UP FRONT
News, Trends & Analysis

GOVERNMENT RECORDS

Audit Faults SEC's Records Management Practices

In a public July 2012 letter to Sen. Charles E. Grassley (R-Iowa) on behalf of a former long-time Securities and Exchange Commission (SEC) official, the SEC said it had violated federal law by destroying financial records related to investigations of various financial institutions from 1993 to 2010. The 9,000 records in question pertained to the initial investigation of institutions that reportedly included Goldman Sachs, Bank of America, Morgan Stanley, and Wells Fargo.

The documents were shredded in compliance with an SEC policy in effect during that time period that stated that documents related to an inquiry that didn't become an official investigation should be destroyed. Unfortunately, that policy conflicted with federal law requiring such documents to be retained for 25 years.

SEC spokesperson John Nester told *The Washington Post* that the agency changed the policy in 2011, requiring employees to follow the agency's records management policy. He also pointed out the retention requirements "pertain to documents that meet the definition of a record, not every document that comes into an agency's possession in the course of its work."

Former SEC enforcement lawyer Darci Flynn contacted the National Archives and Records Administration (NARA) last year. NARA responded with an audit of the agency's records management practices.

NARA released its findings in an audit report dated September 30, 2012. According to *Government Executive.com*, the report faulted the SEC for unclear records management policies and inadequate employee training. The audit findings reportedly included 12 recommendations, including more visits to offices by records management specialists, better internal document controls, and policy training in records retention. An implementation plan was due before the end of 2012.

DATA SECURITY

Android Apps May Leak Personal Data

German security researchers recently determined that some Android applications may pose certain serious security risks.

Researchers at the Leibniz University of Hanover in Germany studied the potential security threats posed by some Android applications that use Secure Sockets Layer and Transport Layer Security (SSL/TLS) protocols to protect data transmissions. According to the study report that was released in October 2012, "Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security," researchers specifically looked at 13,500 popular free apps in Google's Play Market because "the lack of visual security indicators for SSL/TLS usage and the inadequate use of SSL/TLS can be exploited to launch man-in-the-middle (MITM) attacks."

Using MalloDroid, a tool researchers built to detect potential vulnerability against MITM attacks, they determined that 8% of the apps contain code that could be vulnerable. No actual attacks have been reported; however, the researchers concluded the potential is definitely there.

According to the researchers' report, there are a variety of ways to minimize the problem of unencrypted traffic or SSL misuse. They can be categorized into three groups: (1) solutions integrated into the Android operating system, (2) solutions into app markets, and (3) standalone solutions.

The MalloDroid web app is an example of a standalone solution that the researchers intend to make available to Android users.

DATA SECURITY

India to EU: Declare Us Secure

India has asked the European Union (EU) to formally recognize India as a data-secure country. *The Times of India* reported the issue came up for discussion in a recent meeting between Commerce and Industry Minister Anand Sharma and Algirdas Semeta, the European Commissioner for Taxation and Customs Union, Audit and Anti-Fraud.

The issue is an important point of contention in the proposed Bilateral Investment and Protection Agreement (BITA), a free trade agreement between India and the EU that has been in negotiation since 2007.

Sharma pointed out that India's access to the EU market depends on it being declared data secure. The lack of such recognition prevents the flow of sensitive data, including patient information for telemedicine, to India under current EU data protection laws.

"It is our clear analysis that our existing law does meet the required EU standards. We would urge that this issue is sorted out quickly and necessary comfort in declaring India data secure in overall sense needs to be given as almost all the major *Fortune* 500 companies have trusted India with their critical data," Sharma said in an official statement.

The EU is reportedly undertaking a study to determine whether India's laws do indeed meet the EU's directive.

According to *The India Times* October 18, 2012, article, lifting the data flow restrictions on India would significantly increase India's $100 billion IT business processes outsourcing industry; 30% of the industry's exports are to the European market.

CLOUD COMPUTING

The State of Cloud Computing in Canada

The 2012 CloudLaunch conference held in mid-October 2012 in Ottawa was generally regarded as a frank and, at times, divisive discussion of what it will take to advance the adoption of cloud computing in Canada.

Andrew Fisher, executive vice president at Wesley Clover, was quoted in an October 16, 2012, blog posting by *expertIP* editor Shane Schick as saying the biggest barrier to adoption is a lack of interest from organizations, including the government, to stimulate the purchase of cloud computing services.

According to the blog post, Misha Nossik, chief technology officer of Afore Solutions and founder of the Ottawa Cloud Council, suggested that government chief information officers (CIO) are more concerned with protecting their budgets than embracing the cost-savings cloud computing can offer. Some feel, however, that cloud computing will never take off in the private sector until the government embraces it.

Schick contended that "adoption in Canada won't get much farther unless CIOs and vendors can forge a new kind of trusted partnership, one that looks a lot different in a world of ongoing services than it did in the previous one of on-premise sales."

This will be a serious test to those vendor relationships, Schick added. A test they can't afford to fail.

FOIA

NARA, Other Federal Agencies Launch FOIA Online System

The U.S. National Archives and Records Administration (NARA), the U.S. Environmental Protection Agency (EPA), and the U.S. Department of Commerce have developed an online system to expand public access to information requested under the Freedom of Information Act (FOIA).

According to NARA, *FOIAonline* (*https://foiaonline.regulations.gov*) offers the public one place to submit FOIA requests, track their progress, communicate with the processing agency, search other requests, access previously released responsive documents, and file appeals with participating agencies.

For federal agencies, *FOIAonline* provides a secure website to receive and store requests, assign and process requests, post responses, generate metrics, manage records electronically, create management reports, and electronically generate the annual report the FOIA requires from each agency.

The new system leverages the infrastructure developed for the EPA's *Regulations.gov*, the federal rulemaking portal that allows people to comment on federal regulations and other agency regulatory actions. This helped *FOIAonline* avoid many startup costs and is expected to save the government $200 million over the next five years if broadly adopted.

RISK MANAGEMENT

Gartner: A Good Offense Is Best Defense

A good defense isn't enough when it comes to ensuring an organization's data security, Gartner analysts told participants at the firm's Symposium/ITxpo 2012 held in October in Orlando. With the speed at which technology is changing and the agility of hackers is increasing, threats to security are growing faster than the means to defend against them. The time has come to stop just reacting and begin taking proactive measures, said Gartner analysts.

According to *InformationWeek.com*, Gartner Research Vice President Greg Young stressed the need for enterprises to focus on three main areas: protection of infrastructure (keeping the bad guys out); managing identity and access (letting the good guys in); and business continuity, compliance, and risk management (policies that keep the wheels on).

Young cited several factors that have made protecting infrastructure increasingly difficult, including emerging trends around software-defined networking, virtualization, cloud computing, and mobile smart devices. Strategic infrastructure planning, he concluded, doesn't try to address all threats, but rather requires aligning security mechanisms with an effective, carefully considered user-access policy.

Gartner Vice President Earl Perkins addressed the identity and access management issue. He suggested that enterprises could take advantage of social networking processes to improve user access management. Enterprises already manage access through permissions and entitlements; however, Perkins speculated that social media profiles could eventually be used in enterprise security mechanisms. This may be a decade away, said Perkins, but the integration of social media for effective user management has already begun.

Gartner Vice President Paul Proctor echoed Young's point that the processes should not try to protect against everything. The key lies in behavior changes. Enterprises need to increase their focus on employee training, he said. This is especially critical with the bring-your-own-device trend.

Keeping score by reporting security incidents is another area in need of a behavioral shift, contended Proctor. Instead of focusing on the number of incidents, enterprises should focus on identifying protection levels applicable to their needs. These needs will vary from industry to industry. Some organizations (e.g., manufacturing) possess intellectual property and little personal data, while others (e.g., financial institutions) have personal data and relatively little intellectual property to protect. The latter are going to be more likely targets for hackers.

GOING GREEN

Paper Still Rules in Many U.S. Federal Agencies

The U.S. government's digital transformation is well under way. However, a study by Open Text and the Government Business Council that was published in October revealed that only 22% of the 150 federal managers surveyed gave their information management systems an "A" or "B" grade. The average grade given was a "C" largely because of the agencies' reliance on paper records and even older media (e.g., microfiche and microfilm).

Fortunately, 82% of the respondents recognize that electronic information management (EIM) plays an essential or important role in agency operations. Almost half (48%) of the respondents see EIM as essential to operations. Unfortunately, only 28% consider their agency's EIM as being "adequate." The majority (58%) labeled it "inefficient," "confusing," or "outdated," primarily because of the amount of redundancy and the continued prevalence of paper records, despite available technologies. Nearly one-quarter (24%) said their agencies still manage microfiche or microfilm.

Even though paper still seems to rule, 54% of the agencies reported that between 34% and 80% of their information is currently available in a digital format.

Fifty-seven percent of the managers agreed that EIM can reduce time spent looking for records – time that can be reinvested in other tasks that serve the needs of citizens. And in many cases, EIM can improve the bottom line: 30% of federal managers say EIM can reduce operating costs.

Predictably, the biggest roadblock to fully implementing an EIM system is the lack of resources, followed by the lack of a clear information management strategy or policy.

When asked what they needed to fully implement EIM in their agency, two-thirds of the managers answered "agency-wide approach to information management," 57% cited a change in agency culture, and 56% said increased funding.

Read the full research report at *www.opentext.com/EIMreport*. (Registration required.)

DATA SECURITY

Singapore Passes Data Protection Act

Singapore's data privacy act was to take effect January 1, 2013. Enforcement, however, is not scheduled to begin until mid-2014 to give businesses enough time to adjust.

The new law gives individuals more control over their personal data, requiring organizations to apprise their constituents of the purpose for collecting, using, or disclosing their personal information.

The law also gives individuals the right to seek compensation for damages suffered directly as a result of a breach of the data protection rules. Organizations found guilty of violating the rule may be fined up to S$10,000 ($8,181 U.S.) per customer complaint.

A national do-not-call registry is established by the new law, as is a Personal Data Protection Commission (PDPC), which will be the country's primary authority on matters relating to personal data protection and enforcement of the new rule. PDPC could impose a penalty of up to S$1 million ($818,150 U.S.) if an organization doesn't comply.

The new law applies only to organizations in the private sector. The government already had its own data protection rules in place.

An element missing from the law is the requirement that organizations notify individuals when a breach occurs. Mandatory notification is standard in European and American data protection laws and will undoubtedly be added to Singapore's in time.

CYBERCRIME

Firm Lists Top Tricks Used by Spear Phishers

Early on, cybercriminals discovered that e-mail is a great avenue for spam and mass-distributed malware. It still is, according to a recent report from FireEye, a provider of threat protection for web and e-mail.

FireEye's "Advance Threat Report 1H 2012" recorded a 56% increase in malicious e-mails getting past organizations' security defenses between the first and second quarters of 2012.

Cybercriminals use certain common words in file names that trick large number of unsuspecting recipients to download or install files containing malware to their local drives. According to FireEye's "Top Words Used in Spear Phishing Attacks to Successfully Compromise Enterprise Networks and Steal Data," the top five draws in the first half of 2012 were "dhl," "notification," "delivery," "express," and "2012."

Interestingly, with only a couple of exceptions, the first half of 2012's list of the top 20 words is completely different from those deemed successful in the second half of 2011.

The percentage of attachments containing those words is also significantly higher. For example, the top draw in the first half of 2012 ("dhl") was included in the name of nearly 23% of attachments, while the most common word in the second half of 2011 ("label") was included in the name of just 15% of attachments.

FireEye found additional trends between the second half of 2011 and the first half of 2012. For example, the percentage of file names containing words related to shipping (e.g., "postal") grew from 19% to 26%. The number of words associated with urgency grew even more dramatically from nearly 2% to almost 11%.

On a somewhat more positive note, using the .EXE file extension was much less successful in 2012. Unfortunately, today's cybercriminals are using .ZIP and .PDF file extensions more successfully.

To guard against these threats, FireEye stressed that enterprises need to better educate users on how to recognize malware threats and employ more advanced technologies to detect and stop the advanced threats.

CLOUD COMPUTING

EU Looks to the Cloud for Economic Relief

The European Union (EU) is hoping that cloud computing will help its economy recover from its four-year debt crisis and recession. Specifically, CNBC reported the EU is looking to cloud computing to help boost the economy by creating 2.5 million new jobs and increasing the EU's gross domestic product by €583 billion ($760 billion U.S.) between 2015 and 2020.

International Data Corp., which helped the EU develop its cloud computing strategy, is even more optimistic, predicting that the new policy could develop close to 3.8 million new jobs.

Katherine Thompson, an analyst at Edison Investment Research, told CNBC she's not as optimistic. "I'm not sure I strictly agree that it will give such a boost to the economy," she said, "as the move to the cloud is often a shift from one form of expenditure to another, as opposed to incremental spend, and in many cases will be deflationary."

She added that she does agree with the EU's thinking that cloud computing will help create new types of companies and business models, which she said is already happening.

"The EU wants to focus on four key aims to help cloud computing realize its full potential," reported *CNBC.com's* Matt Clinch. "They want users to be able to easily move providers, a certification for trustworthy companies, contracts that would simplify regulations, and clear communication between providers and the public sector so work doesn't drift overseas to the U.S."

Of course, security remains a serious concern, regardless of how many jobs are created and where the data centers are located. It's critical that data security can be ensured.

CYBERCRIME

FTC Targets Computer Support Scams

In October 2012, the Federal Trade Commission (FTC) announced that it had launched "a major international crackdown on tech support scams." The commission took aim at telemarketers masquerading as being associated with major tech companies to scam consumers into believing their computers "are riddled with viruses, spyware, and other malware" and then charging hundreds of dollars to remotely access, fix, and monitor the consumers' computers.

A U.S. District Court judge ordered a halt to six alleged tech support scams and froze the defendants' assets. In announcing the judgment, FTC Chairman John Liebowitz stated that the defendants had "taken scareware to a whole other level of virtual mayhem."

The six operations, most of which were based in India, targeted English-speaking consumers in the United States, Canada, Australia, Ireland, New Zealand, and the United Kingdom (UK). They contacted the consumers by telephone and reportedly claimed they were affiliated with legitimate companies, such as Microsoft, Dell, McAfee, and Norton, and told the consumers that they had detected malware that posed an imminent threat to their computers. They directed consumers to a utility area of their computer and falsely claimed it demonstrated the computer was infected.

According to papers the FTC filed with the court, the scammers sought to avoid detection by consumers and law enforcers by using virtual offices that were, in fact, mail-forwarding facilities. The scammers allegedly used 80 different domain names and 130 different phone numbers.

The commission has publicly acknowledged the assistance it received from the Australian Communications and Media Authority, Canadian Radio-Television and Telecommunications Commission, and the UK's Serious Organised Crime agency, as well as from Microsoft and other computer companies.

The FTC cases targeted 14 corporate defendants and 17 individual defendants in the six legal filings.

Liebowitz announced the filing of the international scam case the day after the FTC won a final judgment in a $163 million case against an operation that used computer "scareware" to trick consumers into thinking their systems were infected with malware.

In this particular case, which was filed in 2008, the FTC charged the defendants with scamming more than 1 million consumers using elaborate and technologically sophisticated Internet advertisements. The ads displayed a bogus "system scan" that detected several malicious or otherwise dangerous files on the consumers' computers and urged consumers to buy the defendants' software for $40-$60 to fix their computer.

TECH TRENDS

Mobile Devices Top Gartner's 2013 Strategic Tech Trends List

Gartner's 2013 top-10 IT trends is an evolution of items from previous years, Gartner Fellow David Cearley told *PCweek.com's* Michael Miller. Many of these issues have moved slower than expected, Cearley observed, but they still have the highest potential for significantly affecting enterprises over the next three years.

Mobile devices, mobile apps and HTML5, cloud computing, Internet of Things, and big data top the list for 2013. Their placement on the list may have changed from last year, but the only new trend is personal cloud computing.

Top 10 Strategic Technology Trends for 2013

1. Mobile Devices Battles
2. Mobile Applications and HTML5
3. Personal Cloud
4. Internet of Things
5. Hybrid IT & Cloud Computing
6. Strategic Big Data
7. Actionable Analytics
8. Mainstream In-Memory Computing
9. Integrated Ecosystems
10. Enterprise App Stores

Source: Gartner

HEALTH RECORDS

U.S. Doctors High on Electronic Information Sharing

The final rules for stage 2 of the Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs (also known as the Meaningful Use Program) go into effect in October 2013 for hospitals and January 14, 2014, for practitioners. Stage 2 contains requirements intended to facilitate electronic sharing of health information to support transitions in care.

An October 2012 report on a survey conducted by the Bipartisan Policy Center (BPC) and analyzed by Doctors Helping Doctors Transform Health Care, more than 80% of clinicians surveyed "believe that the electronic exchange of health information across care settings will have a positive impact on improving the quality of patient care, as well as the ability to coordinate care, meet the demands of new care models, and participate in third-party reporting and incentive programs."

The report, "Clinician Perspectives on Electronic Health Information Sharing for Transitions of Care," also shows that more than half (57%) of the respondents believe the electronic exchange of information will actually reduce healthcare costs.

There are some serious obstacles, however, that must first be overcome. Most of the physicians (71%) surveyed consider the lack of interoperability and an exchange infrastructure – and the cost associated with implementing and maintaining that infrastructure – a major barrier to electronic information sharing.

Stage 2 of Meaningful Use attempts to address these concerns by including requirements for the electronic transmission of a summary of care record 10% of the time and at least one successful exchange with a hospital or clinician that uses a different EHR vendor. The goal is to advance interoperability across vendor systems.

Stage 2 also contains standards and certification criteria that were either weak or nonexistent in Stage 1. "Stage 2 standards and certification criteria are more robust, requiring certified EHR technology to receive, display, and transmit considerably more types of data – using standards," explained the BPC in a companion report, "Accelerating Electronic Information Sharing to Improve Quality and Reduce Costs in Health Care."

The 2014 Standards, Implementation Specifications, and Certification Criteria require certified EHR support for data-transport methods and standards that push data. This is in line with clinicians' preferences. According to the clinician survey, the majority of clinicians prefer to receive information they consider "essential" to be pushed to them; the rest they want to be able to access through a query.

BPC added that "the development, coordination, evaluation of, and effective communication and dissemination of implementation guides and specifications that will support the actual use of standards in practice … is crucial."

It offered several recommendations:

- Develop a national strategy and long-term plans for standards and inoperability to support a broad set of healthcare priorities.
- Provide sub-regulatory and explanatory guidance from the federal government to support query access to priority information and transmission of imaging test results.
- Explore principles, policies, standards, and strategies for improving the accuracy of matching using consumer-facilitated approaches.
- Issue comprehensive and clear guidance from the U.S. Department of Health and Human Services on compliance with federal privacy and security laws.

The clinician study and the resulting reports on electronic information sharing in the healthcare sector is part of BPC's Health IT Initiative. Its goal is to identify "real-world examples and best practices that facilitate coordinated, accountable, patient-centered care," and to ensure "that health IT efforts support delivery system and payment reforms shown to improve quality and reduce costs in health care."

PRIVACY

Data Retention vs. Privacy

Australia's proposed data retention laws may conflict with the intent of the national privacy principles, according to international lawyers James Halliday and Sylvia Li from Baker and McKenzie, who raised the concern in an article on *ITnews.com*. They explained that "the data retention laws will make it mandatory for all Australian telcos [telecommunications companies] and ISPs [Internet service providers] to store the non-content usage records of all individuals for up to two years without the consent of the individuals involved."

The Privacy Amendment (Enhancing Privacy Protection) Bill 2012, on the other hand, will "prohibit the use of all personal information for direct marketing, unless exemptions apply."

Halliday and Li contend that the data retention laws do not meet the basic community expectation of privacy provided for in the Privacy Amendment.

WEB

FTC Still on the Google Case

The Federal Trade Commission (FTC) has moved forward in its antitrust investigation into Google, which it began in 2011. This isn't the first antitrust inquiry Google has been involved in, but it does look like it's one that will have a significant impact.

The FTC staff has been investigating whether Google unfairly ranks its search results to favor its own businesses and whether it restrains competition by engaging in exclusive agreements to provide search services to online publishers and other websites. Google has also been accused of charging higher advertising rates to its competitors, making it difficult for other advertisers to compete with Google and its various businesses.

The European Union is looking into these allegations based on complaints it has received from smaller companies

The Washington Post reported the FTC is also looking into whether Google is using its influence in the Android market to discourage smartphone and device makers from using rivals' applications.

GOVERNANCE

New IGRM Version Recognizes Value of Privacy, Security

The Information Governance Reference Model (IGRM) has been updated to include privacy and security as primary functions and stakeholders in the effective governance of information.

The Electronic Discovery Reference Model (EDRM), which published the IGRM, announced the change in the third quarter of 2012, stating the release of IGRM version 3.0 "reflects broad industry support and collaboration across the expert communities of ARMA International and CGOC (Compliance, Governance and Oversight Council)."

The IGRM provides a common, practical framework enabling organizations to establish information governance programs that more effectively deal with the rising volume and diversity of information and the risks, costs, and complications this presents. The model helps facilitate dialogue and coalesce disparate information stakeholders and perspectives across legal, records management, IT, and business organizations.

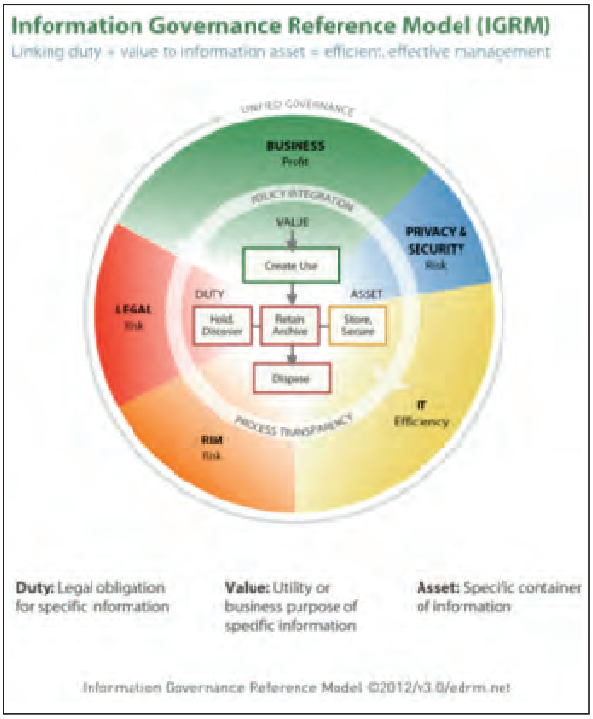
"The Model helps organizations more effectively associate the duties and value of information to information assets through policy integration and process transparency so they can maximize information of value, meet their legal obligations, efficiently manage information and defensibly dispose of it at the right time," explained the EDRM.

Incorporating privacy and security as key stakeholders reflects the increasing importance of privacy and security duties and the efficiencies organizations can achieve when these efforts are more holistically integrated with other essential governance practices and programs.

As the volume and variety of data (e.g., social media, geo-location data, and website tracking data) grow, so do the risks and costs associated with amassing it. Data typically loses its value steadily, yet the costs and risks of managing it increase over time, which inversely means that data without value often costs companies more than data with value.

When information and data are no longer required for business, legal, or regulatory purposes, it must be defensibly disposed. Privacy regulations often require timely disposal of information, and privacy-related litigation is spotlighting weak privacy management process.

"Chief privacy offers must collaborate with their IT, business, records management, and legal counterparts," summarizes the EDRM. The IGRM provides an integrated process and policy framework for that collaboration.


Information Governance Reference Model (IGRM)

Linking duty + value to information asset = efficient, effective management

Duty: Legal obligation for specific information

Value: Utility or business purpose of specific information

Asset: Specific container of information

Information Governance Reference Model ©2012/v3.0/edrm.net

DATA SECURITY

New Zealand Investigates Alleged Breach

Freelance journalist Keith Ng announced on his blog on October 15, 2012, that he had accessed thousands of files on the New Zealand Ministry of Social Development's national accounting server. Some of the invoices stored on the server included private information.

The ministry closed down kiosks at the office through which the journalist was able to access the files, then it engaged an independent security expert to investigate the breach.

The journalist accessed four other servers, but he was not able to gain private information from them. The journalist has cooperated with the ministry rather than release the information.

The ministy's chief executive said the ministry does not know if other breaches had occurred, but he confirmed that no client files were accessed. Once it is certain what information was accessed, the ministry will decide accordingly whether any clients needed to be advised.

CLOUD COMPUTING

Cloud Use Can Complicate E-Discovery

As is true in most cases, people tend to get what they pay for in cloud computing. And, those using free, consumer-grade cloud services for their corporate data may discover that what they are paying nothing for is likely to make e-discovery much more difficult.

In an October 1, 2012, article, *zdnet.com* published the result of its interviews with various analysts and industry veterans about how the unchecked use of cloud computing is complicating e-discovery efforts. The focus was on the "unruly use and management" of cloud services, exemplified by organizations choosing cloud service providers (CSPs) that have no understanding of compliance requirements and no real plans for backup and orderly retrieval.

Organizations that use consumer-grade cloud services for their corporate data are especially vulnerable to legal complications.

Additionally, when employees store data on these consumer-grade sites and there are no records that track the action, the data may be undiscoverable if that employee leaves the organization.

Analyst Barry Murphy of the E-Discovery Journal Group agrees with the idea of due diligence, specifying that organizations must work closely with CSPs on the e-discovery details and on defining the requirements for defensible collection and preservation.

ARMA International has published a number of resources to guide the decision-making and implementation of cloud computing into an organization's technology infrastructure.

For example, *Outsourcing Records Storage to the Cloud* highlights a number of factors that should be considered when moving records storage to the cloud, including suggestions for how to mitigate legal risk. Here are a few of the key points excerpted from the book (which is available for purchase at *www.arma.org/bookstore*):

- Establish clear rules for employee use of corporate information systems that include use of systems outsourced to the cloud, including access to the employees' personal accounts.
- Establish ownership of data and include language in any cloud provider's service contracts that addresses the organization's ownership.
- Establish the allocation of liability for loss or wrongful disclosure of data, preferably as part of the contract.
- Establish a mechanism with the cloud provider for communicating and implementing legal holds. Make it clear in the service contract what the cloud provider's obligation is for implementing and, possibly, managing legal holds.

These factors must be addressed in the service level agreement with the cloud provider, the guideline stresses.

The fall 2012 issue of ARMA International's *Hot Topic*, "The Shift in Information Control: E-Discovery of Information in the Cloud and on Mobile Devices," specifically addresses the records and information management, legal, and technology issues surrounding this topic. It is available as a free PDF download from *www.arma.org/publications/hottopic.*

DATA SECURITY

Big Data Working Group Tackles Privacy and Security

Just over two months after its launch, the Cloud Security Alliance's (CSA) Big Data Working Group published in November 2012 its initial list of the "Top Ten Big Data Security and Privacy Challenges." After interviewing CSA members and security practitioner-oriented trade journals, the working group determined that these challenges are:

1. Secure computations in distributed programming frameworks
2. Security best practices for non-relational data stores
3. Secure data storage and transactions logs
4. End-point input validation/filtering
5. Real-time security/compliance monitoring
6. Scalable and composable privacy-preserving data mining and analytics
7. Cryptographically enforced access control and secure communication
8. Granular access control
9. Granular audits
10. Data provenance

The working group's report, which is available at *cloudsecurityalliance.org/research/big-data/*, describes these challenges and narrates use cases for each.

Formed in August 2012, CSA's Big Data Working Group is tasked with providing specific actionable information and creating standards for big data security and privacy.

According to a Fujitsu press release, the working group will focus on six themes:

- Big data-scale crypto
- Cloud infrastructure
- Data analytics for security
- Framework and taxonomy
- Policy and governance
- Privacy

"Everyday 2.5 quintillion bytes of data are being created resulting in a myriad number of data security and cloud-computing security concerns," said Sre-eranga Rajan, director of Software Systems Innovation at Fujitsu Laboratories of America and a co-chair of the working group. "By collaborating as a global community of thought leaders and researchers, we are not only looking to help the industry overcome these challenges but also to leverage new opportunities for the monitoring and detection of security threats enabled by big data."

Along with Rajan, Neel Sundaresan of eBay and Wilco Van Grinkel of Verizon co-chair the working group.

Those interested in learning more about the group's activities or in joining the group should visit *cloudsecurityalliance.org/research/big-datal*.

LEGAL

Courts Broaden Liability for Data Theft

U.S. federal courts are widening their definition of the damages caused by data breaches, according to an October 29 article on *csoonline.com*. Whereas courts previously dismissed these lawsuits unless the victims could show specific damages, judges increasing are now awarding them class-action status – a trend that puts organizations at greater risk of huge payouts.

These payouts can be significant. A study conducted by the Temple University Beasley School of Law and published in early 2012, "Empirical Analysis of Data Breach Litigation," found that although the mean value of settlements awarded per plaintiff was just $2,500, the mean amount paid for attorney fees was $1.2 million.

To mitigate damages, law firm Pepper Hamilton suggests that organizations fortify their technical and physical security, which will not only help prevent breaches, but will demonstrate a "best practices" approach that can influence the courts positively. The law firm also advises organizations not to link information to individuals and to have an effective notification policy in place.

PRIVACY

Google's Regulatory Woes Continue in EU, U.S.

Google has been under fire in Europe regarding privacy issues for quite some time. In mid-October, France's privacy rights regulator ruled that Google's new privacy policy violates the European Union's (EU) data protection rules. According to *BusinessWeek.com*, the problem was that Google did not set a "limit concerning the scope of the collection and the potential uses of the personal data" or give users adequate means to opt out. The search giant was given three to four months to change the policy or be fined.

Google maintained that it was confident its privacy notices "respect European law."

Although this action was taken by France alone, other countries are expected to follow suit. EU authorities asked the French regulator, CNIL, to conduct the review. *BusinessWeek.com* reported that European national regulators and data protection authorities in Australia, Canada, and several Asian countries reviewed CNIL's findings before they were presented to the EU.

Jeffrey Child, associate professor of communications and privacy expert at Kent State University, told *eweek.com* that any changes Google and Microsoft have to make to meet EU requirements could eventually be felt in the United States.

In the meantime, French media petitioned the government to require Google and other search engines to pay for their content. Agence France-Presse (AFP), a French news agency, reported that Google sent a letter to several French ministerial officers warning that such a move could force it to exclude French media sites from its search results. Google added that requiring search media to pay for displaying links to content would threaten Google's existence and be harmful to the Internet.

Google said it "redirects four billion 'clicks' per month to French media sites." The media argue that readers aren't paying for subscriptions because they can get so much content free on the Internet.

French Culture Minister Aurelie Filippetti told AFP she was surprised by the tone of Google's letter. "You don't deal with a democratically elected government with threats," she said.

Media association IPG criticized Google's attitude, contending that "the objective of discussions should be finding an acceptable compromise that would recognize the value [the media] bring to search engines and would help the further development of [the media and search engines]," AFP reported.

None of this plays well at a time when Google is under the microscope in the United States and Europe for alleged anti-trust violations. Privacy issues don't typically play a role in antitrust enforcement, but in Google's case they do.

"The issue of privacy is absolutely connected to antitrust and competition," Nick Pickles, a lawyer and director of Big Brother Watch, a British advocacy group for civil liberties and privacy protections, told *BusinesWeek.com*. He said that Google's ability to collect data from multiple services gives it an unfair advantage in competing for advertisers.

Microsoft apparently learned from the Google experience when it introduced its new privacy policy complete with an opt-out. Instead, the EU was scrutinizing Microsoft for allegedly violating a 2009 commitment to allow European Windows users to have a choice of web browsers. The agreement struck in 2009 required that Microsoft offer a screen of browser choices to European Windows users through 2014. European regulators weren't pleased when Microsoft failed to live up to its end of the bargain. Microsoft has since admitted that it had "accidentally violated" the earlier agreement and would make corrections. **END**