition." It also specifically includes electronic systems as well as physical systems.

A look at the Principles' complementary Information Governance Maturity Model (IGMM) reveals that elements of protection considered "essential" (Level 3 of the IGMM) include:

- A formal, written policy for protecting records and information

One complicating factor in addressing protection for private information is that it will likely involve several functions. In large organizations, it's common to find compliance officers, privacy officers, legal counsel, and IT and RIM professionals involved. In smaller concerns, the task may fall predominantly on whomever has responsibility for RIM and/or IT. The key to progress in either situation is to find useful guidance that can provide a consistent understanding of concepts and reliable information on how to proceed.

GAPP

The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) developed GAPP to help organizations design and implement privacy programs based on sound privacy practices and policies that address obligations, risks, and business opportunities. Although it was designed by accounting organizations, GAPP's focus is not solely on financial services.

Just as the Principles are based on ISO 15489: 2001 Information and documentation – Records management – Part 1: General), GAPP is based on ISO 27002 *Information technology – Security techniques – Code of practice for information security controls.* Although ISO 27002 has much to say about specific technologies, GAPP is technology-neutral.

Among the useful features of GAPP are standard definitions of privacy, personal information, and sensitive information. GAPP defines *privacy* as "the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure and disposal of personal information."

Personal information is further defined as information that is about or can be related to an identifiable individual, including such items as name, home, or e-mail address, identification number such as Social Security number or social insurance number, physical characteristics, and consumer purchase history. Refining the definition further is GAPP's inclusion of *personal information that is considered sensitive*, such as medical, health or financial information, race or ethnic origin, political opinions, religious or philosophical beliefs, membership in trade unions, sexual preferences, and criminal offenses.

GAPP is also based on key concepts from such laws as the Organization for Economic Co-operation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* and the European Union's Directive on Data Privacy (Directive 95/46/EC). (For a discussion of these, see "An International Perspective on Protecting Personal Information" by Cheri Buckles in the March/April 2014 issue of *Information Management*.)

GAPP lists 10 privacy principles. (See Sidebar: Generally Accepted Privacy Principles). For each of these, there are objective and measurable criteria to guide development and evaluation of an organization's pri-

vacy policies, communications, procedures, and controls. The practitioner's version of GAPP includes a chart showing each principle, the criteria involved in its development, illustrative controls and procedures, and additional considerations. In short, it outlines how to design a privacy program element so it measures up to the standard.

For example, Principle 1: Management notes that the entity must communicate its privacy policies and procedures. The practitioner's chart elaborates on how to do this in an acceptable manner. It specifies that privacy policies must be communicated at least annually to those internally responsible for collecting, using, retaining, or disclosing personal information, that changes in policy should be communicated shortly after approval, and that internal personnel must confirm initially and periodically their understanding of the policies and their agreement to comply with them.

The criteria are specific with good reason. The need to audit privacy practices is not lost on the accounting profession, traditionally the source of business auditors. How well a large organization is addressing its privacy risk is something about which most executives and board members will likely seek an objective opinion. In addition, organizations that provide outsourced services requiring personal information – such as payroll or retirement benefits – may want to have an audit professional attest to their privacy risk management practices.

Those who want to measure their own progress in privacy can also use the Privacy Maturity Model (PMM), a tool very like the IGMM; the PMM provides varying degrees of maturity for each of the GAPP principles. Access it at: *http://www.cil.cnrs.fr/CIL/IMG/pdf/10-229_aicpa_cica_privacy_maturity_model_finalebook_revised.pdf.*

The Generally Accepted Privacy Principles

Privacy Principle	The entity:
Management	Defines, documents, communicates, and assigns accountability for its privacy policies and procedures
Notice	Provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained and disclosed
Choice and Consent	Describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use and disclosure of personal information
Collection	Collects personal information only for the purposes identified in the notice
Use, Retention and Disposal	Limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. Retains personal information only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information
Access	Provides individual with access to their personal information for review and update
Disclosure to Third Parties	Discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual
Security for Privacy	Protects personal information against unauthorized access (both physical and logical)
Quality	Maintains accurate, complete and relevant personal information for the purposes identified in the notice
Monitoring and Enforcement	Monitors compliance with its privacy policies and procedures and has procedures to address privacy related complaints and disputes

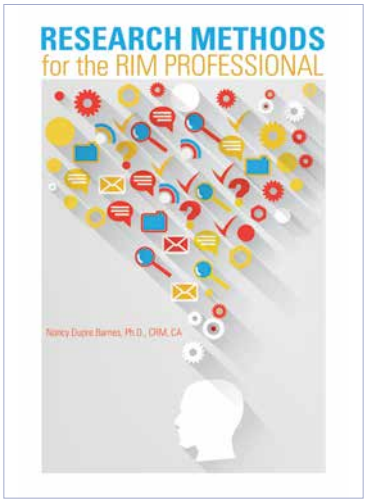
Source: The American Institute of Certified Public Accountants (*www.aicpa.org*) and the Canadian Institute of Chartered Accountants (*www.cica.ca*)

The Principles and GAPP

Given the groundswell of support for legislation regarding privacy, IG professionals would do well to understand the relationship of the Principles and GAPP, even though privacy may not be part of their current mandate. Jason Stearns, IGP, CRM, director of information governance compliance at global investment management company BlackRock, noted how the Principles and GAPP are compatible in his presentation, "Records Management and Privacy

New!

Resources for Advancing Your Career

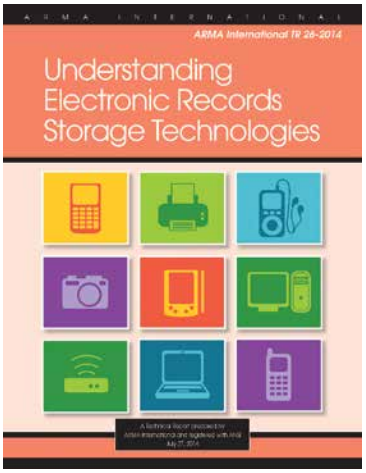


Research Methods for the RIM Professional

Nancy Dupre Barnes, Ph.D., CRM, CA

In this era of "big data," records and information management (RIM) professionals that have a basic understanding of the foundational theories buttressing data analysis, such as research methods, have increased value to their organizations. This book serves as an introduction to research methods, using examples that are specifically relevant to archives and RIM professionals, where possible. It will also help IGP candidates improve the knowledge and skills referenced in the DACUM chart domain of "Managing Information Risks and Compliance."

A4970 Soft cover **$60.00** Professional Members: **$40.00**



Understanding Electronic Records Storage Technologies

(ARMA International TR 26-2014)

This technical report includes a broad discussion of storage technologies and service offerings for electronic records, including operational issues such as outsourcing considerations and contract-related elements. It includes checklists and information purchasers can use for creating a request for proposal and for evaluating and selecting electronic records storage service providers.

Note: This publication does not address the storage of physical records, which is covered in *Guideline for Evaluating Offsite Records Storage Facilities*.

A4958 Soft cover **$60.00** Professional Members: **$40.00**

Order your copy online today!

ARMA INTERNATIONAL BOOKSTORE

www.arma.org/bookstore

See these titles and much more at the ARMA Bookstore during ARMA LIVE! 2014 in San Diego, October 26-28!

ARMA sandiego 2014

Concerns – A Marriage of Principles." Stearns has seen the difficulties that arise in trying to retrofit privacy requirements onto information management systems; he offers three examples.

The desire to … make the most of an existing resource may have to be tempered with the need to meet international data privacy … restrictions

Case Study: The Shared Database

A particular line of business in financial services designed a database in the Americas to track customer order history and account performance. The database was quite successful, and eventually other lines of business started to use it, several of which were outside the United States. Over time, retention requirements began to conflict:

- U.S. data had a six-year retention requirement, but data originating in another country had a 10-year requirement.
- France required that data about its citizens be disposed of once the relationship with the company ended.
- Co-mingling was permitted when the database was designed, but it was not permitted later.

Accommodating all the requirements became impossible. Client information was commingled in one set of database tables but not another, precluding the possibility of simply sorting the database by country. Stearns said that after examining the additional risk of long retention, the company chose to keep all the data for the longest required retention period, i.e., 10 years.

He also noted that this particular example became a cautionary tale of how not to do things. The desire to streamline and make the most of an existing resource may have to be tempered with the need to meet international data privacy retention restrictions going forward.

Case Study: Mining the Data

In another, related example, Stearns related that users of the same database in the United States wanted to send it to a third-party service to do data mining. The business unit had gone so far as to extract data and package it for transmission to the data mining company, being unaware that some countries have restrictions on data being moved. The cause of this potential misstep was lack of education and training about privacy law for those who collect and use data.

Luckily, the company had developed an electronic tool that steps users through the transfer process by asking questions about the type of data, where it originated, and where it is to be sent. Because answering these and other questions reveals whether there are restrictions based on state, national, and international laws, the violation was avoided.

The tool is just a first step, though. Even if no restrictions are found, specific permissions and approvals are still necessary to move the data. The usefulness of the online tool is that it can be updated easily and refined to include new regulations as they come into existence. While this does not fix the problem of what is stored in the database, it does help prevent violating trans-border data requirements.

Case Study: Boxes in the Bahamas

Many countries, notably Germany, the Bahamas, and Mexico, have restrictions on who can look at private data held in that country and on whether the data can leave the country. Stearns told of a case where the company had boxes of records stored in the Bahamas. Box descriptions were held in company-designed software running on a PC located in that country. When the decision was made to discontinue some operations there, Stearns discovered that although the company had the ability to view the box description data from a U.S. location, it was specifically prohibited from doing so by Bahamian law because of its possible privacy implications.

The irony is that boxes eligible for destruction could have been identified easily by just the records category, but again, this could not be done from a remote location. The only solution was to send a company employee to the Bahamas to complete the task.

Stearns noted that for many older systems, it is not even possible to eradicate stored data or to partition it according to country of origin. He strongly advises to invest in Privacy by Design when building a new system or doing a significant upgrade. [Editor's note: See this issue's cover story by Norman Mooradian, Ph.D., "Closing the Gap Between Policy and ECM Implementation Using Privacy by Design.]

"Having tools like the Principles for information governance and GAPP for privacy is an advantage," Stearns said. "They are based on international standards and the issues they address are important to preserving business advantage whether at home or abroad."

Not Once and Done

As with so many aspects of information management, protection is not "once and done" where privacy protection is concerned. Continuous improvement with the help of the IGMM and outside audits will be factors in assessing risks and making intelligent policy decisions going forward. **END**

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

Vendors, Products & People

BULLETIN BOARD

recall™
Your Information. Securely Managed.

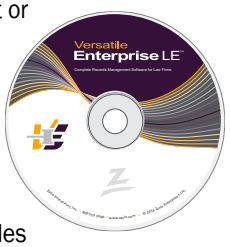
Recall Holdings Limited (ASX: REC), a global leader in information management, announced that it was awarded ISO/IEC 27001:2005 Management System certification by SRI Quality System Registrar on December 19, 2013. Recall is the first information management company to achieve ISO27001 Certification for 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.

RSD is the global leader in Information Governance. Its purpose-built platform, RSD GLASS™, makes it easy for companies in highly-regulated industries to solve the complex problem of what information they should keep and what information they should delete with its policy management and enforcement engine. It is the only platform that orchestrates and maintains information governance while keeping information in its place. RSD GLASS™ lets companies create corporate policies that are actively enforced across organizational and jurisdictional boundaries, IT systems, content repositories, cloud-based applications and paper archives. To learn more, go to ***www.rsd.com***.

ZASIO

Versatile Enterprise LETM

Introducing ***Versatile Enterprise LETM*** (Legal Edition) records management software – a breakthrough software essential to managing business, disciplinary, and professional risk in a working law practice. With Versatile Enterprise LE, your law firm will be able to:



- Manage all electronic and physical records related to a client or matter
- Implement consistent adoption of retention and destruction policies for legal records
- Assure your clients that their legal records are secure
- Protect client confidences and preserve client property
- Preserve evidence for defense of professional liability claims
- Provide reasonable basis and motivation for discarding old files
- Assist in compliance with regulatory obligations

To learn more about Zasio's Versatile Enterprise LE, contact Zasio Sales at **800.513.1000, option 1.**

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.

XDD
XACT DATA DISCOVERY
Because you need to know

NAID®

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

Canon

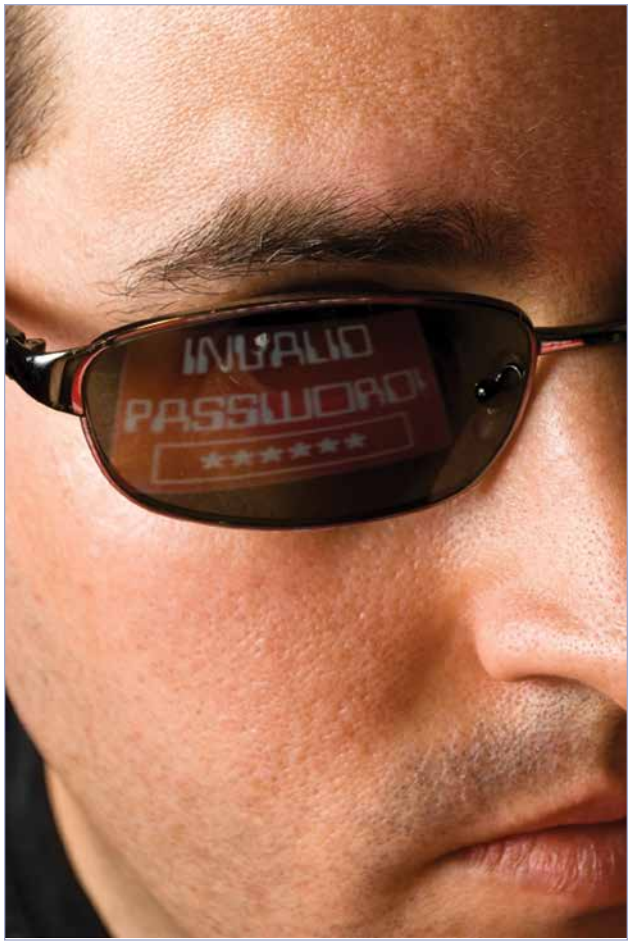
Save $650 with the imageFORMULA DR-M160II High Speed Office Document Scanner Bundled with Kofax VRS Elite

- Scans up to 60 pages per minute; both sides in a single pass
- Handles an assortment of hard copies, from long/oversized documents to embossed plastic cards
- Front LED control panel for one-touch access to pre-programmed scan tasks
- Productivity booster in space-constrained areas

www.usa.canon.com/scanners

10 Things Organizations Should Do to Protect Against Hacking

John J. Isaza, Esq., FAI



A recent *New York Times* report about a Russian gang that collected the Internet security data of 1.2 billion people has stirred a maelstrom of pundits wondering if the situation is as dire as it sounds or just sensationalistic reporting. Regardless, one thing is clear: the mere specter of being hacked reinforces the importance of information governance (IG) and data protection processes, procedures, and technology.

But, some organizations are looking for a "silver bullet" to come along to make it easier for them to stay ahead of the criminals. Indeed, companies like Milwaukee-based Hold Security are now offering monthly fee-based services to help organizations detect if their sites have been affected by this breach. Frankly, though, organizations that need to rely on this type of service to protect themselves will remain a prime target; this incident should serve as a huge wake-up call for them to take more proactive steps to safeguard their information.

Accountability, Preparation Needed

Most importantly, someone with a high level of authority has to be in charge of information security to ensure that people, processes, and technology are in place and working effectively. This might be a chief data officer (CDO) or some similar officer who is tasked solely with responsibility for ensuring data is protected. The first of the Generally Accepted Recordkeeping Principles® (Principles), the Principle of Accountability, speaks directly to this point. (Read more at *www.arma.org/principles*.)

Stay on top of your information governance ecosystem.

After accountability is assigned, preparation is key. Following is a list of 10 things organizations should do to protect their data and stay ahead of the curve.

1. **Hire or appoint a CDO or a similar executive to be responsible for information security.** (See previous comments.)

2. **Learn from the past**. It has been said that those who do not know history are doomed to repeat it. Start by assessing your organization's previous hacking incidents and learning as much as possible from those experiences. If you have not had any breaches, consider yourself lucky and learn as much as you can from other organizations' breaches.

3. **Hire hacking professionals.** If data is stored locally, retain a consultant or task an employee with figuring out how to hack into the organization's systems. Depending on the size of the organization, this could be a full time job for one or more people.

4. **Vet vendor security.** If data is stored in the cloud or with other third parties, vet the vendors' processes and procedures around data protection. Check to see if they have staff dedicated to information security and whether they are technological game-changers in their space. Since data security should be of the highest priority for cloud vendors, for instance, being on the cutting edge of technology should be expected of them.

5. **Conduct a gap assessment.** A gap assessment is essential to identifying areas of vulnerability for critical assets that need to be protected. According to the Principle of Protection, "…every system that generates, stores, and uses information should be examined with the protection principle in mind to ensure that appropriate controls are applied to such systems."

   Use a maturity model and a scale of 1 to 5 to assess your status, with 1 being non-existent or in a dismal state and 5 being in a transformative state. (Check out the Information Governance Maturity Model at *www.arma.org/r2/generally-accepted-br-recordkeeping-principles/metrics*.) Be vigilant about assessing the more recent areas of vulnerability for many organizations, such as use of:
   - Work-from-home arrangements
   - Airplane, airport, and other public WIFI connections
   - Portable devices
   - Third-party contractors

6. **Update your data map.** Most organizations should have at least a semblance of a data map in connection with e-discovery preparedness, if nothing else. Leverage this data map to assess systems that need higher security and closer attention. Be sure to include data created and stored with third parties, including data in the cloud. (See "Six Steps for Creating a Super Data Map" by Mark Diamond on page 28.)

7. **Stay on top of your information governance (IG) ecosystem.** Most organizations focus on their servers and, maybe their "bring your own device" policies. However, the IG ecosystem is much bigger than that. Organizations need to align their data with all possible uses, compliance, data protection, and all other Principles' concerns.

8. **Update your data security policies and procedures.** Organizations should have a defined set of policies and procedures designed to protect data starting with expectations for every employee. If you do not have them, create them. If you do have them, review them annually to update and revise them as indicated by the results of steps 2 to 5.

9. **Train, train, train employees.** Be sure that all new employees are trained on data security policies and procedures as part of their orientation, and provide ongoing, periodic training for all employees.

10. **Audit, audit, audit systems and employee compliance.** Conduct random audits as part of your system checks and balances to ensure that not only are employees complying, but also that processes and technology are working as expected. Use these audit results to resolve gaps and vulnerabilities.

These recommendations are not exhaustive, and they are not intended to be followed as a one-time process. They need to be entrenched in the organization's culture for those who want to step ahead of today's savvy, information-seeking criminals. **END**

John Isaza, Esq., FAI, can be contacted at John.Isaza@InfoGovSolutions.com. *His bio is on page 47.*

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

DIAMOND GABLE GOSALIA ISAZA MOORADIAN REGA SHIVE

Closing the Gap Between Policy and ECM Implementation Using Privacy by Design
Page 20

Norman Mooradian, Ph.D., , is senior engagement manager at Konica Minolta in the ECM solutions group. He received a Ph.D. in philosophy from the Ohio State University and has completed graduate courses in legal studies at the University of Illinois. He has published many articles on information technology issues and business ethics. Mooradian can be reached at nmooradian@kmbs.konicaminolta.us.

Six Steps for Creating a 'Super Data Map'
Page 28

Mark Diamond is founder, president, and chief executive office of Contoural Inc, an independent provider of litigation readiness and records and information management services. He is an online columnist for *InsideCounsel Magazine*, the author of numerous white papers for the legal and IT communities, and a frequent conference speaker. Diamond has a bachelor's degree in computer science from the University of California San Diego. He can be contacted at *mdiamond@contoural.com*.

Tossing the Tape? Implications of Making the Switch to Disk-Based Backups Page 33

Veeral Gosalia is a senior managing director in the FTI Consulting technology segment, where his areas of expertise include data preservation, data analysis, computer forensics, and e-discovery. He has helped attorneys and corporations understand the issues surrounding the acquisition, analysis, and production of electronic evidence. He can be contacted at *veeral.gosalia@fticonsulting.com*.

Antonio Rega is a managing director in the technology practice at FTI Consulting. His areas of expertise include forensic data acquisitions/analysis, recovery of deleted data, and e-discovery. He has handled high-profile computer forensic investigations and has provided sworn testimony on matters relating to computer forensics and e-discovery — most recently before a grand jury for the U.S. Attorney General's office. He can be contacted at *antonio.rega@fticonsulting.com*.

Matt Shive, managing director at FTI Consulting's technology practice, datacenter engineering, has spent nearly 20 years working with engineers and users to create new technologies and solutions. Shive began his career in IT, supporting PCs and the many office peripherals. Over time his skills and expertise have led to roles designing and supporting advanced datacenter solutions. He can be contacted at *matt.shive@fticonsulting.com*.

The Generally Accepted Recordkeeping Principles® Principles for Protecting Information Privacy
Page 38

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

RIM Fundamentals 10 Things Organizations Should Do to Protect Against Hacking Page 44

John Isaza, Esq., FAI, is a California-based attorney, CEO of Information Governance Solutions LLC, and law partner at RIMON, PC, a 21st century law firm that includes specialties in electronic information governance, records management, and overall corporate compliance. A frequent presenter and writer on these topics, he co-authored the book *7 Steps for Legal Holds of ESI and Other Documents*. Isaza can be contacted at *John.Isaza@InfoGovSolutions.com* or *John.Isaza@RimonLaw.com*. You can also follow him on Twitter and LinkedIn.

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