INFORMATION MANAGEMENT

AN ARMA INTERNATIONAL PUBLICATION

NOVEMBER/DECEMBER 2015

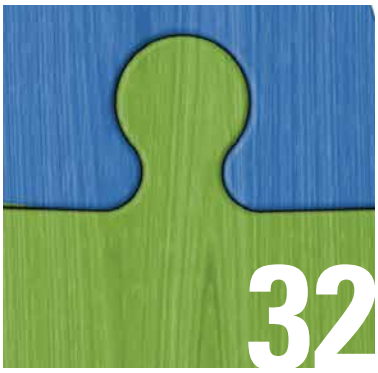
Policies and Processes for Protecting Information Page 20

The Principles, IG Maturity Model: Tools for Professional Growth Page 28

How to Combine RIM Programs After a Merger Page 32

INFORMATION MANAGEMENT

NOVEMBER/DECEMBER 2015 **VOLUME 49 NUMBER 6**



DEPARTMENTS 4 **IN**FOCUS A Message from the Editor

6 **UP**FRONT News, Trends, and Analysis

FEATURES 20 **Policies and Processes for Protecting Information**
Beth Chiaiese, CRM

28 **THE**PRINCIPLES
The Principles, IG Maturity Model: Tools for Professional Growth
Julie Gable, CRM, CDIA, FAI

32 **How to Combine RIM Programs After a Merger**
Blake Richardson, CRM, CIP

SPOTLIGHTS 36 **TECH**TRENDS
Protecting Privacy in an IoT-Connected World
Michael S. Smith, Ph.D., IGP, CRM

40 **LEGAL**MATTERS
Implications of E-Mail Mismanagement and Best Practices for Preventing It
John J. Isaza, Esq.

44 **IN**REVIEW
Learn to Create and Work with Relational Databases
Erik Werfel, J.D., IGP, CIPP-US, CISSP, CEDS

45 **IN**REVIEW
Discovering the Universe of Preservation History and Practice
Stephen E. Haller, CRM

CREDITS 47 **AUTHOR**INFO

48 **ADVERTISING**INDEX

INFORMATION MANAGEMENT

AN ARMA INTERNATIONAL PUBLICATION

Publisher: Robert Baird, PMP

Editor in Chief: Vicki Wiler

Contributing Editors: Nikki Swartz, Jeff Whited

Art Director: Brett Dietrich

Advertising Account Manager: Jennifer Millett

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 governing information as a strategic asset. Established in 1955, the association's approximately 27,000+ members include records and information managers, information governance professionals, archivists, corporate librarians, imaging specialists, legal professionals, IT managers, consultants, and educators, all of whom work in a wide variety of industries, including government, legal, healthcare, financial services, and petroleum, in the United States, Canada, and more than 30 other countries around the globe.

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

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

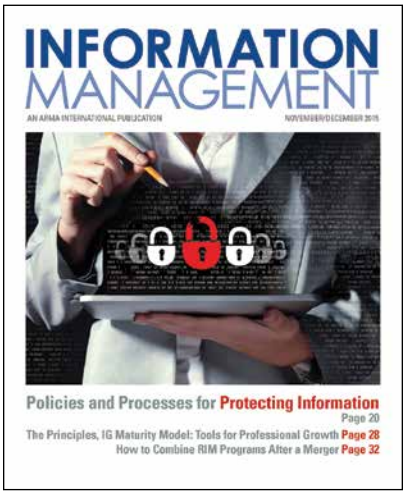
Advertising Inquiries: Contact Jennifer Millett at +1 888.277.5838 (US/Canada), +1 913.217.6022 (International), +1 913.341.3742, or e-mail *jennifer.millett@armaintl.org*.

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.

Focus on Taming Technology to **Maximize Information Security**



No one knows better than records and information management (RIM) professionals that technology is both a blessing and a curse for business. While new and ever-evolving technology tools drive innovation and make many business processes easier and more efficient, they also generate tremendous amounts of information and increase the difficulty of protecting it.

A look at the October 21, 2015, data breach report from the Identity Theft Resource Center shows that there have been 620 breaches of U.S. organizations exposing more than 175 million records this year. And no industry sector is immune – from medical/healthcare organizations, which have accounted for about one-third of the breaches and more than half of the records exposed this year, to education, with the fewest records exposed.

The average cost of a breach in the United States, according to the "2015 Cost of Data Breach Study: United States" conducted by Ponemon Institute for IBM in May 2015, ranged from $5.9 million to $6.5 million – an 11% increase over the previous year. The average cost for each lost record containing sensitive or confidential information increased 8%, from $201 to $217, the report said.

In an excerpt from the ARMA-published book *Confidentiality, Privacy, and Information Security,* author Beth Chiaiese, CRM, provides a great amount of guidance about the policies and processes that will help your organization protect its information. Although written primarily for the law firm environment, this advice is applicable to all business environments.

Rising in tandem with the cost of data breaches is concern about protecting individuals' personal information. The Internet of Things (IoT) – the network of physical objects embedded with electronics, software, and sensors that enable them to collect and exchange data – is a relatively new threat to personal privacy that organizations and individuals need to address. In the Tech Trends sub-feature, Blake Richardson, CRM, raises awareness about the risks associated with IoT and how to mitigate them.

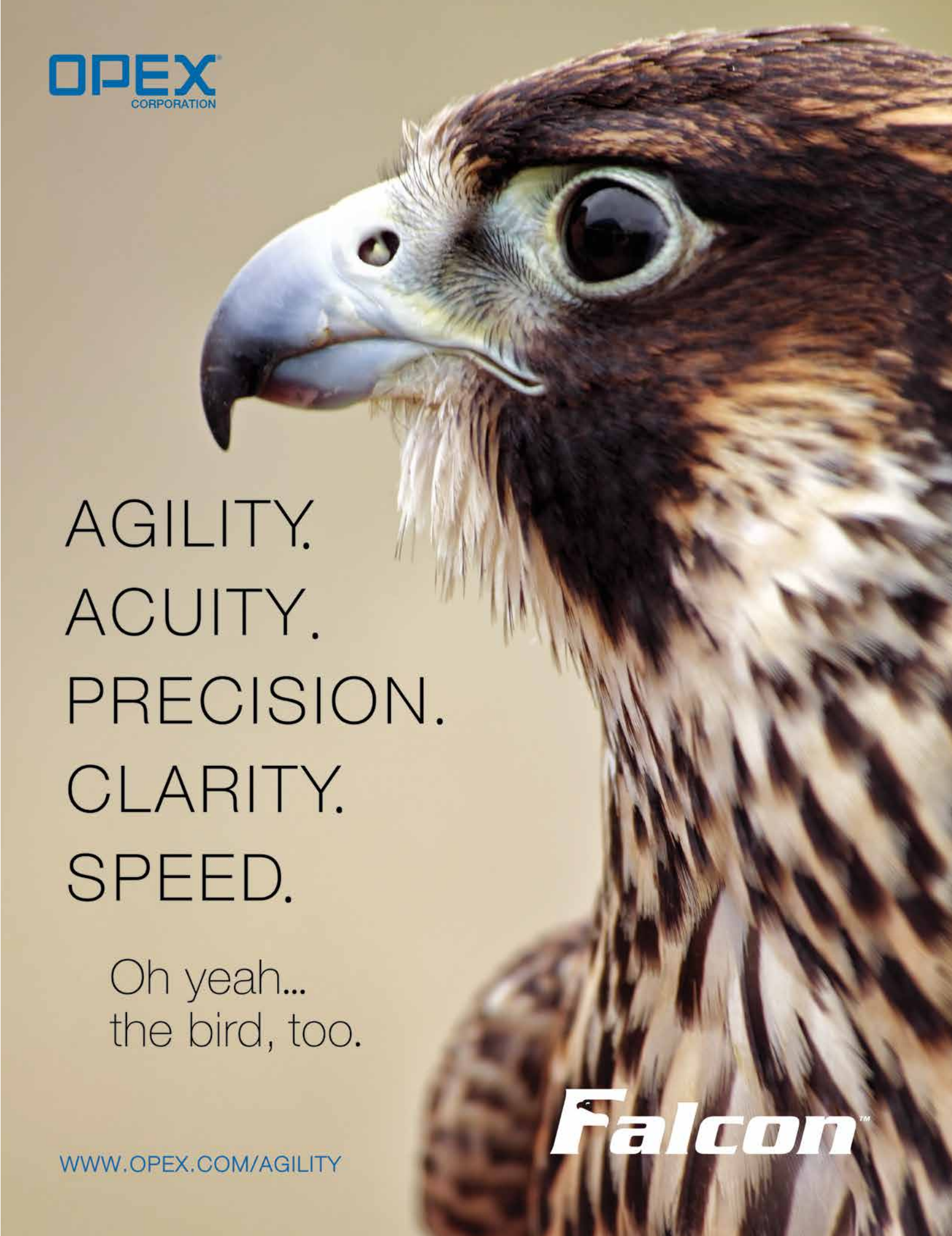
Much higher on the radar screen for business are the risks associated with e-mail, including hacking, destroying it prematurely or keeping it too long, and using personal e-mail accounts improperly for business. John Isaza, Esq., writes about the potential legal repercussions of all of these issues in the Legal Matters sub-feature.

There are also legal risks for organizations involved in a merger, including the potential for violating antitrust regulations with pre-merger discussions between the merging organizations. Blake Richardson, CRM, CIP, writes about those things that can and cannot be discussed pre-merger and the things that *must* be discussed and resolved post-merger to ensure an effective RIM program in the newly merged environment.

To play their leading roles in protecting their organizations and their organizations' information assets, RIM professionals must be credible, able to communicate and collaborate with stakeholders, and open to compromise when needed. In her final Principles series article, Julie Gable, CRM, CDIA, FAI, writes about how they can use the Principles and the Information Governance Maturity Model as tools that will help them in these areas, advancing not only their organizations' RIM programs, but also their careers.

Tell us how we can help you with your career advancement at *editor@armaintl.org*.

Vicki Wiler
Editor in Chief


OPEX
CORPORATION
AGILITY.
ACUITY.
PRECISION.
CLARITY.
SPEED.
Oh yeah...
the bird, too.
Falcon™
WWW.OPEX.COM/AGILITY

GOVERNMENT RECORDS

Survey: Federal Agencies Don't Trust Their E-Discovery Programs

Three-quarters of U.S. federal agency legal and record management teams say they lack confidence in the quality of their e-discovery programs, according to a survey.

Deloitte's "Ninth Annual Benchmarking Study of Electronic Discovery Practices for Government Agencies" reveals that agencies are getting better at responding to the ever-increasing number of requests to produce electronically stored information (ESI). But when it comes to defending those records before opposing lawyers or Congress, three out of four said they were "not confident" their agency could demonstrate their ESI is "accurate, accessible, complete, and trustworthy."

However, the majority (85%) of respondents said they were more confident, or just as confident, as they were a year ago in their ability to manage e-discovery demands.

This apparent contradiction suggests two concurrent trends, said Chris May, a principal with Deloitte Transactions and Business Analytics. Agencies are gaining more experience with e-discovery tools and thus are more confident in their abilities to manage ESI-related inquiries. Yet they are also concerned about resource constraints, a point highlighted by the top three challenges respondents cited in identifying ESI: insufficient staffing, insufficient time, and the volume of data to manage.

"While the tools and technologies continue to mature along with our understanding of ESI, the expanding scope of the issue is daunting, especially since agency resources aren't growing commensurately," May said.

The study also found that mobile devices are playing a bigger role in the document preservation and collection processes that federal government agencies manage in response to legal cases and other information requests.

The percentage of federal government agency legal and records management teams processing requests for data from mobile devices more than doubled in 2015, to 54% from 26% in 2014, according to the study.

CYBERSECURITY

U.S., UK Firms Not Protecting their Cyber Borders

According to a recent survey, 53% of U.S. IT decision makers said it would be at least somewhat easy for a former employee to log in and access data; 32% of UK respondents answered similarly.

Half of all respondents said it can take up to seven days or more to remove access to sensitive systems, highlighting a huge need for securing their company's digital borders.

In fact, Centrify found that 55% of U.S. respondents said their organizations had been breached, and 44% suffered breaches that collectively cost millions of dollars. This compares to 45% and 35%, respectively, of the UK respondents.

Despite the high costs of data breaches, IT managers say their cries for help often go ignored or unheeded. According to the Centrify survey, 48% of U.S. and 30% of UK respondents said they have had to fight their organizations for stricter protocols. Forty-two percent of U.S. and 27% of UK respondents said they have lost the battle for stricter protocols. And 28% of U.S. and 40% of UK respondents said security isn't getting enough attention.

INFO SECURITY

Appeals Court Upholds FTC's Authority Over Data Security

A U.S. appeals court has silenced any questions about whether the Federal Trade Commission (FTC) should have the authority to punish companies for security breaches.

The decision in *FTC v. Wyndham Worldwide Corp.* solidifying the FTC's data security authority stems from a series of hacks of Wyndham's computer systems in 2008 and 2009. The personal and financial data from more than 619,000 customers was stolen, resulting in more than $10.6 million in fraudulent charges.

The FTC filed suit in June 2012, alleging that Wyndham had engaged in "unfair and deceptive" cybersecurity practices since 2008 that "taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft."

Wyndham challenged the FTC's authority to regulate data security issues under the "unfairness" prong of the FTC's consumer protection powers, and the Third Circuit answered with a resounding "yes." The ruling also gave the go-ahead on the lawsuit against Wyndham.

"While the FTC has been active in seeking to address data security issues, this is the first major ruling confirming that it has the authority to do so," Michael Hindelang, head of the data security/privacy litigation and e-discovery/information management practice groups at Honigman Miller Schwartz and Cohn, told *Legaltech News*.

Hindelang predicted that the FTC will likely "look to increase its regulatory activity in this area now that its authority has been upheld. Accordingly, companies that don't adequately protect their customers' data run the risk of having their behavior deemed an unfair trade practice by the FTC."

The U.S. Department of Justice (DoJ) released in April "Best Practices for Victim Response and Reporting of Cyber Incidents" to help companies develop a response plan. The guidance reflects "lessons learned by federal prosecutors while handling cyber investigations and prosecutions, including information about how cyber criminals' tactics and tradecraft can thwart recovery."

The key, of course, is to conduct as much planning as possible before a breach takes place. By defining a process in advance that clearly defines roles and responsibilities for all players in a breach response, an organization can respond quickly and efficiently within pre-established parameters.

PRIVACY

Twitter Report Shows Rise in Government Data Requests

Information requests on Twitter users are at an all-time high, according to a transparency report released by Twitter.

According to the report, 4,363 information requests from 62 nations were made between January 2015 and June 2015, with four previously unlisted countries (Cyprus, Dominican Republic, Poland, and Serbia) joining the pool of governments seeking information from the social media giant. The Twitter report states, "information requests include worldwide government requests we've received for account information, typically in connection with criminal investigation," and of the requests that Twitter received, about 58% resulted in the release of information.

The first half of 2015 marked a 53% spike in the number of requests made by governments and included 78% more users than the previous reporting period.

Information requests were denied for a number of reasons, among them failure to identify a specific Tweet or Twitter account, as well as overly broad requests or challenges made by those targeted, the report said.

The United States was by far the most prolific petitioner of information, making requests 2,436 times for 6,324 accounts. Information was turned over in 80% of the cases. Japan was the second-largest requester, followed by Turkey and the UK.

GOVERNMENT RECORDS

Many Federal Employees Use Personal E-mail for Work

The Presidential and Federal Records Act Amendments of 2014 prohibit federal personnel from using personal e-mail accounts for public business unless messages are transferred to the federal government's system within 20 days.

But federal requirements are not preventing government employees from using their personal e-mail accounts for work, and many who do so are using unsecure technology without considering the security and privacy risks, according to a survey from Alfresco Software.

The survey, which questioned a small sample size of government employees (100), also found that about 33% of them said they used their personal accounts for work e-mail at least occasionally – and nearly 10% said they exclusively use their personal e-mail accounts for work.

The remaining two-thirds of government respondents said they never used their personal e-mail for work.

By comparison, about half of the 650 private-sector workers who took part in the survey said they used their personal e-mail for work.

The survey also found that many government workers don't take data security or privacy issues into account when they share information with vendors or other external stakeholders. Just 56% said they always take those concerns into account.

The survey found that about 11% of government workers never consider data security and privacy concerns, 20% occasionally do, and 12.5% often do.

INFO SECURITY

Long-Term Care Home Hired Chicken Farm to Shred Sensitive Records

A Canadian long-term care company found itself in hot water over its plan to let a chicken farm shred its sensitive health documents.

A chicken farm should not be used to dispose of sensitive health documents, said Ron Kruzeniski, Saskatchewan's privacy and information commissioner, as he announced he was cancelling the agreement, according to media sources.

CBC News reported that the privacy office had been investigating Spruce Manor Special Care Home in Dalmeny after some of the residents' health cards ended up in a recycling bin.

The investigation revealed that the home had signed a contract with an undisclosed chicken farm to destroy its confidential records. In the agreement, the farm said it would "agree to accept full responsibility to maintain the security and confidentiality of all documents" received from Spruce Manor Special Care Home, CBC News said.

That's "unacceptable," Kruzeniski said in his report. He noted that the agreement does not specify how the chicken farm planned to "maintain the security and confidentiality" of the personal health information it received.

"I recommend that Spruce Manor Special Care Home no longer use [a] chicken farm to destroy records in spite of the former administrator asserting he had no problems/concerns with the use of the chicken farm," Kruzeniski said in the report.

According to CBC News, it's unclear whether any sensitive documents ever went to the farm. An administrator at Spruce Manor indicated the farm wasn't involved in destroying records.

The care home ended its contract with the chicken farm and said it is looking for a certified company for all future document shredding.

PRIVACY

States Moving to Protect Student Data

Apps and sites used in schools today feature software that may collect and analyze a vast array of details about the habits and activities of individual students. For example, many schools assign students Gmail or Microsoft e-mail addresses and use those companies' programs for student calendars, documents, web searches, and file-sharing. Some also employ data-driven math and language apps that may record and analyze thousands of pieces of data about each student with the goal of customizing lessons on the spot to that student's abilities and tastes, the *New York Times* said.

This data collection has raised concerns about whether school districts are equipped to monitor and manage how online education services and schools are safeguarding students' personal details. Some legislators have pointed out the risk of identity theft and predatory marketing.

As schools themselves increasingly analyze socioeconomic, behavioral, and emotional data about students, some parents are more troubled by the possibility that the data could be used in making decisions that could potentially affect their children's future college or job prospects, the *Times* reported.

California, a national trendsetter in privacy legislation, enacted a landmark law that specifically prohibits online school services from using students' personal data to show them personalized ads, as well as restricts the services from employing student data for non-school purposes.

This year, according to the *Times*, about two dozen states introduced similar bills. And five bills have been introduced in Congress aimed at protecting student information.

About 170 companies – including Apple, Google, and Microsoft – have voluntarily agreed to refrain from using the student data collected by their classroom products for personalized advertising.

GOVERNMENT RECORDS

Watchdog Seeks to Amend Legal Opinion Limiting Data Access

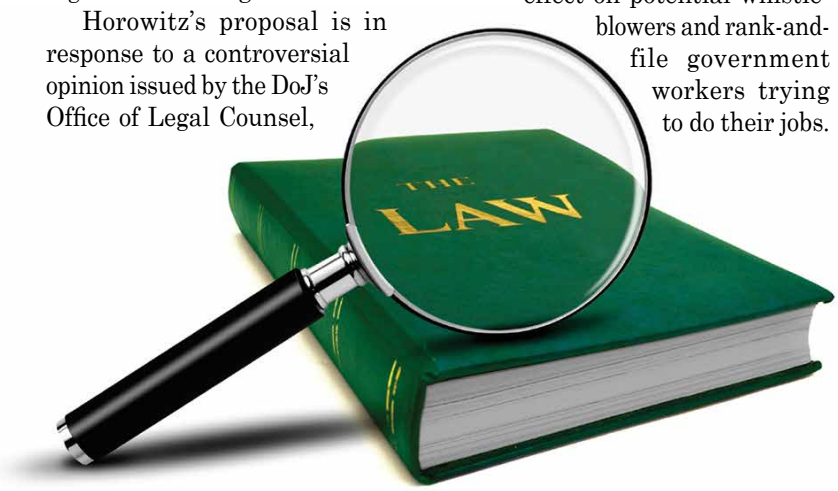
U.S. Department of Justice (DoJ) Inspector General Michael Horowitz has asked Congress to amend the 1978 Inspector General Act to specify that the only information a federal agency can withhold from its inspector general (IG) records that Congress specifically states it does not want watchdogs to see, according to the *Washington Examiner*.

Horowitz's proposal is in response to a controversial opinion issued by the DoJ's Office of Legal Counsel, stating that agency officials can withhold documents from IGs if a law, such as the Fair Credit Reporting Act, blocks their dissemination.

According to Horowitz, if Congress didn't actually mean "all" when it wrote in 1978 that "all records" within an agency's possession should be given to its IG, then it should pass a new law detailing which documents IGs cannot have. Otherwise, he told Federal News Radio, the Inspector General Act should override the Fair Credit Reporting Act and other laws referenced in the Office of Legal Counsel's opinion, such as those protecting information resulting from a wiretap or grand jury proceeding.

"Do you want independent oversight or do you not want independent oversight?" he rhetorically asked lawmakers. The legal opinion states that IGs must ask permission to review information from the very officials they are supposed to be overseeing. "That, in our view, is not independent oversight," Horowitz said.

Horowitz said the 72-member Council of Inspectors General that he leads is "in complete agreement" that their access to information "must be absolute." Beyond potentially hindering investigations, he said the watchdogs worry that the legal opinion could have a chilling effect on potential whistleblowers and rank-and-file government workers trying to do their jobs.



E-DISCOVERY

Counsel's Poor Supervision of ESI Preservation and Production Brings Sanctions

A U.S. federal magistrate judge has issued what some legal experts are calling a "stunning sanctions order" in *HM Electronics v. R.F. Technologies* against multiple defendants and their counsel for widespread discovery misconduct.

The order, which included monetary sanctions as well as a recommendation that sanctions and an adverse inference instruction be imposed on the defendants, is being described as a "wake-up call" to attorneys to become competent in e-discovery.

It was alleged that the defendants "intentionally withheld and destroyed highly relevant electronically stored documents," according to a 78-page order from U.S. Magistrate Judge Mitchell Dembin. The order said the defendants "threatened to interfere with the rightful decision of the case."

In the order, the magistrate noted that the lawyers did not issue a litigation hold, did not do proper follow-up, and overlooked certain issues, concluding that, "this type of lawyering falls below the standard … for discovery."

According to Philip Favro, senior discovery counsel at Recommind, the court identified several breakdowns in the discovery process – some inadvertent and others intentional – that resulted in the sanctions. Key issues were that counsel:

- Certified that clients' discovery responses were true without conducting "a reasonable inquiry" into their truthfulness. Because many of those responses were found to be "false" and "misleading," sanctions were issued under Federal Rule of Civil Procedure (FRCP) 26(g)(3).
- Counted on its client's assertion that it "did not delete documents in the normal course of business," rather than implementing a litigation hold to help ensure the preservation of relevant documents. This resulted in key documents being destroyed and sanctions being levied under FRCP 37.
- Failed to supervise ESI production, allowing the client to withhold a large volume of ESI that should have been produced.

The court held, according to Favro, that by passing off the search and review process to the clients and then taking no steps to verify compliance, counsel fell far short of its duty to supervise others "who are involved in the document collection, review, and production process." The court cited California State Bar ethics opinion no. 2015-193, which says this is "non-delegable," as counsel "must maintain overall responsibility for the work" at all times.

RETENTION

Wall Street Banks Reach Deal on Digital Data Retention

Four of Wall Street's biggest banks have agreed to cooperate with New York regulators and retain copies of communications sent through the messaging platform known as Symphony.

The New York State Department of Financial Services (DFS) was concerned that the platform would allow traders to delete or encrypt information that could be used to track evidence of rigging schemes among traders at various banks. According to the *New York Times*, messaging in chat rooms is believed to have figured prominently in schemes to manipulate global exchange rates and benchmark interest rates.

Deutsche Bank, Goldman Sachs, Credit Suisse, and Bank of New York Mellon have agreed to keep copies of all electronic communication sent through the Symphony platform to and from one another for seven years. They have also agreed to store the duplicate copies of decryption keys for messages with independent custodians. The agreement essentially nullifies a feature initially marketed by Symphony that allowed for "guaranteed data deletion."

"This is a critical issue since chats and other electronic records have provided key evidence in investigations of wrongdoing on Wall Street," said Anthony J. Albanese, the acting superintendent of the DFS, in a statement. "It is vital that regulators act to ensure that these records do not fall into a digital black hole."

Symphony was created by Goldman Sachs and is backed by a consortium of major banks. It has become an alternative to Bloomberg's chat program used by traders and investors around the world. The four banks that reached agreements with the DFS represent the banks with the consortium that the DFS regulates.

GOVERNMENT RECORDS

Former U.S. State Department Staffer to Head Records Management Reform

A former U.S. State Department official has been tapped as its first transparency coordinator, a newly created position meant to reform the way the department manages its records.


Jacobs

Janice Jacobs, who was assistant secretary for consular affairs, is now in charge of improving document preservation and records systems, according to a statement from Secretary of State John Kerry.

She will work with federal agencies and the private sector to explore best practices and new technologies for preserving records. Kerry said he also wants Jacobs to focus on improving systems that are responsible for responding to Freedom of Information Act and congressional requests to make them faster and more efficient. The department has seen a 300% increase in FOIA requests since 2008 as well as numerous requests for information from members of Congress, the statement said.

"It is clear that our systems and our resources are straining to keep pace with the growing number of records we create and the expanding demand for access to them," Kerry said.

Jacobs has a history of reforming records and information sharing programs at State. During her previous time there, she reorganized the visa office after 9/11 and revised how the department shared information with the law enforcement and intelligence communities.

E-DISCOVERY

Greatest Obstacle to ESI? Lawyers Say Soaring Data Volumes

According to a survey from software solution provider Exterro, searching through large amounts of electronically stored information (ESI) to find data is the top challenge for both IT and legal teams at global organizations.

The survey, "The Biggest Obstacles in Locating Responsive Data," reveals that the second-largest obstacle is identifying and accessing data sources for collection.

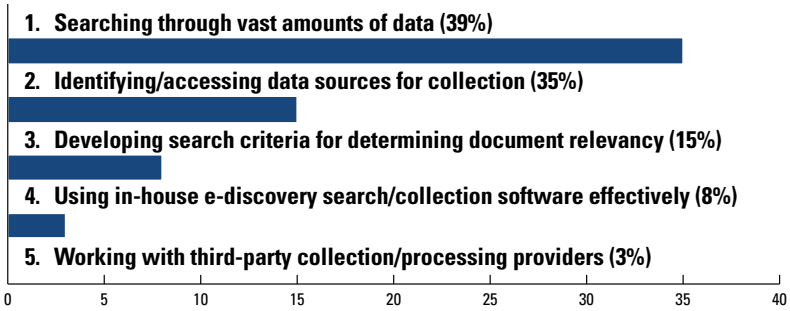
To ease the challenges associated with the e-discovery identification process, the survey advises organizations to take a more proactive approach to managing their data infrastructure, with an eye toward e-discovery optimization.

"For instance, having an updated data map will enable legal teams and IT to quickly identify potentially relevant data sources. Furthermore, utilizing file analysis software can make it easier to find data associated with specific custodians stored throughout their organizations," Bill Piwonka, chief marketing officer of Exterro, explained in an interview with *Legaltech News*.

He also suggests organizations take the following steps:

1. **Automate the custodian interview process.** Use e-discovery interviews to quickly identify other relevant custodians and data sources where responsive information may reside and to get insight into the critical information necessary for properly scoping your search criteria.
2. **Analyze data pre-collection.** In-place search technology empowers legal teams to rapidly identify and locate critical documents in a dataset before collection, dramatically reducing cost and complexity.
3. **Create an integrated search/collection solution.** Streamline data collection and processing by using e-discovery search and collection solutions that can integrate with commonly collected data sources.
4. **Leverage information governance solutions.** Proactively use data mapping and file analysis software to maintain a current view of information across the IT infrastructure.

Exterro's survey results ranked the greatest obstacles for finding responsive ESI as follows:



The Exterro survey was based on 208 responses from in-house attorneys, IT, paralegals, and litigation support professionals in July 2015.

CLOUD

Gartner: Line Between Personal, Business Cloud Use Getting Blurrier

Gartner Inc. predicts that the importance of the personal cloud will continue to grow and that those responsible for building the digital workplace will be increasingly challenged as the personal cloud continues to evolve and intersect with IT initiatives.

"The personal cloud is the collection of content, services, and tools that users assemble to fulfill their personal digital lifestyle needs across any device. Each user's personal cloud is unique and evolving, as the user's daily needs change and as vendors and products come and go," said Stephen Kleynhans, research vice president at Gartner. "Looking forward, we see continued upheaval and challenges from the blending of personal and corporate digital tools and information within each user's life."

According to Gartner, the next wave of the personal cloud will be shaped by two key trends: 1) increased access to personal information and 2) increased intelligence applied to the user experience and against the user's information.

"The rate of change is accelerating as new technologies like Windows 10, ubiquitous sensors, wearables, and smart machines alter the landscape and further blur the lines between consumer and enterprise computing," Kleynhans said. "By 2018, 25 percent of large organizations will have an explicit strategy to make their corporate computing environment similar to a consumer computing experience."

In its report "The Evolving Role of the Personal Cloud in the Digital Workplace," Gartner specifies three areas where the next wave of the personal cloud will influence corporate environments:

1. Virtual personal assistants (VPAs) will increasingly become the anchor point for users' personal clouds and have broad access to both user and corporate data, creating potential security challenges for the digital workplace manager.
2. VPAs are emerging as a critical new service that can hide the differences between multiple services and apps; in the past few years all three of the big smartphone platforms (Apple iOS, Google Android, and Microsoft Windows Phone) have added a VPA capability.
3. VPAs often have access to not only personal data, but also potentially sensitive corporate information about meetings, employee travel, and business operations. Gartner says VPAs will evolve to play different roles — a personal one, a corporate one, and perhaps even a group or team one. This will enable IT organizations to exercise some control over one context while still allowing some freedom for users. Some organizations will be tempted to block use of VPA access to corporate data. However, this will reduce a VPA's effectiveness and encourage employees to bypass IT controls.

This flood of real-time data further blurs the line between work and personal, highlighting critical security and privacy issues for both users and enterprises. According to Gartner, a reliable, secure way for users to ensure the security and integrity of data within their personal clouds will be crucial going forward.

FOI

Court: Texts on Public Employee's Phone Are Public Records

The Washington Supreme Court has unanimously ruled that a public employee's work-related text messages sent and received on a private cellphone are public records.

The case was filed by Pierce County Sheriff's Detective Glenda Nissen, who claimed that Prosecutor Mark Lindquist banned her from his office after she criticized him and supported his opponent. Nissen had requested Lindquist's call and text records, including texts he made and received on his private cellphone.

In response, Lindquist provided a "call log" and "text message log," which included the dates and times of calls and messages as well as phone numbers, but not the content of the messages. Lindquist acknowledged that some of the calls and texts were work-related.

The county gave partially redacted copies to Nissen, but she sued the county, arguing that the records relating to his work should be made public. The trial judge sided with the county, saying private cellphone records are not public records.

The Supreme Court, however, disagreed and ordered Lindquist to produce those records to the county.

Nissen argued that Lindquist sent and received text messages in his official capacity "to take actions retaliating against her and other official misconduct." The court said that since the county and Lindquist acknowledged that some of his texts were work-related, transcripts of those messages are potentially public records.

Therefore, the court ordered Lindquist to get a transcript of his text messages and turn over to the county any that are public records so they could be sent to Nissen.

"As to text messages that Lindquist in good faith determines are not public records, he must submit an affidavit to the county attesting to the personal character of those messages," the court said. "The county must produce that affidavit to Nissen."

In a statement, Lindquist said the case was about constitutional privacy protections for personal phones.

The high court compared the case to a ruling it made five years ago, when it determined that the Washington Public Records Act applied to data stored on a personal computer. Justices argued then that a government worker who tries to circumvent the act by using a home computer would drastically undermine the law.

They reasoned that it would be an affront "to the core policy underpinning the (public records act) – the public's right to a transparent government" – if it didn't include all records that public employees prepare, own, use, or retain in the course of their jobs.

The justices listed certain situations in which their ruling would not necessarily apply – for example, the ruling doesn't impact a public employer wanting to seize a worker's private cellphone to search for public records, or a citizen wanting to sue a public employee for private messages.

FOIA

Court: Accidental Disclosure Does Not Waive Privilege

The California Public Records Act (PRA), which is similar to the U.S. Freedom of Information Act, gives its citizens the right to inspect or to force disclosure of government records to the public upon request. There are some limits, including protecting the attorney-client privilege, as one school district learned after accidentally releasing privileged documents in a PRA request.

In *Newark Unified Sch. Dist. v. Superior Court*, two community organizations requested documents from the Newark (Calif.) Unified School District regarding the school superintendent's resignation. The school district produced the documents, but soon after realized that some of the information contained within them was protected by the attorney-client privilege.

The district asked, and then filed a complaint against, the community organizations to recover the documents, but the organizations refused. The school district, the plaintiff in the case, argued for a temporary restraining order, which was initially denied by the superior court. The defendants, on the other hand, argued that under the PRA, the "disclosure" of a public record constitutes a waiver of applicable exemptions from disclosure.

Ultimately, the San Francisco-based First District Court of Appeal sided with the school district and barred the dissemination of the accidentally produced materials. First, the court ruled, the "waiver" does not cover accidental disclosure. The court considered the legislators' intent behind the PRA, saying that it was "to prevent public agencies from disclosing documents to some members of the public while asserting confidentiality as to other persons. Waiver as a result of an inadvertent release, while not necessarily inconsistent with the Legislature's intent, was not within its contemplation."

The court also ruled that an interpretation favoring the waiver could leave the PRA open to manipulation. Instead, it wrote, "An attorney who receives inadvertently produced documents during discovery has an ethical duty to refrain from unnecessary review of the documents, notify opposing counsel, and return the documents upon request."

This is not the final word on the matter, however. In 2014, a different California appeals court held the opposite view in *Ardon v. City of Los Angeles*, finding that "disclose" within the PRA meant any disclosure of public records, regardless of intent. The California Supreme Court agreed to hear that case in March, where it will likely decide whether to back the Newark Unified or Ardon ruling.

PRODUCTIVITY

Survey: Workers Lose Six Hours a Week on Document Searches

Workers in paper-based offices lose at least six hours a week to searching for documents, according to a recent survey. Meanwhile, employees in digital offices reported almost no time lost.

The survey by Software Advice was small, including only several hundred people, but of those, 91% of digital office employees (almost 100 respondents) said digital management systems make their jobs "somewhat" or "significantly easier." Digital office workers also acknowledge that some forms of paper documents remain in the workflow, most notably faxes (35%), notes between co-workers (35%), and legal documents or contracts (29%).

Another task that cuts into worker productivity is time spent creating reports from paper documents, the survey showed. Collectively, employees reported spending about 1.6 hours per day, or more than eight hours a week, building reports from information contained in paper documents.

Time Spent Per Day Searching for Documents in Traditional Offices

30%	<10 minutes
19%	30 minutes
21%	1 hour
15%	2 hours
9%	3-4 hours
6%	5-6 hours

Source: Software Advice

174 Strong. And Growing.

Congratulations to these
Certified Information Governance Professionals

Elizabeth Adkins
Pey-Jia Angell
Christine Ardern
Deborah Armentrout
DeAnna Asscherick
Randy Aust
Christie Baird
Salvador Barragan
Christopher Beahn
Richard Berlin
Margaret Boeringer
Isabel Bracamontes
Susan Burd
Doug Caddell
Stacie Capshaw
Melissa Carlis
Diane Carlisle
Laurie Carpenter
Alexander Carte
Mark Carter
Anita Castora
Elizabeth Castro
Tod Chernikoff
Carol Choksy
Vicki Clewes
Julie Colgan
Bud Conner
Dani Cook
Marvin Cross
Kristen Crupi
Becky Darsch
Lisa Marie Daulby
Nicholas De Laurentis
Melissa Dederer
G. Derk
Deborah Dotson
Christina Doyle
Sandra Dunkin
Priscilla Emery
Sofia Empel
Tony Epler
Debra Farries
Elizabeth Farthing
Carol Ann Feuerriegel
Glenn Fischer
Matt Fisher
David Fleming
Patricia Franks
Rhonda Galaske
Caroline Gallego
Stephen Garner
Charles Garrett
Irene Gelyk
Sue Gerrity
Kimberly Giertz
Susan Goodman
Joshua Grisi
Komal Gulich
Jocelyn Gunter
Allen Gurney
Michael Haley
Grace Hammar
Joshua Hargrafen
Paula Harris
Charles Herbek
Margaret Hermesmeyer
Caroline Higgins
Gordon Hoke
Patricia Huff
Janice Hulme
Bethany Hynes
Leigh Isaacs
Mary Frances Janicik
C'Les Jensema
Chris Johnson
Todd Johnson
Deborah Jostes
Deborah Juhnke
Soo Kang
Andrew Keller
James Kennedy
Anju Khurana
Ellie Kim
Michelle Kirk
Tamara Koepsel
Greta Krapac
Peter Kurilecz
Tera Ladner
Ronald Layel
Anna Lebedeva
Gilles Legare
Donnell Long
John Loveland
Eric Lynn
Cindy MacBean
Rudolph Mayer
Brian McCauley
Stephanie McCutcheon
Cheryl McKinnon
James Merrifield
Sandy Miller
Dana Moore
Dermot Moore
Rafael Moscatel
Linda Muller
Jen Murray
Stephen Murray
Joe Nadzam
Lindy Naj
Peggy Neal
Lee Nemchek
Sheri Nystedt
Carolyn Offutt
James Owens
Eleanor Ozaeta
Lewis Palmer
Jadranka Paskvalin
Alan Pelz-Sharpe
Graham Pescod
Denise Pickett
Debra Power
James Presley
Cindy Pryor
Fred Pulzello
Tony Ratcliffe
Joshua Rattan
Jessica Rickenbach
Deborah Rifenbark
Carol Rittereiser-Coritt
David Rohde
Donna Rose
Kathryn Scanlan
Danna Schacter
Teresa Schoch
Terry Schrader
Karen Schuler
Mary Sherwin
William Silvio
David Skweres
Michael Smith
Natalie Spano
Brian Starck
Jason Stearns
David Steward
Melissa Suek
Paula Sutton
Marjorie Swain
Sheila Taylor
Robin Thompson
Brian Tretick
Susan Trombley
Nathan Troup
Brian Tuemmler
Martin Tuip
Amy Van Artsdalen
James Vardon
Jennifer Watters Farley
Bridgett Weldner
Erik Werfel
Steven Whitaker
Kristi Whitmore
Jesse Wilkins
Marc Willemse
Dylan Williams
Steven Williams
Rick Wilson
Terri Wilson
Brett Wise
Jennifer Witt
Kristin Wood
Robin Woolen
Jeffrey Yawman
Andrew Ysasi
Ryan Zilm

Application deadlines: Nov. 14, 2015 and March 28, 2016.

Register today at ***www.arma.org/igp.***

PRIVACY

Google's Right-to-Be-Forgotten Appeal Rejected

The French data regulator has rejected Google's appeal against the global enforcement of "right to be forgotten" (RTBF) removals. RTBF allows individuals to request that information about them be erased from Internet records.

In May, the Commission Nationale de l'Informatique et des Libertés (CNIL) ordered Google to apply RTBF removals not only to the company's European domains such as *google.co.uk* or *google.fr*, but also to the search engine's global domain *google.com*.

Google filed an informal appeal in July to the president of CNIL, Isabelle Falque-Pierrotin, arguing that it would impede the public's right to information, would be a form of censorship, and would have a chilling effect on the Internet.

Falque-Pierrotin rejected the appeal, stating that once a delisting has been accepted under the RTBF ruling it must be applied across all extensions of the search engine and that not doing so allows the ruling to be easily circumvented, the *Guardian* reported.

CNIL said in a statement: "Contrary to what Google has stated, this decision does not show any willingness on the part of the CNIL to apply French law extraterritorially. It simply requests full observance of European legislation by non-European players offering their services in Europe."

The rejection means that Google now must comply with the order and remove tens of thousands of delistings from its *google.com* and other non-European domains for named searches.

Google cannot appeal the order at this stage under French law.

According to the *Guardian*, CNIL will likely begin to apply sanctions, including the possibility of a €300,000 ($340,000 U.S.) fine against Google, if it refuses to comply with the order. Under incoming European regulation, the fine could increase to between 2% and 5% of Google's global operating costs.

Google can then appeal the decision and the fine with the supreme court for administrative justice, the Conseil d'Etat.

A Google spokesman said: "As a matter of principle, we respectfully disagree with the idea that one national data protection authority can assert global authority to control the content that people can access around the world."

EMR

Are Electronic Medical Records Worth the Costs?

Electronic medical records were supposed to be at least a partial cure for healthcare inefficiencies and expense in the United States, enabling better record coordination for individuals and thus better care, as well as reigning in the trillions of dollars spent on health care each year.

However, implementing and using such records systems have been neither inexpensive nor without challenges. While the costs for many providers have been largely offset by the federal incentive payments, the evidence thus far seems to suggest that most providers are not yet seeing the payoff, according to a recent report from the American Action Forum (AAF).

The report found that only a few years after passage of the HITECH Act, adoption has significantly increased and much more data is being collected and reported digitally. An estimated 78% of office-based physicians were using some form of EMR system in 2013, and 48% were using a qualified "basic" system. Among non-federal acute care hospitals, 76% were using a "basic" system by 2014.

However, implementing an EMR system could cost a single physician approximately $163,765, according to the report. The AAF found that as of May 2015, the Centers for Medicare and Medicaid Services (CMS) had paid more than $30 billion in financial incentives to more than 468,000 Medicare and Medicaid providers for implementing EMR systems.

In addition, with a majority of Americans now having at least one and likely multiple EMRs generated on their behalf, data breaches and security threats are becoming more common. Nearly 135 million healthcare records have been compromised in more than 1,200 separate data breaches since October 2009, and AAF estimates the total cost of these breaches to be $50.6 billion in less than 6 years.

BYOD

10 Smart Strategies for BYOD Success

Far from just a trend, the bring your own device (BYOD) policy is quickly becoming more entrenched in the corporate world. Gartner Inc. predicts that by 2017 half of all employers will require their employees to supply their own devices for work purposes. Businesses have known for a while now that a BYOD model delivers several benefits, including improved user productivity, engagement, and satisfaction, as well as the possibility of cost savings.

A recently released CIO white paper, "10 Best Practices for Implementing a Successful BYOD Program," instructs companies who want to adopt a BYOD program to:

1. **Define program objectives and get executive buy-in.** Ensure that executive sponsors support the program objectives and will provide the budget and people resources necessary for program success.
2. **Determine eligible BYOD users.** BYOD no longer needs to be the exclusive privilege of the highly mobile. Every employee can benefit from the increased productivity, flexibility, and efficiency that mobility offers.
3. **Define acceptable use policy.** A well-defined policy should not constrain the use of any personal data, apps, or other content because the users own their devices.
4. **Create a communication plan.** To ensure policy compliance, you should implement simple, repeated end-user communication and training.
5. **Identify a pilot program.** CIO recommends using a pilot program for the initial roll out to gain insight into potential barriers to adoption, incremental training, and IT readiness, and to help assess whether the benefits are aligned with its defined goals.
6. **Decide which devices to allow.** Your BYOD program should include a recommended list of devices that will work best with users' job profiles and the apps they will be using.
7. **Negotiate mobile service rates with carriers.** Before your employees start to rely on their mobile devices for work, negotiate favorable rates with your preferred mobile carriers – for both voice and data plans – to make the transition to BYOD at least cost-neutral to employees.
8. **Define your end user support model.** To manage support costs in a BYOD deployment, determine whether you have the right staff and expertise on hand to support the growing number of users.
9. **Define your mobile app strategy.** To get the maximum bang for your BYOD buck, you need to provide your users the right set of corporate apps to help them stay productive wherever they are. The apps, which should be defined by business objectives and user profiles, may include basic ones, such as e-mail, file sharing, or a secure browser, or a suite of custom apps that enables powerful mobile workflows.
10. **Monitor program usage.** Define how you'll measure success for your BYOD program and how it will align with your business goals. **END**

Policies and Processes for **Protecting Information**

Though written primarily for a law firm audience, this article provides all organizations with practical advice about protecting personal, confidential, and trade secret information. It is an excerpt from *Confidentiality, Privacy, and Information Security: A Primer for Law Firm Records and Information Governance Professionals*, written by Beth Chiaiese, CRM, with Lee. R. Nem-chek, IGP, CRM, editor for the Information Governance in the Legal Environment series.

Beth Chiaiese, CRM

Best practice dictates that law firms must use a variety of tools and techniques to secure Covered Information in their possession. [*Editor's note:* Throughout this excerpt, the term "Covered Information" refers to all private or confidential law firm information that is regulated by ethics rules, data privacy and security laws, or common law.] These include implementing a strong security infrastructure for the firm's network, developing robust policies, using specific procedures and systems designed to minimize the risks of a data loss, and auditing to identify gaps in compliance with the established policies and procedures. [This excerpt focuses on policies and processes.]

Policies

A significant component of a law firm's IG [information governance] framework consists of guidance on information confidentiality, privacy, and security. Some IG policies relate narrowly to information security. Others include statements related to the protection of Covered Information but also cover topics such as records management, legal holds, and accepting and releasing client information.

Regardless of the specific objective of a policy, the underlying message regarding information security should be that the firm expects all personnel to manage information in ways that support compliance with professional duties of confidentiality, relevant regulations that govern the use of PI, and requirements to protect intellectual property and trade secrets.

The section below discusses specific policies that a firm can adopt within an overall IG policy framework to strengthen its information security program. Many firms require new personnel to acknowledge receipt, read, and agree to the provisions of such policies on their first day of employment, and they may also require annual re-certification by all personnel.

Confidentiality Policy

A statement of the firm's requirements to maintain the confidentiality of client and firm information is a threshold compliance policy in most law firms. Many law firm liability insurance providers strongly recommend that firms enforce this type of policy. Firms generally place so much importance on maintaining confidentiality that violations can result in severe discipline, including dismissal from employment. Recommended policy elements include:

- Definition of confidential information
- Scope statement defining the policy as covering all client and business confidential information, regardless of format, media, storage location, or method of transmission
- Statement regarding consequences of non-compliance
- Specific requirements to protect oral, written, electronic, and physical confidential information
- Permitted use, access, and disclosure of confidential information
- Transmittal protocols for confidential information, including any requirements to encrypt data in motion
- Guidelines in the event of the inadvertent disclosure of confidential information
- Securing confidential information from guests
- Retention and disposal of confidential information

Information Security Policy

A firm's information security policy should set forth expectations regarding how firm personnel must secure Covered Information. Some firms may also wish to excerpt a brief statement of their expectations regarding information security that can be given to clients and third parties.

The information security policy is a good vehicle to include requirements for password control, although some firms create separate password policies. In addition, some firms create broader "technology acceptable use" policies that incorporate information security requirements.

Recommended elements for general information security policies include:

- Password and authentication requirements
- Securing confidential matters and matters under ethics walls
- Securing confidential documents
- Encrypting information in transit
- Appropriate use of portable devices, including device encryption
- Rules for participation in the firm's BYOD program
- Permissible uses of the Internet
- Permissible use of social media and networking sites
- Use of public cloud storage services
- Securing physical information

BYOD Policies

While policies governing participation in a firm's BYOD program might be included in a general information

… the underlying message regarding information security should be that the firm expects all personnel to manage information in ways that support compliance…

security policy, best practice dictates that firms require program participants to sign a separate [BYOD] agreement, certifying that they understand the parameters of the program and their responsibilities, including a requirement to re-certify annually. Other recommended elements of the agreement include:

- Program definition and scope
- Eligibility statement
- Provision detailing the types of devices that are and are not covered by the program
- Requirements regarding virus protection and encryption
- Requirements regarding temporary and permanent storage of client and firm information
- Description of how the firm ensures connectivity to firm systems
- Requirements that the participant is responsible for software and hardware maintenance
- Financial reimbursement processes

Policy on Managing Personal Information

A policy providing guidance on the management of PI [personal information] should include the following elements:

- Definition of PI
- Approved locations for storing PI
- Approved methods of securing PI
- Permitted access, use, and disclosure of PI
- Notification of a PI breach
- Requirements for use of a BAA [business associate agreement]
- Release or transmission of PI
- Retention of PI
- Destruction of PI

Social Media and Networking Policy

Lawyers and non-lawyer firm personnel alike engage in social networking both professionally and personally. Law firms have an interest in ensuring that such interactions comply with professional duties, regulatory requirements, and firm policies. Although there are personal privacy considerations that prohibit firms from dictating how employees use social media in their personal lives, professional obligations covering the behavior of lawyers are in force at all times. This means that lawyers cannot identify their clients or divulge any confidential client information while using social media.

Social networking policies typically include provisions dealing with a variety of professional responsibility and legal issues that extend beyond confidentiality and security. These issues include (1) prohibitions against providing legal advice while using social media; (2) using disclaimers to advise readers not to interpret content as legal advice; (3) complying with copyright and trademark laws; (4) complying with lawyer advertising rules; (5) posting content in an objective and factual manner; (6) refraining from expressing defamatory opinions about individuals; and (7) not using social networking to seek input on candidates for firm employment.

Certain elements of such policies touch directly on privacy and confidentiality, including:

- Prohibitions against discussing firm business and professional relationships with clients, judges, and other lawyers
- Prohibitions against using social media to discuss legal matters with clients
- Requirements to be transparent and not to use misleading language or pretext
- Requirements to protect the privacy of others

Processes and Systems

The ability of firm personnel to comply with mandated policies depends on a number of strong processes, systems, and associated tools. This monograph does not cover all of these in depth, but several significant components of law firm information security programs are discussed below.

…best practice dictates that firms require program participants to sign a separate [BYOD] agreement, certifying that they understand the parameters of the program and their responsibilities…

Approved Repositories

As noted earlier, a contributing factor to data loss in law firms is the dispersion of Covered Information across multiple repositories. Increasingly, law firms attempt to aggregate information into approved locations in order to better manage the information from a security standpoint. Each approved repository in the firm should share certain common characteristics. Approved recordkeeping repositories in a law firm must be able to:

- Classify information by a common identifier, such as a client/matter number
- Preserve information for a prescribed period in the event of a lawsuit, claim, or investigation, or as part of a record "declaration" process (in order to prevent further modification)
- Secure information from access by unauthorized individuals
- Permanently delete/destroy information in accordance with policy,

Privacy+

Look for it. Ask for it. Expect it.

PRISM International (Professional Records and Information Services Management) was established in 1980 as the trade association for the commercial information management industry. The vision of PRISM is to be the global advocate for safeguarding physical and digital information by serving organizations who provide information management services.

In 2012 PRISM launched the Privacy+ certification program in order to allow offsite records and information management companies to clearly demonstrate their commitment to ensuring the privacy of information in their custody.

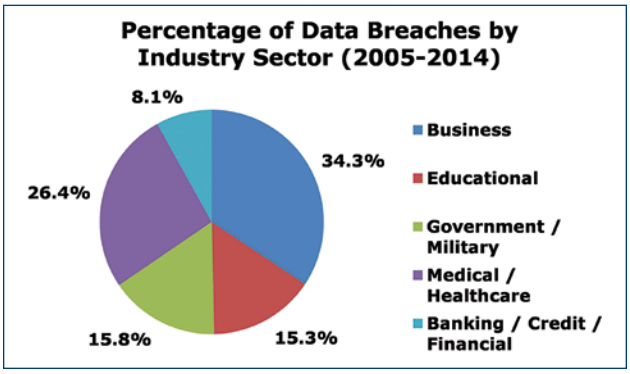


Chart provided by Identity Theft Resource Center (ITRC) and sponsored by IDT911™

The program was built using recognized industry laws and standards, including:

- Health Insurance Portability and Accountability Act (HIPAA)
- HIPAA Privacy Rule Payment Card Industry Data Security Standard (PCI DSS)
- The Personal Information Protection and Electronic Documents Act (PIPEDA)
- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes-Oxley Act (SOX)
- Federal Trade Commission (FTC) "Red Flags Rules"
- American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization
- Family Educational Rights and Privacy Act (FERPA)
- Fair and Accurate Credit Transaction Act (FACTA)
- State information security laws including 201 CMR 17.00
- European Data Protection Directive

PRISM knows your information is priceless.
Using a Privacy+ certified company should give you peace of mind and confidence that your information is being protected against unauthorized access and data breaches, and that your chosen records and information storage partner is using best practices.

To achieve Privacy+ certified status, records and information storage companies must establish and have a third-party independent audit of internal controls designed to meet a specific set of control objectives designed to preserve information privacy. The control objectives have been established by PRISM International and must be met by all Privacy+ participants.

The number of data breaches in the United States has grown exponentially in recent years. As you search for a company to help with your off-site records management and storage, look for the Privacy+ logo, ask for it in your RFPs, and expect it from those trusted with your information management storage.

To find a Privacy+ Certified records and information management company, or to find out more information about the Privacy+ program, visit ***www.prismintl.org*** or call **1.800.336.9793**.

agreement, or court order

Firms can identify approved and non-approved repositories using these characteristics as defining guidelines. For example, most DMS [document management system] products can function as approved repositories, as can a physical file folder. E-mail systems, on the other hand, cannot, because, although e-mail boxes are private to the individual user and e-mail can be permanently destroyed, e-mail systems per se do not support classification or preservation.

- Integration with multiple firm information systems—e.g., DMS, RMS [records management system], docket systems, and time-entry systems—thus allowing consistent security across systems
- Alerts to system administrators that a non-authorized individual is trying to gain access to a confidential matter
- Monitoring of the time-keeping system for individuals who have billed time to confidential matters, and either alerting the system administrator if the individual is also working on the opposite side of the wall or automatically adding the individual to the wall
- Allowing the system administrator to grant end-user capability to manage access; for example, if all matters for a client are considered confidential, it may be helpful for the relationship partner's assistant to manage access. Alternatively, the office of the General Counsel may want to manage security for all firm legal matters.
- Restricting or allowing access by group; for example, based on the area of law code assigned to a matter (e.g., health care or employee benefits), it is possible to grant access to matters containing PHI [personal health information] to only a defined group of lawyers and staff. Similarly, it is possible to create a group of foreign nationals and restrict them from accessing matters that contain information covered by ITAR [The International Traffic in Arms Regulations] / EAR [Export Administration Regulations].
- Reporting on all confidentiality walls in the firm, as well as the walls on which individual lawyers or staff are named
- Auditing capability to monitor spikes in downloading and e-mailing activity

As noted above, confidentiality software assists users to comply with the requirements of certain DSP [data security and privacy] laws. To facilitate this assistance, some firms ask at matter intake if the new matter requires the receipt of PI or PHI. If yes, a confidentiality wall can be created.

… most DMS [document management system] products can function as approved repositories, as can a physical file folder. E-mail systems, on the other hand, cannot …

Securing Matters from Unauthorized Access

Software is available that secures all content related to one or more matters for a client. Matter level security can be configured to be either exclusionary or inclusionary. Exclusionary security applies when specific individuals are excluded from access. Typically, this occurs when an ethics wall is required to screen lawyers or others who have confidential information related to the client or matter that could result in the firm's disqualification. [States vary in their recognition of ethics walls as effective screens against conflicts imputation. Records managers and IG professionals are encouraged to consult with their firm's professional responsibility lawyer regarding the appropriate use of ethics walls.]

Inclusionary security is applied when *only* specific individuals are permitted access to the subject information. This generally occurs when the matter itself is confidential, such as merger and acquisition matters, criminal matters, family law, and other highly personal client matters.

Confidentiality software should include the following functionality:

Document Level Security

DMS systems include functionality that defines access parameters at the document level.

Defining Access Rights – In general, law firms maintain "optimistic" or "open" DMS environments. This means that the default security setting for documents is public, i.e., all documents are accessible by everyone in the firm. Document authors can change this setting to "read only," which allows everyone to view the document, but only the author and other approved users are permitted to modify it.

Alternatively, authors can change the setting to "private," which means that no one other than the author and other approved users can view and/or modify the document. Because this level of security is controlled by the end user, it requires awareness, skill, and accountability on the part of all firm personnel. Thus, it is a significant component of the firm's security training program.

Tagging by Document Type – Most DMS applications allow system administrators to configure specific document types to default as private to the author, which makes it easier

to set security at the document level. The author can grant access to others as appropriate. Examples include the document types Personnel, Personal, and Firm Management. An alternate approach is to create a document type called PI or PHI, which satisfies the requirements of certain DSP laws that require organizations in possession of PI to take affirmative steps to control access to it.

Encryption

Encryption is accomplished by using software to apply a complex series of mathematical algorithms on data to convert it to cipher text. The more complex the algorithm, the more difficult it is to decrypt the data. Although a complete technical description of encryption is beyond the scope of this monograph, law firm records and IG professionals must understand certain key concepts about encryption.

Encrypting Data in Transit – Individual data sets (documents or e-mails) can be encrypted at the time of transmission. In such instances, software applied by the sender translates plain text into cipher text. The recipient needs a key (i.e., a password) to decrypt the data to make it readable. Users must encrypt PI before e-mailing or otherwise transmitting it electronically. Passwords should always be communicated orally; do not send them in plain text via e-mail or facsimile.

Encrypting Data at Rest – Encryption can be applied to an entire hard drive, and a password is needed to decrypt the drive. The advantage of this approach is that if a strong password is used, it is almost impossible for an unauthorized user to access data on the hard drive. The disadvantage is that if the password is broken, the entire hard drive is decrypted when the password is entered. This consequence further supports the necessity to create complex, hard to crack passwords.

Many firms automatically encrypt the hard drives of firm-owned laptops. Increasingly, they are also requiring users to encrypt the hard drives of personal devices, although several factors constrain such policies:

- *Some devices do not support encryption.* Firms can address this issue by specifying the types of devices that can be encrypted and giving individuals a time period within which to migrate. In addition, the firm's BYOD policy can limit the types of devices for which the firm will provide reimbursement to only those that support encryption.
- *Firms have limited capabilities to monitor personal devices.* Because certain applications can be accessed directly over the Internet, or because individuals might e-mail documents to personal e-mail accounts or store them on portable media such as thumb drives, firms cannot entirely con-

trol whether Covered Information is stored on encrypted devices.

- *Installing encryption software can be technically challenging*. On certain devices, encrypting the hard drive is as simple as enabling a feature in the operating system or securing it with a password. Other devices require the installation of encryption software. Law firms that mandate encryption of personal devices should be prepared to assist individuals who do not have the skill to do it on their own.

conditions exist, do not examine or review the information until the client's intent has been documented, to avoid inadvertently accessing privileged or otherwise confidential information.

- Examine any portable media on which electronic information resides to confirm that it is not infected with a virus or malware.
- Load electronic data onto a review site that is not connected to the network, allowing further examination to identify viruses. In addition, this allows staff managing the transfer to organize and aggregate data by appropriate client and matter and provides a location for lawyers to access information while the transfer proceeds. Finally, it allows file transfer staff an opportunity to further examine data to remove records for clients who have not engaged the firm and inadvertently transmitted trade secret information from the former firm.
- After data has been thoroughly examined, client engagement has been confirmed, and client/matter numbers have been issued, the data can be loaded into firm systems on the network.

Release of Information – When information is released from the firm, take precautions to avoid the inadvertent disclosure of confidential client information, a breach of PI, or the potential release of firm trade secrets:

- Release information only after an appropriate analysis to determine the firm's potential need to review the file to remove records necessary to defend the firm. This analysis should be done by a loss prevention or professional responsibility lawyer or by the firm's General Counsel.
- Follow firm guidelines for the removal of firm trade secret information from the file.
- Encrypt any PI or PHI before transmission to the receiving party.
- Appropriately secure physical files prior to shipping.
- Use an FTP site or other secured means to transmit electronic records. If using portable media, such as a CD or DVD, confirm that it is virus-free.
- If shipping physical files or portable media, use a courier or other traceable method.

Examine any portable media on which electronic information resides to confirm that it is not infected with a virus or malware.

File Transfer Protocols

As noted earlier, movement of confidential client information has become an operationalized component of RIM and IG programs. Whereas law firms have had processes to manage physical file transfers for many years, these processes must now include the ingestion or release of significant amounts of electronic information. File transfer methods were explored in depth in the second monograph of this series [*Lawyer and Matter Mobility*]. With respect to information security, however, the following additional considerations apply:

Ingestion of Information – When receiving physical and electronic records from an outside source, such as a client or former law firm, confirm the following:

- The current firm has been engaged by the client and is thus permitted to have the information. This can be accomplished by receiving an e-mail confirmation from the client, by obtaining a copy of the written consent from the former firm to release records to the current firm, or by executing an engagement agreement with the client. If none of these

Collaboration Systems

Lawyers are increasingly downloading inexpensive or free solutions from the Internet to share information and collaborate with clients and other parties. To combat this risky behavior, firms are either developing internal solutions that provide the same functionality within the firm's security architecture, or they are implementing commercial solutions that meet the firm's security requirements.

Mobile Device Management (MDM)

A number of services impose centralized control over mobile devices that connect to firm networks. Common features of MDM systems include [according to Sharon D. Nelson, David G. Ries, and John W. Simek in *Locked Down: Information Security for Law Firms]*:

- *Inventory control* – Once a device, such as a smartphone, tablet, or laptop, connects to firm networks, the MDM system uses its IP address to track it, ensuring that

users are relying on devices that support firm guidelines regarding encryption. Inventory control also allows the firm to monitor devices that have been inactive for a specified period so they can be wiped of firm data and removed from the network.

- *Connectivity management* – Examples include deploying secured virtual private networks (VPN) or wireless networks that allow users to gain remote entry to firm systems.
- *Password management* – This includes protocols to require regular password changes and system authentication.
- *Remote wiping of lost or stolen devices* – Although remote wiping is a critical aspect of mitigating data breach risks, it also endangers personal data on the device, as noted earlier. In addition, the firm's ability to wipe the device depends on a user's notification that his device was lost or stolen.
- *Timing out* – After periods of inactivity, password re-entry is required.
- *Remote installation* – Applications and updates can be installed wherever the device is being used.

Removal or Restriction of Administrative Rights

Firms can restrict the ability of users to access certain administrative rights in the operating systems of their networks, including the ability to install software and devices. Although partners may push back heavily on this restriction, IT and IG leaders should not back down. Not only does the restriction of administrative rights ensure that only firm-approved systems are in place, it can prevent the inadvertent entry of viruses and other malware into the firm's environment, either through direct download by firm personnel or by social engineering manipulation.

Secure Disposal

Many DSP laws require secure methods of records disposal. In addition, secure disposal prevents leaking other types of Covered Information, including confidential client PI and trade secrets. Records managers are well-acquainted with secure methods of disposing of hard copy records, including cross-cut shredding and pulping. However, securely disposing of electronic records is more complex. Pressing the Delete key removes the pointers that allow data to be accessed, but it does not expunge data from the hard drive on which it is written.

Acceptable methods to dispose of electronic information include the following [according to Nelson, Ries, and Simek]:

- Physically destroying the drive or portable media on which the data is written by disintegration, pulverization, incineration, or shredding
- Degaussing, "a magnetic process by which magnetic media are erased (returned to zero) by applying a reverse magnetic field using a degausser"
- Overwriting the media with a disk-wiping program. Such applications overwrite each block or segment on the disk several times to obliterate the data.
- Encryption. If a device is securely encrypted, the data is not accessible unless it is unlocked with a password or key. If the device has strong encryption it can be disposed of using one of the methods listed above without otherwise sanitizing the device.

Culture

As with the IG program as a whole, the success of any law firm's information security program is dependent on building a culture of awareness, accountability, and compliance. Support from firm leadership and ongoing training are important contributing factors to making information security an accepted and followed protocol throughout the law firm. **END**

Beth Chiaiese, CRM, is the director of professional responsibility & compliance for Foley & Lardner LLP. She can be contacted at bchiaiese@foley.com. *See her bio on page 47.*

The Principles, IG Maturity Model: Tools for Professional Growth

Julie Gable, CRM, CDIA, FAI

In a field of endeavor where change is incessant and uncertainty is constant, the Principles and the IGMM are signposts that point out current position, future direction, and the means for getting the RIM program – and the professional – from one place to the next.

For the last three years, articles in this space have discussed the value of the Generally Accepted Recordkeeping Principles® (Principles) and the Information Governance Maturity Model (IGMM) to the enterprise. Emphasis has been on how these tools benefit organizations by providing a framework on which to build an information governance (IG) program and an objective set of criteria for measuring progress toward its maturity.

Yet the Principles remain abstract ideals until they are put into practice. They tell *what* good governance comprises, but they do not offer recipes for *how* to make it a reality. The hard work of translating the Principles into practice rests with an important, but often overlooked, element in program success: the records and information management (RIM) professional.

While RIM professionals have embraced the Principles and IGMM as tools they can employ to help their organizations attain excellence, they may not have realized they can also be used to their personal advantage. In addition to serving as the basis upon which to build, measure, and judge RIM and IG programs, the Principles and IGMM

can also be a means by which RIM professionals can grow, achieve, and advance their careers.

The Tools' Explicit Uses

The Principles and the IGMM have both explicit and tacit aspects. *Explicit* uses are those for which the tools were developed. For example, the Principles of Accountability, Compliance, and Transparency show how a program should operate, and the Principles of Availability, Integrity, Protection, Retention, and Disposition show what a program should include. Taken together, these function as a roadmap for building or revising a RIM program; this is their *explicit* use.

The IGMM's *explicit* use is as a maturity meter, defining characteristics associated with sub-standard, developmental, essential, proactive, and transformational IG program levels. The IGMM tells what must be in place at each level, and its explicit use is as an assessment tool to take stock of a program and determine what it lacks. Once these deficiencies are clear, RIM professionals can prioritize them according to the risk they pose and formulate systematic plans to address them, ensuring that resources and budgets are used on the higher priorities. In this way, the IG program will ripen over time to its full potential.

The Tools' Tacit Uses

What is not immediately apparent on the surface is that the Principles and the IGMM also have secondary, *tacit* aspects. In the knowledge management discipline, explicit knowledge is factual and tacit knowledge is experiential. While it is easy to see how the tools' primary uses benefit the IG program, it may not be quite as easy to see how their tacit or secondary uses benefit RIM professionals personally.

Enhancing Communication

The Principles and the IGMM are useful as communication tools, providing simple, standard, descriptions of the elements of good RIM and IG. They can be shared with everyone in the organization as the fundamental concepts that will help get people with diverse ideas about IG on the same page. The Principles provide a brief way to say, "This is what we are doing and why," and they are useful to RIM professionals in explaining their own role within the organization, as well as in outlining the expectations for others who serve in program leadership, accountability, advisory, or technical capacities. They provide the narrative framework in which to tell the story of the IG program to insiders and outsiders alike.

Establishing Credibility

While clear communication is always a mark of excellence, the underlying reality is that the Principles and the IGMM confer credibility on RIM professionals. These tools, because they are based on international standards and best practices, can be used as a basis of comparison for any proposed IG methods or processes. They are a means to keep discussion, assessment, comment, and criticism on an objective plane, beyond the realm of personalities or politics.

The Principles and the IGMM are useful as communication tools, providing simple, standard, descriptions of the elements of good RIM and IG.

Improving Collaboration

This is invaluable to RIM professionals participating on collaborative teams charged with evaluating proposed solutions, systems, and software. The Principles and the IGMM provide objective justification for why RIM professionals must sometimes point out the trade-offs and deficiencies inherent in proffered solutions. They offer a codified way for RIM professionals to assert their viewpoint, a subtle but effective background statement of "Here's where I'm coming from and why I must comment as I do."

They remove the taint of mere opinion from criticism, and rather than speak in general terms, the Principles allow RIM professionals to be specific in showing where a proposed strategy is strong or weak. By doing so, the tools remove the tendency to label RIM objections as being obstructionist or negative. The Principles make clear that the RIM professional is focused on specific concerns for good reasons.

Identifying Areas for Compromise

Credibility bolsters the RIM professional's role as an internal consultant who provides unbiased advice and guidance based on standard and measurable criteria. But as most consultants know, their sound judgment and caution about risks may be ignored in favor of profit or other motives. Just as the Principles are useful for collaboration, they can also show where compromise is needed. For example, cloud storage is not optimal from the standpoint of the Principles of Retention and Disposition, and it may raise serious concerns for Protection as well, but it may be the organization's best hope for reducing exponential growth in server costs and bolster much-needed profit margins.

Highlighting Good Performance

Just as the Principles provide a narrative framework

for communicating about the necessary elements of IG, the IGMM provides a cohesive way to talk about RIM professionals' accomplishments. Information management work can resemble a patchwork of small projects without many connecting threads.

What results from the use of the Principles and the IGMM tools testifies to the skill and creativity of the professionals who use them.

For example, separate projects to develop uniform metadata elements, standardize protection levels, and streamline response to information requests can seem insignificant when viewed as separate items. But placed in the context of the IGMM, it is easy to see that the three projects strengthen Integrity, Protection, and Availability, three areas that can affect the organization's audits, how it interacts with its legion of contract workers, and how competent, efficient, and effective it appears to the outside world.

In short, the IGMM helps put the work into perspective as being part of a whole – not just random little pieces, but tiles that are part of an intentional mosaic. The IGMM elevates each project's value and worth because it shows where it fits in the overall enterprise IG effort, and in doing so it highlights the value and worth of the person who conceives, manages, and delivers the projects' results.

Evaluating Career Opportunities

Aside from assessing the internal IG program, the Principles and the IGMM have demonstrated great versatility as tools for examining the programs of acquired companies (see the Principles article in the May/June 2014 *Information Management*), evaluating the trade-offs inherent in outsourcing agreements (March/April 2015 *IM*), and understanding the maturity levels required for successful technology implementation (May/June 2015 *IM*). For RIM professionals, there is yet another possible use of these tools.

Most successful RIM professionals are offered other opportunities in the course of their careers, from within and outside of their organizations. There are many aspects to consider when one evaluates a new position; interview questions based on the IGMM's specific levels could help the applicant find out what is in place and what is needed – a good way to see what may be in store for the person who accepts the position.

More important, where an organization is in its IG maturity also conveys an impression of how the culture regards IG. How much time, money, and effort has it invested? Is there a stakeholder committee that reviews governance issues (Accountability – Level 4)? Has the organization comprehensively identified key compliance laws and regulations (Compliance – Level 3)? Are there written policies and a training program based on them (Transparency – Level 3)?

The answers to questions based on the IGMM can help RIM professionals decide whether their skills and personal objectives are a match for what the opportunity requires. Although it is nice to walk into a Level 4 situation, there is more challenge and more room for growth in a Level 2. Besides, a Level 4 may be quite complacent, while a level 2 may be hungry for change. It depends on what you want.

Prompting Lifelong Learning

There is so much to learn about IG that it can seem overwhelming. Perhaps the greatest value of the Principles and the IGMM is what RIM professionals learn by working with them. Although they are not meant as guidance for RIM education, the concepts engendered in the Principles and the work of putting them into practice comprise a learning experience that never ends.

Consider that working on the Principle of Integrity will lead through topics such as audit trails and the reliability of electronic systems and their infrastructure, or that the Principle of Availability will require knowing more about topics as diverse as privacy, proprietary information, security clearances, and information leaks. It is true on-the-job training, and what is learned remains because it is that unforgettable combination of theory and practice.

Furthermore, this is knowledge that is transferable from one situation to another, whether the career path is a straightforward trajectory through a corporate hierarchy or a staggered path through private sector companies, non-profits, consulting, or government.

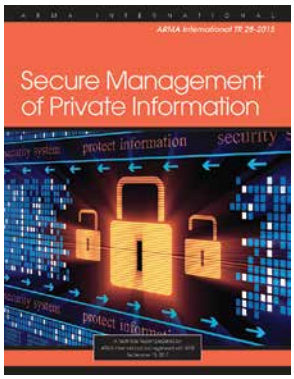
Signposts for Program, Career Growth

In a world where change, collaboration, and compromise have become the watchwords of information management, the most important element in program success remains the RIM professional.

What results from the use of the Principles and the IGMM tools testifies to the skill and creativity of the professionals who use them. In a field of endeavor where change is incessant and uncertainty is constant, the Principles and the IGMM are signposts that point out current position, future direction, and the means for getting the program – and yourself – from one place to the next. **END**

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

Resources for Advancing Your Career

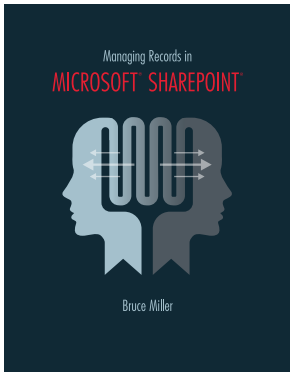


NEW!

Secure Management of Private Information (ARMA International TR 28-2015)

This technical report identifies the risks associated with private information, provides policies, tools, and techniques for mitigating them, and tells how to audit for compliance with privacy policies.

A4968 **$60.00** Professional members: **$40.00**
V4968 PDF **$55.00** Professional members: **$35.00**

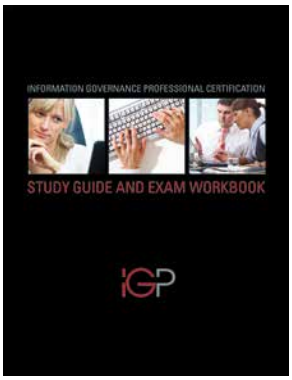


NEW!

Managing Records in Microsoft® SharePoint®

This book examines SharePoint's® native recordkeeping capability's shortcomings and explains how to optimally deploy third-party recordkeeping technology to overcome them.

A5024 **$85.00** Professional members: **$60.00**
V5025 PDF **$80.00** Professional members: **$55.00**



Information Governance Professional Certification: Study Guide and Exam Workbook

This PDF study guide will help you develop and execute your preparation plan for taking the IGP certification exam. It provides a self-assessment tool that will help you identify content areas where you need to focus your study and suggested resources to help you learn more about each of those areas.

V5028 PDF **$75.00** Professional members: **$50.00**

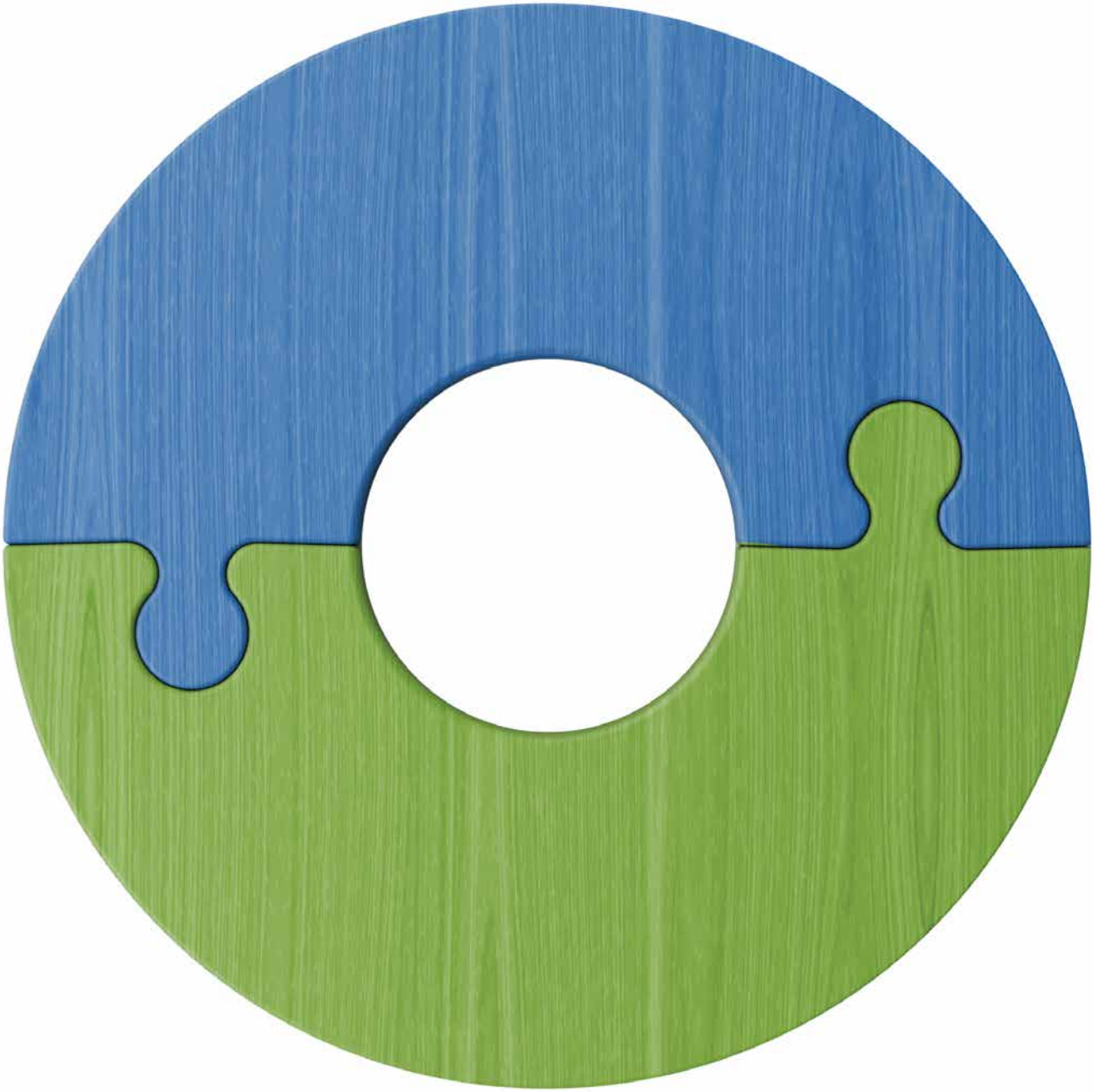
Order online today! **ARMA INTERNATIONAL BOOKSTORE**

www.arma.org/bookstore

How to Combine **RIM Programs** After a Merger

Blake Richardson, CRM, CIP

From the moment two companies publicly announce a merger, their operational wheels begin turning. This article identifies issues that may not be discussed before the merger is completed and provides advice about the issues that must be discussed post-merger.



Mergers and acquisitions (M&A) are a potential reality for organizations regardless of their industry, revenue, geography, or size. They occur for a variety of reasons, such as gaining economies of scale, increasing operational synergies, reducing tax liabilities, and pre-empting competition.

Whatever the reason may be, one constant exists: an M&A will have an impact on the combined organization. This article addresses the impacts to records and information management (RIM) in a newly merged environment.

Merging Parties' Discussions

Pre-Merger

From the moment two companies publicly announce a merger, their operational wheels begin turning, though there are regulatory limitations on what the two organizations can discuss, share, and plan until the merger has been approved. The limitations exist to prevent "gun-jumping," which according to attorney Richard Liebsekind, is the term the Antitrust Division of the U.S. Department of Justice (DoJ) and the Federal Trade Commission (FTC) use to refer to a "variety of actions that merging parties might enter into prior to closing to facilitate the merger and expedite the integration of the companies."

In the presentation "Gun-jumping: Antitrust Issues Before Closing the Merger," Liebsekind made to the ABA Section of Business Law, Antitrust Committee ABA Annual Meeting in San Francisco clear examples of gun-jumping provided by the DoJ and the FTC are coordinating prices and terms to be offered to customers or allocating customers for sales to be made *prior* to the merger and coordinating negotiations with customers for sales to be made *after* the merger.

"The government's position," Liebsekind said, "is that firms must remain competitors until closing, and cannot lessen competition between them in order to facilitate a merger that has not been consummated."

Therefore, merging companies conducting pre-closing due diligence and planning activities need to know that antitrust agencies might view their activities as violations of federal law.

In most cases there are operational matters that *can* be discussed between the organizations during this phase of the merger process. RIM professionals should consult with their legal or compliance department to determine what can and cannot be discussed with their counterparts in the other organization.

RIM matters that may be allowed for discussion in the pre-merger phase include:

- Record retention schedule formats
- Offsite storage vendors used (but not contractual terms or pricing)
- Number of employees (but not pay rates)
- Technology and how it is used (but not related pricing or maintenance costs)
- Reporting structure
- Approach to disposition
- Geographical operating locations and related challenges

Conducting pre-merger discussions with the other organization's RIM manager allows for early insight into the operational differences between the RIM programs and facilitates additional Q&A and planning once the merger has been approved.

> Once a merger has been approved, the combined organization is permitted to strategically and tactically plan and execute.

Post-Merger

Once a merger has been approved, the combined organization is permitted to strategically and tactically plan and execute. RIM professionals can now discuss in detail matters such as offsite vendor contractual terms, conditions and pricing, employee responsibilities and pay rates, policies and procedures, disposition processes, legal holds, and technology.

The following sections address specific issues to consider when merging RIM environments.

Storage of Physical Records

A merged RIM environment commonly has contractual relationships with multiple offsite record storage vendors, or in some cases both organizations use the same vendor but have different terms, conditions, and pricing. Sometimes one or both organizations manage record storage and related activities in-house instead.

Multiple Vendors Used

If multiple offsite storage vendors are used, the RIM manager of each merged organization should discuss the following issues to determine the most efficient and economical course of action:

Contracts – Discuss the duration, terms, conditions, and pricing.

Volume of records in storage – Discuss the volumes of boxes, tapes, files (open-face shelving), and non-document content, such as physical evidence and items related to company history. Discuss whether the combined storage volume will result in a potential reduction in monthly storage fees.

Vendor issues – Discuss issues regarding customer service, vendor reliability, and operational procedures related to the vendor choice and vendor management.

Vendor service footprint – Discuss which vendors are best positioned to ser-

vice the merged organization's geographical areas of operation.

Vendor service offerings – Determine the business and RIM requirements of the merged organization. Consider such topics as shredding, document imaging, consulting, and using online technologies and software.

RIM managers have several offsite storage options to consider during this process. They might determine that multiple storage vendors best serve the interests of the merged organization. This option is often selected if one vendor is unable to service all of the merged organization's areas of operation.

While it is an option to assign all storage tasks to one current vendor, there are contractual and monetary issues to consider first. For example, if the records of company "A" are to be permanently withdrawn from its current storage vendor and moved to the vendor used by company "B," RIM must determine if penalties exist for early termination of the contract, what the costs will be for the permanent withdrawal of the records, and whether the vendor used by company "B" will absorb the transfer cost.

Same Vendor Used

If both companies use the same offsite storage vendor, the combined company should compare existing contracts to determine which has the more favorable terms, conditions, and pricing. Then, the merged company's RIM professionals should quantify its combined storage volume and negotiate a new contract that retains the most favorable terms and conditions and provides an even more favorable pricing structure based on the increased storage volume and transactional activity.

Onsite Records Storage Used

If one of the companies manages its records storage in-house, either onsite or at an offsite facility it owns or leases, the RIM managers of the combined company should determine if an in-house approach will meet its current and anticipated needs.

Can it support the requirements of the new organization, or will additional staff, space, and equipment be needed? Does the combined company have the appropriate technology, such as a physical records management system or warehouse software applications that help with shelving configuration, barcode tracking, and check-in/check-out?

In analyzing the costs related to in-house storage of their combined records, they should consider expenses for payroll (including benefits), equipment, space, utilities, and liability insurance to protect against such issues as accidents and workers' compensation claims.

RIM Employees

Merged organizations usually expect to realize increased operational efficiencies based on eliminating personnel "redundancies" – and this expectation certainly applies to RIM.

Once the merger is finalized, the RIM managers should evaluate the functions performed by each staff member to identify duplicate functions or processes. Duplicate functions and processes do not automatically warrant a staff reduction. In some cases, current staff levels should be maintained to support the increased size of the merged company and anticipated growth.

RIM managers should identify the need for advanced or specialized skill sets, who has those skills, and whether additional specialized personnel are needed.

RIM managers must also determine if certain functions will be discontinued – for example, transitioning from onsite to offsite records storage – and how the change will impact staffing. Ultimately, RIM managers must submit to senior management their staffing recommendations for the combined operation.

Record Retention Schedules

When companies merge, the likelihood exists that if both organizations have an established retention schedule, the format, record types, and retention periods may differ. For example, many companies use a detailed, departmental records retention schedule format, while some use a functional or big bucket approach.

The combined RIM team should compare the record retention schedules of the merged companies and document the differences related to formats, record types, and retention periods. If the schedules are fundamentally different, the RIM managers should discuss why they chose their approach, evaluate the RIM requirements in the combined environment, and determine which type of schedule better serves the merged organization.

Additionally, RIM managers should discuss and agree on the process for adding or modifying retention schedule components. For example, one company may have had a policy that all retention schedule modifications must be approved by their respective legal and tax departments, while the second company may not have required such approvals.

RIM managers must also determine if certain functions will be discontinued and how the change will impact staffing.

Technology

During pre-merger discussions it is appropriate for RIM managers to talk about the software they use for managing records and documents. Once the merger has been approved, they should have detailed discussions about how their technologies are used, deployed, administered, and supported.

During the discussions it is important to get answers to the following questions:

RIM Software

- Do the companies rely on a vendor's online portal or database for physical records management?
- Is content management performed with or without integrated electronic and physical records management functionality?
- Does the content management application integrate with other applications, such as SharePoint, PeopleSoft, SAP, or contract management?
- Has document management functionality, such as versioning, checking in/out, annotating, and redacting, been deployed with the content management application?

Application Activities

- Are they centralized? That is, are the majority of application activities performed by RIM?
- Are they decentralized? That is, are the majority of application activities performed by departmental end-users?
- Are they a hybrid, with just designated actions, such as applying legal holds, system administration, configuration, and disposition, performed by RIM?

Support, Maintenance, Scalability

- Does the application require heavy IT intervention, or can the majority of administration and configuration be performed by a RIM "power user?"
- What are the annual maintenance costs?
- What are the licensing models?
- What is the scalability in the combined environment?
- What is the date of the last upgrade and the current version?
- What deficiencies have been identified and what remediation efforts have taken place?

RIM should determine the RIM requirements in the merged environment and evaluate each aforementioned matter to determine what applications will best serve the combined organization and if any should be decommissioned or integrated. If applications are decommissioned, RIM managers and staff must work closely with IT to determine a migration or conversion strategy.

Legal Holds and Disposition

Upon approval of the merger, RIM managers should evaluate each company's approach to legal holds and disposition. This includes identifying who is responsible for communicating, applying, and rescinding legal holds. Some companies may assign the entire process to the legal department; others might depend on legal to initiate the communications and to send any periodic hold reminders while keeping RIM responsible for applying the holds in the records management application.

Organizations may differ on how disposition is administered. Some companies require a multi-stage approval process involving department heads, RIM managers, and tax and legal representatives before any records can be destroyed or deleted, while other companies may only require one level of approval, such as a department head or a legal representative.

In addition, after the retention period has expired, some companies allow low-risk, non-sensitive information to be destroyed without approval or deleted automatically from a content management application. RIM should understand how each company has approved and performed disposition and consult with the combined legal department to determine how disposition is to be administered in the combined environment.

Upon approval of the merger, RIM managers should evaluate each company's approach to legal holds and disposition.

An Opportunity

Although the thought of an impending merger can be a source of anxiety and uncertainty, the merging of two organizations' RIM functions can be rewarding and educational, as RIM professionals gain insight into how others manage records and information and the tools, policies, and procedures they use.

The process of merging programs also provides RIM professionals the opportunity to improve their analytical, technical, and constructive debating skills. Therefore, if you are in the process of a merger or your company someday announces one, take advantage of the opportunities, and use the approaches addressed in this article to help ensure that your combined RIM program is successful. **END**

Blake Richardson, CRM, CIP, is the information governance manager for a utility corporation. He can be contacted at titansfan100@gmail.com. *See his bio on page 47.*

Protecting Privacy in an IoT-Connected World

Michael S. Smith, Ph.D., IGP, CRM

To say we live in a connected world is an understatement in light of the growth of the *Internet of Things* (IoT), which is described in "Internet of Things Global Standards Initiative' by ITU – the United Nation's agency for information and communications technologies – as the network of physical objects embedded with electronics, software, sensors, and connectivity that enable them to collect and exchange data.

The Rise of IoT

Gartner says by the end of 2015, 4.9 billion connected things will be in use – up 30% from 2014. Three factors have played a significant role:

1. The development of the personal computer
2. Ubiquitous computing at low costs
3. Low-cost storage

A more recent business trend contributing to escalating data volumes is commonly referred to as SMAC, which involves using four major technologies – social, mobile, analytics, and the cloud – to engage with and collect data about customers, which is then analyzed and used to drive innovation, process improvements, and productivity.

IoT's Anticipated Growth

The number of IoT connections continues to grow exponentially: Gartner predicts 25 billion devices will be connected to the IoT by 2020.

IDC predicts that in that same year, the "digital universe" will reach 44 zettabytes – that's 640.2 billion 64GB tablets full of data – by a world population that's projected to be fewer than 8 billion people, according to the July 2015 update to the International Data Base.

IoT's Daily Influence

The IoT is being leveraged by people and organizations across the industry spectrum for a variety of purposes, changing nearly everybody's daily lives, as shown in the following examples.

Personal Use

IoT connections can send an individual's blood pressure, glucose levels, and other medical metrics to doctors. Pedometers and health meters on smart watch devices also help people track and share their progress toward their personal health goals.

Sensors on cars alert emergency services to accidents, and responders locate accidents via geographic positioning systems.

"Smart" homes have thermostats that can be adjusted, lights that can be turned off and on, and garage doors that can be opened and closed via smartphone, refrigerators that can track food supplies through radio frequency identification tags and automatically order more, and washing machines that turn on when the demand for energy is low.

Introduced in March, Amazon's Wi-Fi-enabled Dash buttons can be located in kitchens, bathrooms, and garages, enabling users to reorder the products they use frequently in those locations with a single click.

Government Use

"Smart" cities are also a growing trend around the globe. Sensors combined with information and communication technologies run cities more efficiently and effectively, reducing costs and the consumption of valuable resources.

Singapore, for example, connects smart devices to taxi mirrors to monitor traffic congestion. The sensors feed data into a centralized hub and analytics predict traffic patterns and redirect traffic lights to improve traffic.

Global Use

The Organization for Economic Co-operation and Development's Digital Economy Outlook shows South Korea as the most-connected country, with 37.9 things connected to the Internet per 100 people. Interestingly, the United States is fourth at 24.9 per hundred. (See Figure 1 below.)

The Cost for IoT: Privacy

The real cost of the IoT may be greater than most people think. While most understand the potential threats of searching web pages and take steps to protect themselves with antivirus software, they may not understand the need for the same type of protection related to IoT use.

Smart Homes

That thermostat or security camera purchased to be controlled with a smartphone, for example, needs to be connected to the Internet to work, which opens the home to potential risks, including invasion of the residents' privacy.

"The appealing convenience of Smart Home devices comes with a sobering downside," writes Randy Southerland on *SourceSecurity.com*. "They can also send a steady flood of personal data to corporate servers, where it's stored and even shared with companies and individuals you don't know and over whom you have no control."

Southerland recounted the furor earlier this year that came from the revelation that televisions with features that control channels and volume by voice command also record conversations and could potentially send them to outside parties. The fine print in privacy policies, Southerland wrote, revealed this, as well as the fact that the function could be turned off.

Freemiums

A lot of personal information is proliferating from IoT devices and individuals subscribing to digital services, such as LinkedIn, Facebook, Gmail, and Snapchat, as well as

Rank	Country	Per 100 inhabitants
1	South Korea	37.9
2	Denmark	32.7
3	Switzerland	29.0
4	United States	24.9
5	Netherlands	24.7

Source: OECD Digital Economy Outlook 2015 available at h*ttp://dx.doi.org/10.1787/888933225312*

smartphone applications. These are known as *freemiums* – free services that many eventually pay a premium for to gain additional features and functionality.

People signing up for these accounts generally must agree to the providers' terms of use, which often comprise a long list of legalese that few read. Instead, users click "yes," oblivious to the privacy rights they may be forfeiting. Companies offering the free services are not intent on invading their users' privacy, but they are in the business of providing personalized data to organizations that will pay for it.

In this age of *quid pro quo*, or "something for something," these companies provide services in exchange for user information, which they scientifically aggregate, sort, and index in order to deliver personalized responses to their users. For example, the ads that pop up on users' screens are determined by complex algorithms and predictive analytics of data derived from the user's profile, preferences, browsing habits, and spending history.

According to the 2015 Altimeter Group study "Consumer Perceptions of Privacy in the Internet of Things," while the vast majority of consumers don't know what the term *Internet of Things* means, they know they have Internet-connected devices – and 45% of the respondents expressed very low trust that the companies are protecting the personal data they are collecting.

Read More About It (accessed 19 Oct. 2015)

Gartner Inc. "Gartner Says 4.9 Billion Connected 'Things' Will Be in Use in 2015," November 11, 2014. *www.gartner.com/newsroom/id/2905717*

Higginbotham, Stacey. "Companies need to share how they use our data. Here are some ideas." July 16, 2015. *http://fortune.com/2015/07/06/consumer-data-privacy/*

ITU. Internet of Things Global Standards Initiative. July 1, 2015. *www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx*

Mejia, Paula. "Wary of Privacy Issues? Ditch Dropbox and Avoid Google, Says Edward Snowden." *Newsweek*, 11 Oct. 2014. *www.newsweek.com/wary-privacy-issues-ditch-dropbox-and-avoid-google-says-edward-snowden-276956*

National Strategy for Trusted Identifies in Cyberspace. "The Fair Information Practice Principles," February 2014. *www.nist.gov/nstic/NSTIC-FIPPs.pdf*

Organization for Economic Co-operation and Development. "OECD Digital Economy Outlook 2015," 29 May 2015. *http://dx.doi.org/10.1787/888933225312*

_____. "Guidelines on the Protection of Privacy," ammended 11 July 2013. *http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf*

Southerland, Randy. "Smart Home Security Risks with Internet of Things (IoT)." SourceSecurity.com U.S. edition. *http://us.sourcesecurity.com/news/articles/18159.html*

U.S. Federal Trade Commission. "Staff Report: Internet of Things: Privacy & Security in a Connected World," January 2015. *www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf*

Consumers' Protection of Data

The IoT wave is moving much more rapidly than the right of privacy can be ensured. And although the U.S. Federal Trade Commission (FTC) has proposed federal law to address data privacy, and groups meeting at various summits, trade shows, and think tanks are coming together to address these concerns, consumers must own the responsibility for their data privacy.

One man who infamously put privacy on the front page of newspapers around the world in 2013, U.S. National Security Agency whistleblower Edward Snowden, recently provided advice for how to protect your own privacy.

In an account of an interview with The New Yorker's Jane Mayer that was published online by Newsweek, Paula Mejia quoted Snowden as saying people should "search for encrypted communication services" because they "enforce your rights" and to be cautious about online services like Facebook, Google, and Dropbox, which he said are "hostile to privacy." He recommended using secure services to encrypt information and using online storage providers that care about privacy.

Consumers should document the accounts they have opened, review the providers' privacy policies, and review the information stored with or transmitted through these providers. If any of it is private, it might be time to reassess their use.

Further, document every "thing" connected to the Internet, as this could help track the source if any "leak" should occur.

Organizations' Protection of Data

Assessing personal privacy risks is a good first step in considering how to protect the privacy of the organization's internal and external customers and stakeholders. IG professionals need to ensure the organization has implemented and is in compliance with comprehensive security and privacy policies to protect private data.

In the FTC's January 2015 staff report "Internet of Things: Privacy & Security in a Connected World," the agency recommended data minimization as a way to balance data use with privacy protection. Organizations can decide not to collect data at all; collect only the data necessary to the product or service being offered; collect less data that is sensitive; or de-identify the data they collect. If none of these options works, the organization can seek consumers' consent for collecting "additional, unexpected" data.

IG professionals must ensure comprehensive internal compliance audits to confirm their organizations' adherence to the long-standing U.S. "Fair Information Practice Principles" (FIPP). Rooted in the seminal report on privacy issued in 1973 by The Secretary's Advisory Committee on Automated Personal Data Systems, "Records, Computers and the Rights of Citizens," the FIPP are at the core of the U.S. Privacy Act of 1974.

OECD Guidelines

The FIPP also form the core of the widely accepted 2013 *OECD Guidelines on the Protection of Privacy*:

1. **Collection Limitation Principle**. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. **Data Quality Principle**. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3. **Purpose Specification Principle**. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. **Use Limitation Principle**. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:
   a. with the consent of the data subject; or
   b. by the authority of law.
5. **Security Safeguards Principle.** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
6. **Openness Principle**. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. **Individual Participation Principle**. An individual should have the right:
   a. to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
   b. to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
   c. to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
   d. to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
8. **Accountability Principle**. A data controller should be accountable for complying with measures which give effect to the principles stated above.

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

A Balancing Act

The vast volume of data being generated by the IoT is a double-edged sword of value and risk that must be balanced carefully. In this hyperconnected world, informed citizens must balance the benefit of using IoT with their need for protecting their privacy. Organizations that consume the vast supply of data the IoT generates must also balance the value of using that data against the risk of violating customer and stakeholders' rights to privacy.

It is the responsibility of IG professionals that their organizations do this by following the OECD Principles, recommending the collection of personally identifiable information be minimized, and ensuring compliance with applicable privacy laws. **END**

Michael S. Smith, Ph.D., IGP, CRM, can be contacted at mike.s.smith@charter.net. *See his bio on page 47.*

Implications of E-Mail Mismanagement and Best Practices for Preventing It

John Isaza, Esq.

E-mail mismanagement continues to make headlines almost daily. In this article, California-based attorney John Isaza answers several questions about e-mail best practices and the legal repercussions of poor e-mail management in the United States – because bad press can be costly to any organization.

In the United States, could a person really go to jail for destruction of e-mails?

In short, yes. However, at the U.S. federal level, the punitive provisions under the Sarbanes-Oxley Act are rarely cited or used, and even so, they are limited to federal investigations and don't apply to court cases.

Should the courts ever choose to entertain it more regularly, culprits could face jail time or millions of dollars in sanctions under the little-utilized 18 USC Section 1519 (Destruction, alteration, or falsification of records in Federal investigations and bankruptcy), which states:

> Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both.

Fines in the millions and the specter of 20 years in jail are serious business. The questions, thus, become:

- To what extent can an organization destroy information if it knows it is not relevant to an investigation?
- Should the organization, instead, preserve information to avoid the appearance of impropriety?

Ultimately, the choice to delete e-mails during pending or threatened litigation or agency investigations is a risk-based decision that organizations with multiple legal holds have to entertain on a daily basis. Among the questions to ponder is "Can an organization delete, say, disaster recovery tapes that include e-mails, even if there is pending or threatened litigation?" To answer that question

affirmatively, the organization must be absolutely certain that the tapes are purely redundant for disaster recovery only and don't constitute their *de facto* records management system.

With the above as a backdrop, following are some related areas of concern.

What are some best practices in encouraging – or compelling – the deletion of old e-mails?

All these issues go the core tension between records retention and the need to dispose of expired data. If the information exists and is relevant to the subject matter of a lawsuit or investigation – even if it is merely anticipated or foreseeable litigation – it is discoverable. Therefore, it behooves organizations to dispose of needless e-mails and data *before* litigation/investigation ensues or becomes credibly probable.

If a *record* – which ARMA defines as "any recorded information, regardless of medium or characteristics, made or received and retained by an organization in pursuance of legal obligations or in the transaction of business" – has expired according to the organization's retention schedule, it should be disposed of immediately, unless, of course, it is subject to a legal hold at the time. Otherwise, the organization opens itself up for liability and discoverability of e-mails that could be read out of context.

The real trick for organizations is to determine which e-mails are *records* that must be retained per the retention policy, versus all other non-record data that can be disposed of at any time as long as it is not subject to a legal hold.

Are there any cybersecurity repercussions for comingling personal and work e-mail accounts?

Attempted breaches of mobile devices are on the rise, especially considering that most mobile devices include e-mail accounts. In the first quarter of 2012, for instance, McAfee Labs recorded more than 8,000 mobile malware strands, with the vast majority seeking to penetrate Android systems. This was a 400% increase over the previous year, according to Visage Mobile's white paper "Lighting the Path to Successful BYOD Programs."

Thus, the seriousness of a potential breach is palpable, especially in the case of a government official or corporate officer accessing personal e-mails on a mobile device, which could have less secure connections than official state business accounts.

If an e-mail account is hacked, does it put all the people in the organization using the server at risk?

Not necessarily. The security risk depends entirely on such things as the type of hacking, the target, its breadth, and the content accessed. Hacking into a person's e-mail account does not necessarily mean access to his or her e-mail contacts, though it could be damaging to the extent that any of the contents could be discerned from the e-mail account. It would depend on how the account is configured and what kind of integration it has with other devices, such as the person's laptop, office computer, iPad, and cloud-based servers.

Is there required self-reporting if an e-mail account is hacked?

Depending on the organization's industry, a hacking incident may be subject to requirements to notify government authorities, third-party associates, and customers. Basically any organization housing personally identifiable information (PII) or payment card industry (PCI) regulated data could be subject to disclosure requirements and, by extension, so would the individuals of that company.

In the healthcare sector, for instance, data breaches are a serious event that would trigger all kinds of regulatory scrutiny. On the opposite end of the spectrum, even organizations that are not in a highly regulated PII or PCI environment need to vet all breaches.

All organizations' BYOD policies should include language requiring employees to notify them about any breach of their personal devices. Depending on the size and industry of the organization, it might also provide a reporting hotline.

How can organizations find out if an executive is using personal e-mail accounts for business?

Typically, the use of personal e-mail accounts is discovered during routine audits. However, since audits may be infrequent or audit recommendations ignored, it may take an embarrassing event to bring attention to the issue for some organizations. At its core, the biggest problems arise from the ever-increasing use of personal devices in the workplace and with employees logging into work from their home computers or laptops.

Although the BYOD issue has been on the radar of most large organizations for the last three to five years, they are succeeding in setting policies around it only to varying degrees.

Presumably, the BYOD policy will stress that personal e-mail accounts are never to be used for business. In practicality, though, this can be a challenge to prevent. When a device has both business and personal accounts attached to it, for example, it is easy to erroneously send a work-related e-mail from a personal account. Once that happens, if the recipient replies to all, the stage is set for a breach in the BYOD protocol.

What are some good tips for an organization to prevent use of personal e-mails or applications for business purposes?

All organizations should have BYOD policy, procedures, and guide-

lines that include five core elements:

1. Guidance on acceptable uses of personal devices to transact official business, including instructions on distinguishing personal e-mail account usage from official business accounts
2. A list of the types of sanctioned devices (e.g., iPad, Blackberry, iPhone) and rules of engagement with IT
3. Policies around logistics, such as whether the company will reimburse for usage of the personal device
4. Security information that addresses encryption and other features that must be enabled to protect the data in the event of a loss or breach
5. A section on risks, liabilities, and disclaimers to help protect the organization against the employee misuse of the device

Armed with the BYOD policy, other organizational documents (e.g., policies for password usage, cloud computing, social networking) could get into the specifics of training and auditing for compliance, including the frequency for these.

Who is at fault for user violation of e-mail protocols?

Ultimately, progress and the competition to stay on top of the competition are at fault for e-mail protocol violations. The adoption of technology has far outpaced the ability of organizations to keep up with the implications of using it. Consumers and customers demand the immediacy facilitated by technology, so people, processes, and procedures take a back seat in favor of adoption.

In the ideal scenario, before organizations roll out or permit any new technology (e.g., e-mail tools, social media, content management), they need to vet their change management process (i.e., a controlled roll-out that ensures proper user adoption and compliance), as well as their ability to audit and monitor compliance with their policies and procedures. In today's fast-paced world, constant auditing and monitoring are required.

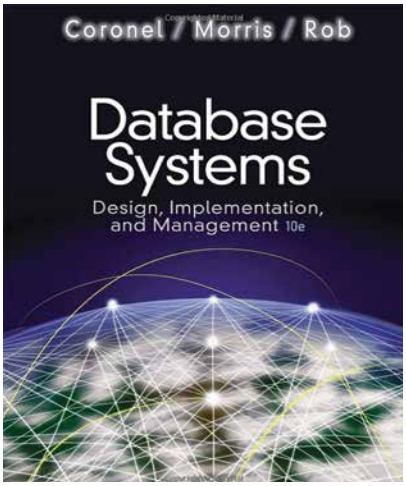
Those looking for "fault" are looking at those who do not learn from their experiences. In those instances, those in charge of the program roll-out are at fault for not paying attention to system failures.

All that said, a corporate leader confronted with a systematic policy failure, coupled with high-level customer demands to keep up with technology, faces a losing battle. The key is to strike a balance between controls and business needs. **END**

John Isaza, Esq., can be contacted at *John.Isaza@InfoGovSolutions.com* or *John.Isaza@RimonLaw.com*. See his bio on page 47.

Learn to Create and Work with **Relational Databases**

Erik Werfel, J.D., IGP, CIPP-US, CISSP, CEDS



Database Systems Design, Implementation and Management, 11th Ed. is an up-to-date, well-organized textbook that provides a comprehensive look at relational databases. It thoroughly covers entity relationship modeling, database modeling, normalization, and the development of useful database systems using structured query language (SQL), as well as relational database optimization, database administration, and security. From the basic to the complex, it is intended to get the reader to the point of creating and working with databases.

The book doesn't presuppose any familiarity with the material – it starts with the fundamentals – but some understanding of computer systems would be helpful to readers, particularly if they are reading it outside the context of a course. As a good reference for database concepts, it would be handy to keep it on the shelf for its practical glossary and as a refresher.

Contents

The book is divided into six parts:

1. Database Concepts provides an interesting history of data and database management systems.
2. Design Concepts covers data modeling and normalization.
3. Advanced Design and Implementation gets into detail about SQL.
4. Advanced Database Concepts focuses on performance tuning and optimization.
5. Databases and the Internet covers connectivity and web applications.
6. Database Administration focuses on administration and security.

Database Systems Design, Implementation and Management provides many practical SQL examples and is implementation agnostic. It covers SQL language variants specific to SQL Server, Oracle, MySQL, and even MS Access, providing SQL examples for each. The book also provides advice and cautions for specific database types.

The book also discusses business intelligence, data analytics, cloud-based systems and big data, and no-SQL systems, but these topics are not covered in the same detail as SQL and relational databases, which are at the core of this book. While it makes readers aware of these newer topics, they are a bit of an afterthought. Those who are not focused specifically on relational database management systems should look elsewhere.

Database Systems Design, Implementation and Management
Authors: Carolos Coronel, Steven Morris, Peter Rob
Publisher: Cengage Learning
Publication Date: 2013
Length: 752 pages
Price: $243.95
ISBN: 978-1111969608
Source: *www.cengage.com*

Supplemental Materials

The publisher's website provides downloads of the sample databases discussed for several different systems, as well as free downloadable appendices. Additional study materials are provided with the purchase of a separate website access card, but I did not have the opportunity to review them.

Usefulness for RIM

Database Systems Design, Implementation and Management could serve as a good introduction to relational database management systems for the records and information management (RIM) professional who is familiar with them at the 10,000-foot level but needs to gain additional practical knowledge. It is written as a textbook, however, so there are no

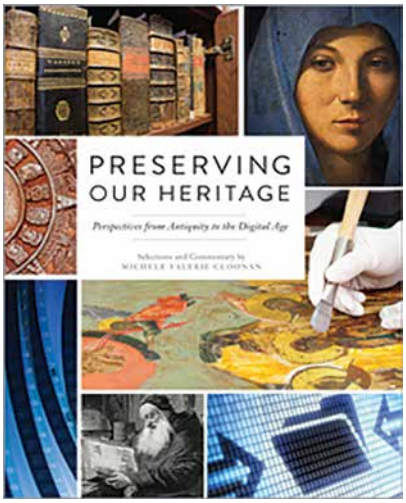
answers provided for the quizzes at the end of each chapter, and some topics that might benefit from a more in-depth discussion seem to be left to the instructor. A different book might be more appropriate for self-study, but this one would be a good supplement for independent study.

Because of the degree of detail provided, this book is probably inappropriate for someone interested in gaining just high-level familiarity with the functioning of various database systems, rather than acquiring a practical understanding of relational database development and management. **END**

Erik Werfel, J.D., IGP, CIPP-US, CISSP, CEDS, can be contacted at erik.werfel@gmail.com. *See his bio on page 47.*

Discovering the Universe of **Preservation History and Practice**

Stephen E. Haller, CRM



Preserving Our Heritage is a lengthy, fairly comprehensive examination of a range of practices and challenges regarding information preservation for almost three millennia. This undertaking and the book's sheer size may seem initially imposing, but its organization and added features greatly facilitate navigation for specific or extensive study or as a reference resource.

The legion of contributors offers a rich collection of resources for students, instructors, and professionals in not only the library field, but also for allied areas of archives, museums, and others responsible for or concerned with the preservation of cultural heritage.

Organization

Before considering the 11 major chapter headings for the 95 essays in the book, readers should note some particularly helpful features beyond the standard preface and table of contents. A 14-page, briefly annotated "Preservation Timeline" (ca. 750 BC – 2013) provides very useful context for the scope of this work. Although there are appropriate endnotes throughout the essay sections, descriptive "Contributors" and "Credits" sections are also included. The work concludes with two separate indexes: an "Author and Title Index" and a "Subject Index."

Cloonan brings together numerous essays from respected experts who represent and/or are knowledgeable about a wide range of disciplines and practices comprising preservation as she presents them in the major chapters for each component.

These major sections allow for more than linear access to extensive sets of information for the variety of individuals making up the book's intended audiences. Each of the 11 major "chapters" begins with a solid overview and proceeds with a number of essays on the chapter topic.

Preserving Our Heritage: Perspectives from Antiquity to the Digital Age
Editor: Michele Valerie Cloonan
Publisher: ALA Neal-Schuman
Publication Date: 2015
Length: 736 pages
Price: $98
ISBN: 978-1-55570-937-2
Source: *www.alastore.ala.org*

Chapter Content

Chapter 1, "Early Perspectives on Preservation," sweeps from Biblical times through the late nineteenth century with practical and intriguing glimpses of the nature and challenges of what was almost more like survival of cultural memory rather than intentional, systematic preservation (with some important exceptions).

Chapter 2, "Perspectives on Cultural Heritage," pauses for writers to define and further explore the notions of memory and heritage.

The next chapters provide what most readers would expect to find

in such a work, as the contributors delve into the primary components of modern or recent institutions, practices, and management. Chapter 3, "Preservation in Context: Libraries, Archives, Museums and the Built Environment," includes 21 essays to extensively describe the preservation efforts and concerns over time in the four disciplines. The tension of preserving objects and/or the information they contain is well covered, up to and including the volume of information challenges of the digital age.

Chapter 4, "Collections Development and Management," is somewhat mistitled, since it primarily focuses on preservation practices and the difficulties in prioritizing what to preserve and various "how to" approaches for both physical and digital materials. In many settings, collection development also encompasses subject area and acquisition strategies and policies.

Chapter 5, "Risks to Cultural Heritage: Time, Nature, and People," begins to place preservation challenges within a risk management framework, ranging from natural to manmade disasters, and making choices on what to protect and/or preserve.

Chapter 6 "Conservation," provides a survey of practices over time, as well as a level of technical detail by some well-known contributors (e.g., Paul Banks' "The Laws of Conservation"). The concept of "reversibility" is revisited, as is the impact of availability of high quality digital surrogates.

Chapter 7, "Frameworks for Digital Preservation," offers eight essays to provide a thorough and interesting view of the considerable past thinking about this evolving challenge. Unfortunately, only two of the essays were written within the past eight years, perhaps disappointing a reader hoping for more practical, current practice or solutions.

Chapter 8, "Preservation Policy," examines a number of high-level policy approaches to preservation programs and prioritizing by describing technical and public policies (including examples of cultural policies).

Chapter 9, "Ethics and Values," incudes 16 essays that range from codes of ethics at institutional and key professional associations and to a number of cultural heritage considerations from the indigenous people and international perspectives (e.g., UNESCO) regarding preservation, protection, and treatment of material.

The essays in Chapter 10, "Multicultural Perspectives," expand somewhat on the previous chapter, especially regarding sensitivity to a number of often conflicting issues within current museum practices.

Chapter 11, "Sustainability," again focuses on conservation's role, but it also brings the reader's attention to the need to also regard the larger (non-institutional) communities and environment where cultural heritage institutions live and do their work.

Offers Something for Many Readers

The compiler's concluding "Epilogue" encourages readers to continue to build on this "anthology" – especially the always-evolving "digital media" implications and practices for an equally challenging notion of what "preservation" will mean.

This massive work is both a comprehensive resource and retrospective examination of topics of interest to several types of cultural heritage organizations and professionals. Although it covers a large universe of preservation history, practice, context, and recommendations, many readers will be able to easily find content within chapters relevant to their own situation or discipline. **END**

Stephen E. Haller, CRM, can be contacted at stephen.haller@usm.edu. *See his bio on page 47.*

UNITED STATES POSTAL SERVICE® Statement of Ownership, Management, and Circulation (All Periodicals Publications Except Requester Publications)

1. Publication Title: Information Management
2. Publication Number: 1 5 3 5 – 2 8 9 7
3. Filing Date: 10-21-15
4. Issue Frequency: Bi-Monthly
5. Number of Issues Published Annually: 6
6. Annual Subscription Price: $140
7. Complete Mailing Address of Known Office of Publication (Not printer) (Street, city, county, state, and ZIP+4®): ARMA International, 11880 College Blvd., Suite 450, Overland Park, KS 66210
Contact Person: Vicki Wiler
Telephone (Include area code): 913-217-6014
8. Complete Mailing Address of Headquarters or General Business Office of Publisher (Not printer): ARMA International, 11880 College Blvd., Suite 450, Overland Park, KS 66210
9. Full Names and Complete Mailing Addresses of Publisher, Editor, and Managing Editor (Do not leave blank)
Publisher (Name and complete mailing address): Robert Baird, CEO, ARMA International, 11880 College Blvd., Suite 450, Overland Park, KS 66210
Editor (Name and complete mailing address): Vicki Wiler, ARMA International, 11880 College Blvd., Suite 450, Overland Park, KS 66210
Managing Editor (Name and complete mailing address): N/A
10. Owner (Do not leave blank. If the publication is owned by a corporation, give the name and address of the corporation immediately followed by the names and addresses of all stockholders owning or holding 1 percent or more of the total amount of stock. If not owned by a corporation, give the names and addresses of the individual owners. If owned by a partnership or other unincorporated firm, give its name and address as well as those of each individual owner. If the publication is published by a nonprofit organization, give its name and address.)

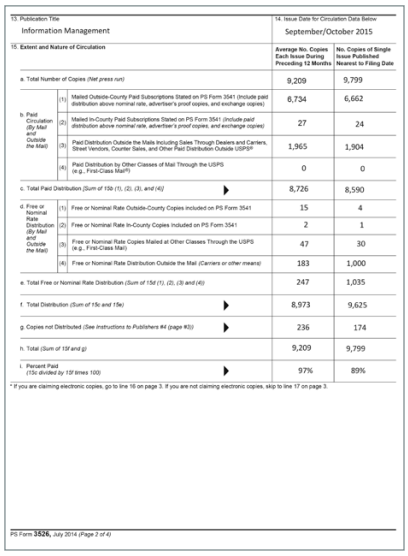
Full Name	Complete Mailing Address
ARMA International	11880 College Blvd., Suite 450, Overland Park, KS 66210

11. Known Bondholders, Mortgagees, and Other Security Holders Owning or Holding 1 Percent or More of Total Amount of Bonds, Mortgages, or Other Securities. If none, check box ► ☐ None

Full Name	Complete Mailing Address

12. Tax Status (For completion by nonprofit organizations authorized to mail at nonprofit rates) (Check one)
The purpose, function, and nonprofit status of this organization and the exempt status for federal income tax purposes:
☐ Has Not Changed During Preceding 12 Months
☐ Has Changed During Preceding 12 Months (Publisher must submit explanation of change with this statement)

PS Form 3526, July 2014 (Page 1 of 4 (see instructions page 4)) PSN: 7530-01-000-9931 PRIVACY NOTICE: See our privacy policy on www.usps.com.



13. Publication Title: Information Management
14. Issue Date for Circulation Data Below: September/October 2015

15. Extent and Nature of Circulation		Average No. Copies Each Issue During Preceding 12 Months	No. Copies of Single Issue Published Nearest to Filing Date
a. Total Number of Copies (Net press run)		9,209	9,799
b. Paid Circulation (By Mail and Outside the Mail)	(1) Mailed Outside-County Paid Subscriptions Stated on PS Form 3541 (Include paid distribution above nominal rate, advertiser's proof copies, and exchange copies)	6,734	6,662
	(2) Mailed In-County Paid Subscriptions Stated on PS Form 3541 (Include paid distribution above nominal rate, advertiser's proof copies, and exchange copies)	27	24
	(3) Paid Distribution Outside the Mails Including Sales Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Paid Distribution Outside USPS®	1,965	1,904
	(4) Paid Distribution by Other Classes of Mail Through the USPS (e.g., First-Class Mail®)	0	0
c. Total Paid Distribution (Sum of 15b (1), (2), (3), and (4))		8,726	8,590
d. Free or Nominal Rate Distribution (By Mail and Outside the Mail)	(1) Free or Nominal Rate Outside-County Copies included on PS Form 3541	15	4
	(2) Free or Nominal Rate In-County Copies included on PS Form 3541	2	1
	(3) Free or Nominal Rate Copies Mailed at Other Classes Through the USPS (e.g., First-Class Mail)	47	30
	(4) Free or Nominal Rate Distribution Outside the Mail (Carriers or other means)	183	1,000
e. Total Free or Nominal Rate Distribution (Sum of 15d (1), (2), (3) and (4))		247	1,035
f. Total Distribution (Sum of 15c and 15e)		8,973	9,625
g. Copies not Distributed (See Instructions to Publishers #4 (page #3))		236	174
h. Total (Sum of 15f and g)		9,209	9,799
i. Percent Paid (15c divided by 15f times 100)		97%	89%

* If you are claiming electronic copies, go to line 16 on page 3. If you are not claiming electronic copies, skip to line 17 on page 3.

PS Form 3526, July 2014 (Page 2 of 4)

UNITED STATES POSTAL SERVICE® Statement of Ownership, Management, and Circulation (All Periodicals Publications Except Requester Publications)

16. Electronic Copy Circulation

	Average No. Copies Each Issue During Preceding 12 Months	No. Copies of Single Issue Published Nearest to Filing Date
a. Paid Electronic Copies ►		
b. Total Paid Print Copies (Line 15c) + Paid Electronic Copies (Line 16a) ►		
c. Total Print Distribution (Line 15f) + Paid Electronic Copies (Line 16a) ►		
d. Percent Paid (Both Print & Electronic Copies) (16b divided by 16c × 100) ►		

☐ I certify that 50% of all my distributed copies (electronic and print) are paid above a nominal price.

17. Publication of Statement of Ownership
☒ If the publication is a general publication, publication of this statement is required. Will be printed in the Nov/Dec 2015 issue of this publication. ☐ Publication not required.

18. Signature and Title of Editor, Publisher, Business Manager, or Owner: Vicki Wiler, Editor in Chief — Date: 10-21-15

I certify that all information furnished on this form is true and complete. I understand that anyone who furnishes false or misleading information on this form or who omits material or information requested on the form may be subject to criminal sanctions (including fines and imprisonment) and/or civil sanctions (including civil penalties).

PS Form 3526, July 2014 (Page 3 of 4) PRIVACY NOTICE: See our privacy policy on www.usps.com

Contact Information **AUTHOR**INFO


CHIAIESE


GABLE


HALLER


ISAZA


RICHARDSON


SMITH


WERFEL

Policies and Processes for Protecting Information Page 20

Beth Chiaiese, CRM, is the director, professional responsibility & compliance for Foley & Lardner LLP, where she has worked since 2001. During her 36-year career, she has worked as both a practitioner and a consultant, helping firms develop work processes and technology based on best practices in the areas of information governance, records management, conflicts of interest, new business processing, and risk management.

A frequent speaker for national and local groups such as ILTA, ARMA, ALA, ABA, and the Attorneys' Liability Assurance Society, Chiaiese is a co-author of *Records Management in the Legal Environment* and is the author of three monographs in the ARMA series Information Governance in the Legal Environment: *Ethical and Legal Foundations of Law Firm Records Management and Information Governance, Lawyer and Matter Mobility*, and *Information Confidentiality, Privacy and Security in the Law Firm*. She is a Certified Records Manager and holds a master's degree in library and information sciences.She can be contacted at *bchiaiese@foley.com.*

The Principles: The Principles, IGMM: Tools for Professional Growth Page 28

Julie Gable, CRM, CDIA, FAI, is the retired president and founder of Gable Consulting LLC, a firm that served clients' information governance needs for 25 years. The author of numerous articles on information-related topics, she has a master's degree in finance from St. Joseph's University and a bachelor's degree in management from Drexel University. Gable can be contacted at *juliegable@verizon.net.*

How to Combine RIM Programs After a Merger Page 32

Blake Richardson, CRM, CIP, is the information governance manager for a utility corporation. He is a Certified Records Manager (CRM) and a Certified Information Professional (CIP) with more than 18 years of records and information management experience with three Fortune 500 companies. The author of *Records Management for Dummies*, published by Wiley, Richardson is also a member of the Institute of Certified Records Managers' Examination Development Committee and frequently speaks at association events. He attained his undergraduate degree in accounting from Middle Tennessee State University. He can be contacted at *titansfan100@gmail.com.*

Protecting Privacy in an IoT-Connected World Page 38

Michael S. Smith, Ph.D., IGP, CRM is the data governance officer for Citi Group. Formerly he was an industry consultant in information governance for IBM Global Business Solutions and served in executive roles at Iron Mountain. His 15 years of RIM experience solving customers' information needs provides him insights into current changes within the information management industry. Smith earned a doctorate in information systems & technology from the University of Phoenix. He can be contacted at *mike.s.smith@charter.net.*

Implications of E-Mail Mismanagement and Best Practices for Preventing It Page 40

John Isaza, Esq., is a California-based attorney, chief executive officer of Information Governance Solutions LLC, and law partner at RIMON, PC, a twenty-first century law firm that includes specialty in electronic information governance, records management, and overall corporate compliance. He can be contacted at *John.Isaza@InfoGovSolutions.com* or *John.Isaza@RimonLaw.com.*

Learn to Create and Work with Relational Databases Page 44

Erik Werfel, J.D., IGP, CIPP-US, CISSP, CEDS, is a technologist who has been a member of the technical staff and management at Fragomen, Del Rey, Bernstein and Loewy for more than eight years. He previously was a developer at Bright Ideas Software and Lucent Technologies. A certified Information Governance Professional, Certified Information Privacy Professional-US, Certified Information Systems Security Professional, and Certified E-Discovery Specialist, he earned a juris doctor degree from the University of Pennsylvania Law School and a bachelor of arts degree in economics from Hampshire College. Werfel is a member of the New Jersey Bar. He can be contacted at *erik.werfel@gmail.com.*

Discovering the Universe of Preservation History and Practice Page 45

Stephen E. Haller, CRM, is curator of historical manuscripts and university archives/assistant professor at The University of Southern Mississippi. He has served in archives and records management posts over three decades at historical organizations, including senior director of collections and library for the Indiana Historical Society and director of archives and records for the Colonial Williamsburg Foundation in Virginia. Haller, who received his bachelor and master of arts degrees from Miami University (Ohio), has taught college classes, held offices in professional organizations, and authored historical and technical publications. He can be contacted at *stephen.haller@usm.edu.*

ADINDEX CONTACT INFORMATION

IBC	**Fujitsu**	*www.fcpa.com*
19	**Institute of Certified Records Managers**	518.694.5362 – *www.ICRM.org*
FC, BC	**Iron Mountain**	800.899.4766 – *ironmountain.com/BestPractices*
3	**NAID**	*http://directory.naidonline.org*
IFC, 43	**Next Level**	*www.arma.org/nextlevel*
5	**OPEX Corporation**	*www.opex.com/agility*
23	**PRISM International**	*www.prismintl.org*
11,13	**Syscom Service**	*info.syscomservices.com/security*

FUJITSU

When it comes to document imaging the value is in the data we capture

Richard Stinnett
V.P. of Operations, BTCO
www.btcoinc.com

fi Series scanners with PaperStream

When it comes to document imaging, the value is in the data. That's why Fujitsu Computer Products of America created a portfolio of software products to complement our industry-leading scanners to help you get the most from your capture solution. At the heart of every high-speed fi Series document scanner is PaperStream IP. The powerful drivers behind PaperStream Capture Pro that ensure high quality image processing—while PaperStream Capture Pro enables efficient document separation and content indexing. For fast, easy-to-use, and simple release, Fujitsu helps you get the most out of data capture by reducing resources, minimizing manual errors, and increasing your bottom line. See us at **www.fcpa.com**

shaping tomorrow with you

PaperStream