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

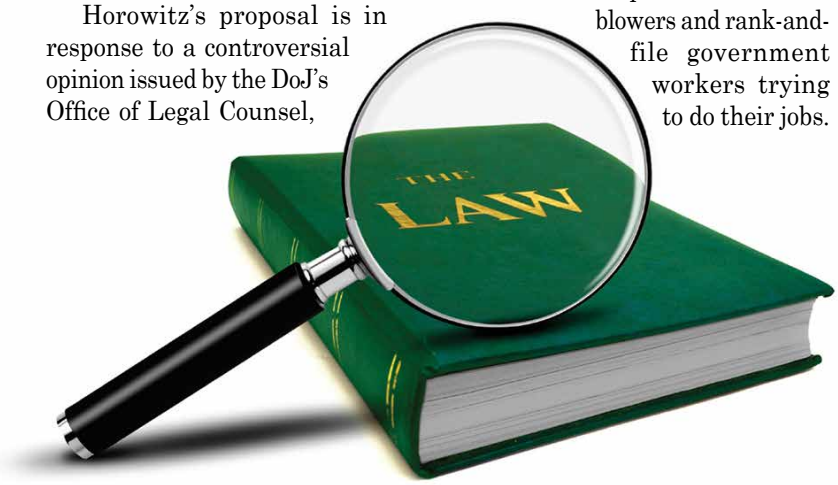
U.S. Department of Justice (DoJ) Inspector General Michael Horowitz has asked Congress to amend the 1978 Inspector General Act to specify that the only information a federal agency can withhold from its inspector general (IG) records that Congress specifically states it does not want watchdogs to see,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

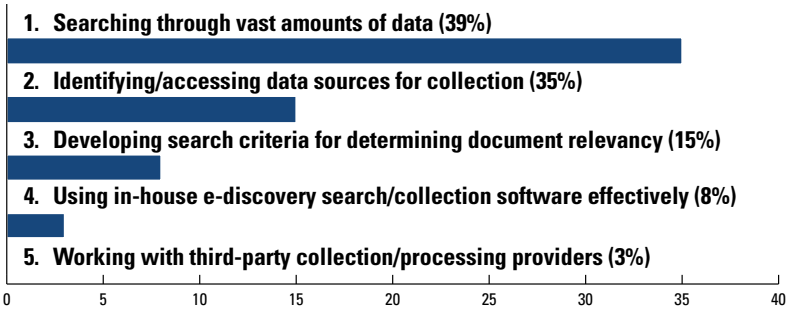
To ease the challenges associated with the e-discovery identification process, the survey advises organizations to take a more proactive approach to managing their data infrastructure, with an eye toward e-discovery optimization.

"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

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**