GOVERNMENT RECORDS

Feds' Budgets Out-Paced by Volume of Information to Manage

U.S. federal agencies – and their budgets – are being overwhelmed by the amount of information they must manage, according to a recent study of federal records managers and finance professionals from MeriTalk and Iron Mountain.

Published in March, the results of the online survey of 100 federal records managers and 100 federal finance professionals conducted in September 2012, "Federal Records Management: Navigating the Storm," showed that each federal agency spends an average of $34.4 million a year on records management, $5 million – or about 17% – more than budgeted.

According to the survey report, records management spending will likely more than double to $84.1 million by 2015 because of a projected 144% increase in records per agency.

Some of the main reasons for the overspending are:

- Too many records – a single federal agency currently manages about 209 million records, which totals 8.4 billion records government-wide.
- Runaway information growth – the number of records per agency is expected to grow to 511 million by 2015.
- Multiple information types – records are increasingly being created in more varied formats and sources.

Add to this the race to comply with the Presidential Directive on Managing Government Records, which instructs agencies to modernize their records management policies, predominantly by digitizing records and establishing a new infrastructure to minimize costs and promote openness and accountability.

The survey respondents said additional training, more funding, and greater support for records management from their agencies' leadership would enable them to meet the objectives of the directive. The federal finance professionals estimated that focusing on these three factors would allow them to save an estimated 24% of their records management budgets; the records management professionals estimated savings of up to 36%.

CYBERSECURITY

Reuters Social Media Editor Charged with Hacking

Federal charges were filed in March against Matthew Keys, a deputy social media editor for Reuters, for allegedly conspiring to hack the *Los Angeles Times* website in 2010.

Keys is accused of giving the website's password to the notorious hacker group "Anonymous" through its chat room, encouraging the group to breach the newspaper's website. One of the hackers followed up and altered an archived article. The *Los Angeles Times* is owned by the Tribune Co., which also owns a Sacramento television station at which Keys used to work as a web producer.

The U.S. Justice Department charged Keys with one count each of transmitting information to damage a protected computer, attempted transmission, and conspiracy. If convicted, Keys could face up to 10 years in prison on two of the counts, five years on a third, and a fine of $250,000 for each count.

As of press time, Keys had not yet been arraigned.

BIG DATA

With Big Data Comes Big Privacy Concerns

The potential of big data is huge. It opens the door to smarter decision making and greater advances in every field – provided it is effectively managed and mined, of course.

That potential in turn raises serious concerns around protecting privacy.

Last year, the World Economic Forum conducted a series of workshops attended by government officials, privacy advocates, and business executives from the United States, Europe, Asia, and the Middle East. The discussions centered on three major areas:

- Protection and security
- Accountability
- Rights and responsibilities for using personal data

Out of those workshops came the recently published report "Unlocking the Value of Personal Data: From Collection to Usage." The report, which was prepared in collaboration with The Boston Consulting Group, recommends an approach that shifts focus away from governing the usage of data to governing the data itself; recognizes the importance of context because there is no black and white, only shades of gray; offers new ways to engage individuals and help them understand how their information is to be used; and provides them with the tools to make real choices based on "clear value exchange."

For such an approach to be successful, the participants agreed there is a need 1) for principles to be updated and enforceable in a hyperconnected world; 2) to include technology as part of the solution – allowing permissions to flow with the data and ensuring accountability at scale; and 3) to demonstrate how a usage, contextual model can work in specific, real-world application.

EIM

Enterprise Info Management Critical, But Not Priority

Although business executives are generally well aware that information is an asset and that poorly managed information can be a potential legal and competitive liability, making enterprise information management (EIM) a reality is another story.

According to the OpenText white paper "Unleashing the Power of Information," a recent IDG Research survey of nearly 140 chief information officers (CIOs) and other IT and business executives showed that the majority believe in the benefits EIM can deliver, such as better data access and analysis, reduced costs, and better alignment of IT with business objectives. Yet only 67% of the organizations represented said they treat EIM as a strategic priority.

Part of the challenge is the overwhelming volume of unstructured data organizations are generating. According to the white paper, it is estimated that up to 80% of the information produced in organizations today is found in documents, e-mails, social media, slide presentations, videos, and other unstructured data formats. This information is often mission-critical and resides in a number of different locations and devices.

"Given the variability and complexity of today's information landscape," IDG wrote, "many companies find themselves dealing with distinct and nonintegrated information silos. Information in these silos is often disorganized, dated or duplicated, and data that could identify key trends or deliver critical insight is often buried under mountains of insignificant information."

That's why 80% of the survey respondents said a comprehensive EIM strategy is critical or, at least, very important to their organizations. Unfortunately, this recognition of the value of that information has not translated into policy. Organizations are not making EIM an institutional priority – even though it directly affects their ability to meet their top business objective: increasing business productivity, according to the IDG report.

BIG DATA

Report Examines Trends in Big Data

It's been talked about and written about at great length, but to what extent are companies actually addressing big data today?

A Tata Consultancy Services (TCS) survey of 1,217 companies in nine countries in the United States, Europe, Asia-Pacific, and Latin America that was completed in January 2013 found that more than half (53%) had undertaken big data initiatives in 2012. The countries with the highest percentage of companies with initiatives were India, Mexico, the United States, and the United Kingdom. Japan, The Netherlands, and Australia had the fewest percentage reporting initiatives in place.

The level of investment in big data initiatives varied greatly, the report found: 15% of the companies with initiatives spent at least $100 million per company on those initiatives last year; 7% invested at least $500 million. On the other hand, nearly one-quarter (24%) spent less than $2.5 million apiece. The industries that spent the most on the initiatives were telecommunications, travel-related, high tech, and banking. Life sciences, retail, and energy/resources companies spent the least.

More than half (55%) of the investments in big data initiatives went toward four business functions that generate and maintain revenue: sales (15%), marketing (15%), customer service (13%), and research and development/product development (11%). Only about a quarter (24%) of the investment went to IT (11%), finance (8%), and human resources (5%).

Forty-three percent of the companies that have invested in initiatives anticipated a return on investment (ROI) of more than 25% in 2015. The business functions expecting the greatest ROI were not sales and marketing, as might be expected, given that they received 30% of the funding, but rather logistics and finance, which received only 14% of the funding.

Companies reported that the biggest obstacles to getting business value from big data were as much cultural as they were technological. More specifically, it was the challenge of getting business units to share information across organizational silos. A close second was a technological issue: dealing with the volume, velocity, and variety of data. The third was determining which data to use for different business decisions.

"By applying Big Data in the right places in the organization, centralizing and nurturing talent, and building bridges to functional managers who need data-driven insights to make superior decisions, companies will greatly raise the odds of keeping up in a world in which digital data-driven decisions become the norm, not the exception," the TCS report concluded.

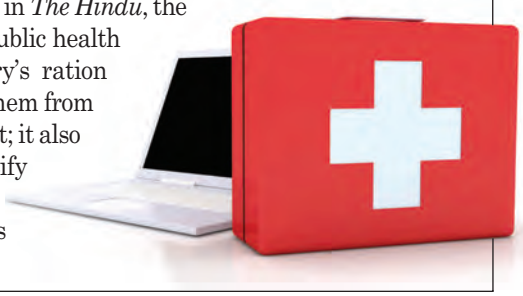
EHR

India Launches Electronic Health Records Program

The Jawaharla Institute of Postgraduate Medical Education and Research (JIPMER) rolled out the "Partners in Prevention Programme" for the police department in Puducherry (India) in mid-March as the first step in the country's move toward electronic health records.

Medical records of the policemen who are screened at JIPMER will be maintained online in a database accessible from anywhere in the world. The patients are issued a "Meddrecords Online Card" with a unique identification number and barcode, which will enable them to update daily blood pressure, blood sugar level, family history, and other details that their doctors could access as needed.

According to an article in *The Hindu*, the plan is to integrate the public health records with the country's ration card, which would help them from a public health standpoint; it also would help them identify those who had completed their immunization cycles and various screenings.



PRIVACY

U.S. Electronic Communications Privacy Act Amendments Proposed

When the U.S. Electronic Communications Privacy Act was introduced in 1986, no one could have foreseen how the Internet and mobile communications technology would transform the world. To bring the law up to date, senators Tom Leahy (D-Vt.) and Mike Lee (R-Utah) introduced a bill in mid-March that they believe will strengthen the privacy protections for e-mail and other electronic communications.

Leahy explained that the bill strives "to improve Americans' digital privacy rights, while also promoting new technologies – like cloud computing – and accommodating the legitimate needs of law enforcement."

The bill requires law enforcement to obtain a search warrant based on probable cause to access e-mail and other electronic communications' content requested from a third-party provider. There are "balanced exceptions" to this requirement in emergency circumstances and to protect national security under current law.

The bill would further require law enforcement to "promptly notify" any individual whose e-mail content has been accessed. The government can ask the court for a temporary delay in notifying the individual, however.

The bill would not affect the government's ability to use administrative, civil discovery, and grand jury subpoena to access corporate e-mail and other electronic communications directly from a company.

EHR

DoD, VA Pullback on EHRs Draws Fire

Early this year the U.S. departments of Defense (DoD) and the Veterans Affairs (VA) announced they were scaling back their plans to create a single shared electronic health records (EHRs) system that would manage service members' and veterans' medical records from recruitment to grave. They decided, instead, to build their system on existing IT architecture and programs, pointing out that it would be more cost- and time-efficient.

The decision drew fire from the top lawmakers on the Senate and House Veterans' Affairs committees, which had charged the agencies in 2008 with creating and deploying an integrated health records system by 2017 at a cost of about $4 billion.

Unfortunately, the project has reportedly met technology challenges and delays. The new approach will enable the departments to exchange real-time data by the end of the year and allow patients online access to their medical records by summer. It is also expected to save hundreds of millions of dollars, according to DoD Deputy Chief Management Officer Elizabeth McGrath, according to an article in *Federal Times*. The endeavor has already cost an estimated $1 billion.

House Veterans' Affairs Committee Chairman Rep. Jeff Miller (R-Fla.) was less optimistic. "Previous attempts by DoD and VA to use disparate computer systems to produce universal electronic health records have failed and unfortunately it appears they are repeating past mistakes," the *Federal Times* reported.

The new system is being built with the VA's VistA EHR as its core system and a more current core EHR system. VistA system has generally been considered a strong EHR platform, but there is concern over its age and its ability to keep pace with newer systems.

CLOUD

The Best Countries for Cloud Computing

Japan, Australia, the United States, Germany, and Singapore are the top five countries for cloud computing based on their policy environment, according to the BSA | The Software Alliance (BSA) 2013 Global Cloud Computing Scorecard.

The study rated 24 countries (which together account for 80% of the global information and communications technology market) based on their policies in seven areas:

- Privacy
- Security
- Cybercrime
- Intellectual property rights
- Data portability across borders
- Free trade promotion
- IT infrastructure

Singapore showed the most improvement (up five places from last year) due largely to its introduction of a modern, balanced privacy regime. A late-comer to privacy regulation, Singapore passed its Personal Data Protection Act in October 2012.

"That timing has helped the country develop a regulatory framework that picks and chooses from the best parts of the European Union and Asia-Pacific Economic Cooperation approaches to privacy regulation and avoids much of the excessive legalese and administrative complexity found in other country's laws," observed BSA in its report.

Singapore took a broad, principles-based approach to privacy protection. It contains short sections on notice, consent, security, access, correction, and data retention, all of which are based on international standards.

Brazil improved its ranking by finally passing cybercrime legislation last November. That change alone moved it up two spaces and out of last place. That distinction now belongs to Vietnam.

Malaysia moved out of the group of countries still striving toward cloud-readiness by making a range of changes in cybercrime and intellectual property laws and improvements in efforts to improve digital trade.

The United States moved up one spot, not through major policy improvements, but through advances in standards development for cloud computing and infrastructure improvements.

Less positively, there continued to be efforts to keep data within national borders. Germany was cited in last year's report for some overly restrictive legal interpretations that would keep some data within its borders.

This year, Indonesia undermined any advantages it may have made from improving its privacy law by introducing regulations that would force some providers to establish local data centers and hire local staff.

In general, Indonesia, Korea, and Vietnam are taking steps to actually unplug from the global cloud. This works against the goal of making data more accessible globally.

CLOUD

Thailand Takes First Step Toward G-Cloud Computing

Thailand's Information and Communication Technology (ICT) Ministry and Electronic Government Agency (EGA) and Cloud Security Alliance (CSA) recently signed a memorandum of intent (MOI) to establish the official CSA office in Thailand. *The Nation* reported that EGA will handle the human resources budget issues to support CSA's activities.

"This effort aims to promote security system[s] for cloud computing among users. CSA will support all activities and provide know-hows," said Nattapong Seetavorarat, advisor to the ICT minister. The cloud computing system, especially G-Cloud, will build upon the GIN system currently in place. The system "can be scalable to Super GIN for more network expansion to other areas, availability of government data with accessibility for related agencies and bodies."

The MOI was signed during the ASEAN CSA Summit 2013. Topics discussed during the two-day event included cloud security, challenges to cloud adoption, public cloud, cloud for education, cloud businesses, and applications of cloud for national crisis management.

DATA SECURITY

Retailer Sues Visa over Data Breach

The Payment Card Industry's Data Security Standards (PCI DSS) are being put to the test in a suit filed in early March by specialty sports apparel retailer Genesco against Visa. Genesco is seeking nearly $13.3 million in fines that Visa assessed following a breach of Genesco's systems that may have resulted in fraudulent transactions.

According to *Wired* magazine, this is the first known case challenging the PCI DSS. The regulations require merchants that handle credit and debit card data to follow certain security practices or face fines from the credit card industry. Visa fined Genesco $13.3 million for noncompliance to the PCI standards after Genesco announced it had been hacked back in 2010.

In the filing, Genesco states that although it found packet-sniffing software on its network at that time, there was no forensic evidence of any card data having been stolen. Genesco alleges it was never out of compliance with PCI DSS regulations and, therefore, should not have been fined.

The PCI standards state that merchants are not to store card data, but may store some parts of the data, if necessary, as long as it's encrypted.

"Visa is not the only card company to go after Genesco and its banks. MasterCard did as well," reported *Wired* senior reporter Kim Zetter. "The two companies combined imposed $15.6 million in fines and assessments, but Genesco has so far only sued Visa."

Genesco is not the first company to be fined, but it is the first to fight back against the credit card companies. In Utah, a restaurant reportedly has sued its bank for wrongfully seizing money from its merchant bank account to pay credit card fines. Visa and MasterCard levied the fines after alleging the restaurant had failed to secure its network, leading to a data breach that resulted in fraudulent charges on customers' credit cards. That case is ongoing.

EHR

Electronic Health Records: How Transparent Should They Be?

How much access should patients have to their electronic health records? According to an Accenture study completed in December 2012, most (49%) physicians favor transparency, but only 21% allow online access.

"Many physicians believe that patients should take an active role in managing their own health information, because it fosters personal responsibility and ownership and enables both the patient and doctor to track progress outside scheduled appointments," said Mark Knickrehm, global managing director of Accenture Health. "Several U.S. health systems have proven that the benefits outweigh the risks in allowing patients open access to their health records."

The Accenture study surveyed 3,700 physicians in the United States, England, Spain, France, Germany, and Singapore. U.S. doctors were marginally more open to allowing patients to update their records online. There was a clear consensus among the respondents that, generally, patients should be allowed to update all or some of their information, from demographic details to lab test results. More than half of the responding physicians favored providing update privileges.

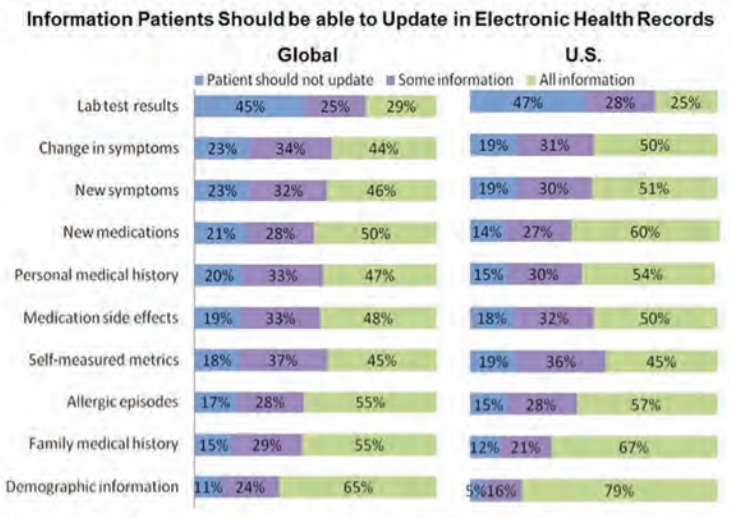


Figure 2: U.S. doctors were the most open toward patients updating the information in their electronic health records, according to Accenture's eight country survey of 3,700 doctors

Source: Accenture Doctors Survey

CYBERSECURITY

European Commission Launches Cybersecurity Strategy

The European Commission (EC) and the High Representative of the European Union for Foreign Affairs and Security Policy recently introduced a cybersecurity strategy for the European Union (EU). Part of the strategy included a directive on network and information security, a draft of which was released in conjunction with the strategy.

The strategy aims to clarify the principles the EC believes should guide the cybersecurity policy in the EU and internationally. Those principles are:

- The EU's core values apply in the digital world the same as in the physical.
- Protection of fundamental rights, freedom of expression, personal data, and privacy
- Access for all
- Democratic and efficient multistakeholder governance
- A shared responsibility to ensure security

It is predominantly the task of member states to deal with cybersecurity challenges; however, the EC strategy established five strategic priorities with both short- and long-term activities for the government, industry, and member states. Those priorities are:

1. Achieving cyber resilience
2. Reducing cybercime drastically
3. Developing cyberdefense policy and capabilities related to the Common Security and Defense Policy
4. Developing the industrial and technological resources for cybersecurity
5. Establishing a coherent international cyberspace policy for the EU and promoting the core EU values

On a related note, proposed changes to the European Data Protection Directive introduced about the same time the EC launched the cybersecurity strategy have come under heavy fire. *Wired.co.uk* reported that UK Information Commissioners past and present denounced the changes as being bad for business, and they said they should be thrown out.

Among other things, the EU directive is being described as "too prescriptive in terms of its administrative detail."

E-DISCOVERY

ISO Starts Committee on E-Discovery

The International Organization for Standardization (ISO) recently established a committee to develop standards for e-discovery processes. Its goal is to define procedures for technology companies, discovery providers, and their clients to follow when handling electronically stored information.

"We're not trying to impose requirements on lawyers or judges. That's not the intention of the activity," Hitachi Data Systems' Eric Hibbard, co-editor of the project and international representative on a U.S. contingent to ISO, told *Law.com*. "It's really intended to help them sort through some of the technology issues that are really nebulous."

The standards will refer to product auditing and will describe how discovery services and software should operate. They will also cite ISO 9001 quality control procedures, which means e-discovery companies could then achieve ISO 9001 certification and promote their products as being ISO 9001-compliant.

Other organizations, such as the American Bankers Association, are also working on legal technology standards. Reactions to plans to develop standards in this area have been mixed. While many fully support it, others think it premature.

"A lot of us think that standard-setting for an area in which the technology has not yet matured is a little bit premature," Steven Teppler, an attorney and data security expert, told *Law.com*.

DATA SECURITY

Keep Your Data from Walking Out the Door

The consensus in the industry is that regardless of how you feel about the bring your own device (BYOD) trend, you can't afford to ignore it.

A 2012 Nielsen study found that almost half (49.7%) of U.S. mobile subscribers own smartphones. According to Nielsen, this is an increase of 38% over 2011. It's a safe bet to expect a large percentage will want to connect to their company's wireless network. They'll forward documents to their personal accounts to read at home or while traveling.

With this increased access come increased security risks. Potentially sensitive corporate data is being sent to less-secure sites.

In a recent *BizTech* article, IBE.net co-founder Richard Minney suggested an alternate BYOD strategy in which the company actively allows BYOD, specifies what data can and cannot be transferred to and stored on those devices, and installs an app or two to provide some level of protection.

He added that the company may also want to insist that all devices used for work purposes be registered with the company's mobile device management (MDM) solution, which applies policy and security management capabilities across many operating systems or platforms. These applications are typically modeled after the client server architecture where software is centralized on a back-end server and a client component resides on the end system device.

Another option is for the company to allow employees to choose the devices they want, but the company supplies and owns them.

CLOUD

Cloud Adoption in India Grows

A recent report by ARC Advisory Group shows that the cloud market growth rate in India is outpacing the global market by a wide margin. Almost all the IT vendors in India have cloud offerings, as do many global players.

The report cites the country's growing IT industry, currently valued at $100 billion. The industry's rapid growth is due largely to the demand from global companies. But even micro, small, and medium businesses are turning to the cloud to reduce the cost of ownership.

CYBERSECURITY

Report Finds Data Breaches Mainly Involve Outsourced IT

A recent report published by Trustwave revealed that 64% of security breaches it analyzed last year involved IT outsourcing providers. The findings drive home the need for enterprises to be more aware of the security measures outsourcing providers have in place before contracting with them.

"We are not saying outsourcing is bad," explained John Yeo, director of Trustwave's SpiderLabs unit in Europe, the Middle East, and Africa, "but what we are saying is that there may have been a lack of due diligence in the selecting of outsourcing providers."

The UK's Data Protection Act requires data controllers to take "appropriate technical and organizational measures" to avoid "unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

Some feel more clarity is needed from regulators as to what sort of security standards can be considered as compliant with the Data Protection Act. Also, too many senior business executives lack sufficient knowledge or understanding of cybersecurity risks.

Other trends revealed in the Trustwave report include:

- Businesses are getting slower at containing cyber breach incidents, taking an average 210 days in 2012 compared to 175 days in 2011.
- Businesses tend to rely on third parties to tell them they've been hacked: 24% detected the breach themselves, while 48% were discovered by regulatory bodies and 25% by law enforcement.
- There were 400% more samples of mobile malware affecting the Android operating system last year than in 2011. Yeo said the company had not found a case where a smartphone was being used to hack a corporate network, although it could happen and may already have happened.

ELECTRONIC RECORDS

CIOs' Top Priorities for 2013

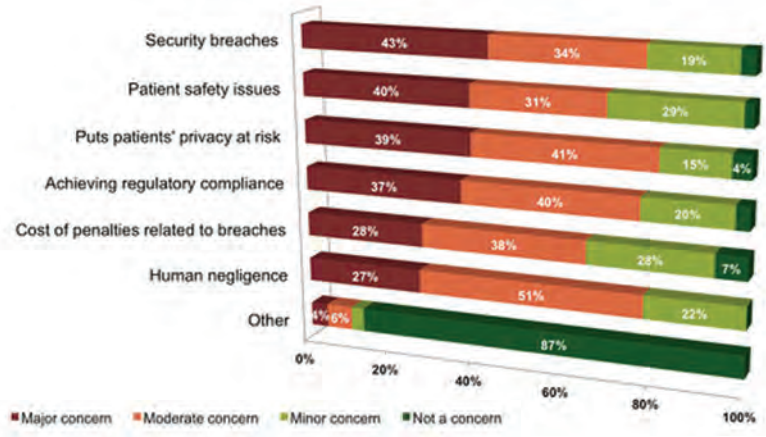
Ask 100 healthcare CIOs and senior IT executives what their top priorities are in 2013 and you'll hear network security issues, IT infrastructure upgrades, and electronic health records (EHRs) implementation. Those were the findings of an independent research study by Level 3 Communications.

Those surveyed were less inclined to focus on mobile-enabled healthcare (mHealth) and slow to adopt cloud computing.

Other findings include:

- 56% were only "somewhat confident" in their ability to prevent a privacy or security breach on their network.
- 80% agree the EHR-based systems will improve patient care.
- More than 60% think EHR and "meaningful use" mandates are a "good idea" to support better quality patient care.
- 76% plan to upgrade their network infrastructure in the next two years.

EXHIBIT 3:
Possible Security and Compliance Concerns EHRs



Source: Level 3 Communications

HIPAA

HIPAA Final Rule Tightens Data Security Requirements

On March 26, the final rule to the Health Insurance Portability and Accountability Act (HIPAA) went into effect, ending the more than three-year effort to overhaul the provisions of the 1996 law. Most of the changes were required by the 2009 HI TECH Act, which incentivized the implementation and use of electronic health records and prompted the development of standards, implementation specifications, and certification criteria for the exchange and use of electronic health information.

The new rule expanded the definition of "business associates," requiring more entities to take a more proactive role in complying with HIPAA. Previously, the law required healthcare providers and other "covered entities" to contractually require that any organization that handles protected heath information (PHI) on behalf of the covered entity (business associate) also to comply with HIPAA.

Under the new rule, the business associate must take full responsibility for ensuring it complies with HIPAA's data security and privacy rules. This means that business associates will also be subject to annual civil penalties for each HIPAA violation, which could be as much as $1.5 million per violation.

Breach notification requirements were also addressed in the new rule. The proposed rule defined a data security breach as the "acquisition, access, use, or disclosure of [PHI] in a manner not permitted [by the Privacy Rule] which compromises the security or privacy of the [PHI]." It went on to say the standard should be whether there was a "significant risk of financial, reputational, or other harm to the individual."

The final rule, however, requires that the entity trying to avoid breach notification obligations conduct a risk assessment that considers the following:

1. The nature and extent of the PHI involved and how easily it is or could become identifiable
2. The unauthorized person who accessed the PHI
3. Whether the PHI was actually acquired or viewed
4. Whether and to what extent the risk to the PHI has been mitigated

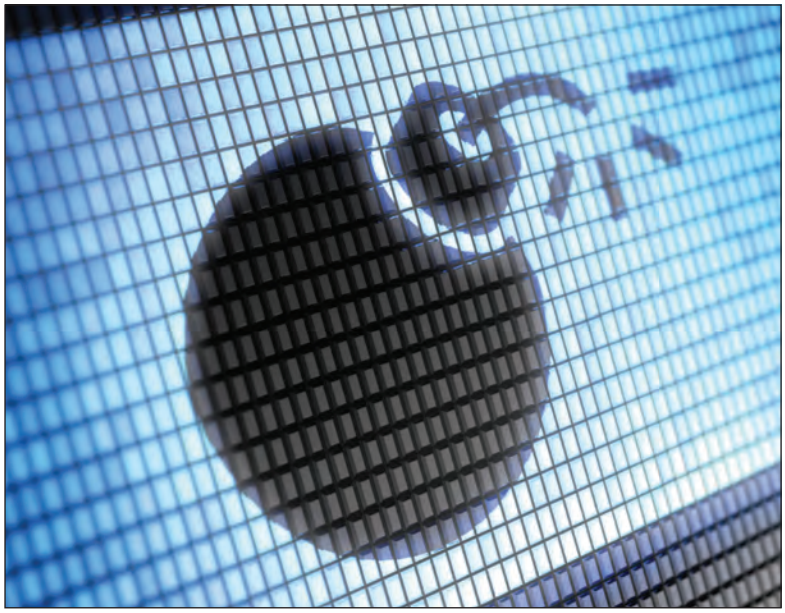
If it can be shown that there was a low probability that the protected information was compromised, it would not be considered a breach. If that can't be proved, the breach notification requirements must be met.

The other area addressed by the final rule limits the sale of PHI for marketing purposes. Bottom line is that protected information may not be sold or used without the individual's consent. Additionally, the covered entity or business associate must disclose the nature and extent of its relationship with the third party.

The compliance deadline for the final rule is September 23. Contracts entered into before January 25, 2013, that complied with the previous HIPAA Data Security and Privacy Rules will be considered compliant until September 22, 2014, as long as the contracts have not been renewed or modified during the grandfathering period.

CYBERSECURITY

Preventing 9/11 in the Cyber World



The evidence that cyber threats are very real and growing is ubiquitous. Earlier this year, U.S. Department of Homeland Security (DHS) Secretary Janet Napolitano warned Congress that a "cyber 9/11" could be imminent and strongly urged lawmakers to pass legislation governing cybersecurity, which it failed to do last year.

President Obama made it clear that cybersecurity is an issue to be taken seriously by signing an executive order that directs the National Institute of Standards and Technology to develop cybersecurity performance standards and methods to reduce risks to the country's critical infrastructure (CI). Among other things, it also directs DHS and agencies to proactively encourage CI owners and operators to voluntarily adopt the standards.

Given the increased volume and strategic nature of cyberattacks, many are convinced they are state-sponsored, and many are pointing fingers at China as the origin of the most sophisticated hackers. It's becoming a potentially lethal weapon of modern warfare.

For example, Team Cymru, a Florida-based Internet security firm, recently revealed to *The Verge* that its analysts have uncovered a massive overseas hacking operation in which one terabyte of data is being stolen on a daily basis.

A study released by the American computer security firm Mandiant detailed that company's efforts to track down a group of "cyber commandos" responsible for hacking the networks of hundreds of American companies over several years to steal trade secrets. Mandiant traced members of the group back to a Shanghai-based military unit. The claim is supported by reports from other security firms and all 16 of the U.S. intelligence agencies, according to the *New York Times*.

The group in question, dubbed "Comment Crew" by some of its U.S. victims, has allegedly stolen terabytes of data from companies such as Coca-Cola and reportedly is focusing increasingly on companies involved in the U.S.'s CI, its electrical power grid, gas lines, and waterworks.

China's government has repeatedly denied that it has engaged in computer hacking, stating that it has been the victim of such attacks, as well. Chinese officials claimed that they experienced, on average, 144,000 cyberattacks per month against its military sites in 2012. They blame the United States for almost two-thirds (63%) of them, saying that there are many hacking groups inside the United States as well.

The war of words between the two countries escalated when the White House warned China to end its campaign of cyberespionage against the United States or risk derailing efforts to build stronger ties between the two countries. China responded by agreeing to enter into dialogue with the United States about cybersecurity.

In the meantime, tension continues to build around the issue. In late March, attention shifted to Korea when South Korean banks and top television broadcasters were simultaneously paralyzed by a cyberattack. Speculation at the time was that North Korea was involved in the attack. The network paralysis took place a few days after North Korea accused South Korea and the United States of a cyberattack that shut down the country's websites for two days.

"This needs to be a wake-up call. This can happen anywhere," James Barnett, former chief of public safety and homeland security for the U.S. Federal Communications Commission, told Fox News following the attack on South Korean networks.

E-DISCOVERY

Information Governance Key to Containing E-Discovery Costs

As the volume of information generated by enterprises today continues to grow exponentially, so do the potential costs of e-discovery.

"One of the best ways to avoid excess costs of discovery is a reasonable dialogue with the other side," Magistrate Judge Andrew Peck, of the Southern District of New York, recently told a LegalTech New York audience.

Senior Judge Michael Baylson, of the U.S. District Court for the Eastern District of Pennsylvania, agreed, pointing out that "'I don't want to cooperate' may be a legitimate strategy, but it's going to cost them money in the long run."

Peck added that IT is usually the best source of reliable information when it comes to estimating what it will require to generate the necessary information.

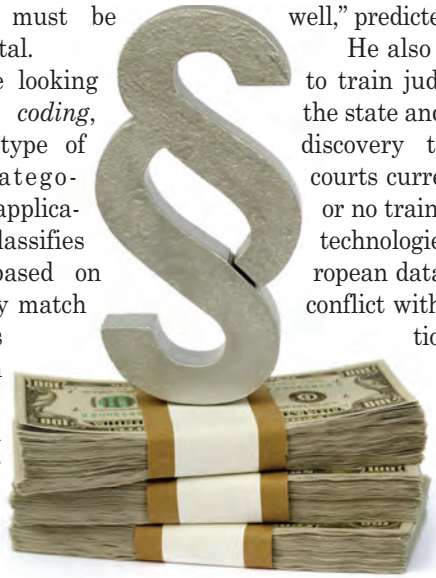
Document review is the largest expense associated with e-discovery, at 73% of the total, according to a 2012 study by RAND Corp. Thus, finding ways to reduce the volume of documents that must be reviewed is vital.

Many are looking to *predictive coding*, which is a type of computer-categorized review application that classifies documents based on how well they match the concepts and terms in sample documents, as a solution for reducing information volume. RAND reported that studies have found that the reduced man-hours required to search fewer documents can cut document review costs by as much as 80%.

Peck encouraged federal judges to learn from the *Global Aerospace Inc. v. Landow Aviation L.P.* case, in which predictive coding was ordered despite plaintiff's objections. "That was a very, very successful use" of predictive coding, Peck said.

Perhaps more importantly, though, Peck foresees a much-needed shift toward information governance. "If 2012 was the year of predictive coding or technology-assisted review, 2013 or '14 seems to be information governance," he said.

"Despite the economy, companies are going to realize that it's important to get their information retention, their information governance, under control; get rid of the data that has no business need and mine the data that has business need…in ways that will improve the company's bottom line on the business side and reduce costs on the e-discovery side as a benefit as well," predicted Peck.



He also stressed the need to train judges, especially at the state and local levels, on e-discovery technologies. The courts currently receive little or no training on e-discovery technologies and on how European data privacy laws can conflict with discovery obligations here.

"I would advise lawyers to assume that they need to educate the judge," he said. **END**