PRIVACY

NSA Leak Shrouds EU-U.S. Trade, Privacy Discussions

Data protection and privacy were critical issues in the July trade talks between the European Union and the United States regarding the Transatlantic Trade and Investment Partnership (TTIP). Although these are not new issues, they have grown in importance thanks to recent reports on the U.S. National Security Agency's (NSA) PRISM project, which included the bugging of EU diplomatic offices in Washington, D.C.

As reported by *Politico*, the goal of TTIP is to "'liberalize' trade between the EU and the United States with a view to remove cross-border regulatory issues, which can bring about extra costs and stifle trade."

The first round of negotiations focused on online privacy and piracy as negotiators tried to reconcile the technology industry's "push for digital freedom with European desires for individual protections," according to the article.

Proposed reforms to the EU's data protection laws center on the concept of "clear rules for a clear Internet and the choice for the individual to give his data or not," said Viviane Reding, European commissioner for justice, fundamental rights, and citizenship, in a recent speech.

According to *ZDNet*, Reding further stressed that data protection rules must apply to any EU citizen data, regardless of whether the company holding that data is based outside the EU; to cloud software and platform providers; and to metadata.

The proposed data protection reforms that Reding referenced are the General European Data Protection Regulation, which concerns general data processing by companies, and the Data Protection Law Enforcement Directive, which relates to the processing of data by police and judicial authorities. A third is a "bilateral data protection agreement being negotiated between the U.S. government and the EU to try and establish the principle that any transfer of EU citizen data should take place through 'established legal channels,'" according to *ZDNet* writer Nick Heath. This agreement would likely have the most impact on intelligence gathering activities such as PRISM.

PRISM Fuels Cries for EU Clouds

One of the cornerstone issues in discussions of cloud services is whether to focus on building national clouds or take advantage of existing clouds offered by international providers, especially U.S. providers.

Estonian President Toomas Hendrik Ilves, chair of the steering board of the new European Cloud Partnership, contends Europe should have its own clouds rather than rely on those from U.S. service providers, reported *ZDNet*.

"Recent months have proven it again: it is very important for Europe to create its own data clouds, operating under EU law and completely safe for users," said Ilves.

Citing the claim that 95% of cloud services in Europe are provided by U.S. companies, Ilves said EU data protection legislation needs to be modernized and that people must understand that large private firms can gather more information than any state. Ilves added that Europe must establish its own cloud at a European level because "otherwise the economies of scale will leave us behind."

CLOUD

How's Your Cloud Insurance Coverage?

There is a big gap between the cloud computing insurance offered by conventional insurance companies and the risks presented by cloud computing, according to Eric Lowenstein, client manager with the financial services group of Aon, in Sydney.

"There is a broad range of cover options available but these have problems," he recently told *ITPro*. "What are the geographical exclusions in regard to data sent offshore? And there are uncertainties about the definition of networks. Do they include devices like iPads, laptops, etc.?"

Lowenstein stressed that this is not simply an IT issue. The cloud poses risks to many stakeholders – IT, marketing, legal, communications, and even the CFO and CEO – and they all need to be engaged.

A cloud computing insurance industry is emerging in the United States. Earlier this year, the MSPAlliance, an association of cloud service providers, announced a partnership with insurance broker Lockton that offers comprehensive protection for cloud and managed service providers around the world. MSPAlliance reportedly has been offering cloud coverage in Australia since 2008.

According to *ITPro*, the U.S. organization CloudInsure has also partnered with Lockton "to provide indemnity assurance to cloud service providers and enterprises in support of service level agreements, and financial protection for customers 'commensurate with their data risk within the cloud.'"

The U.S.A. Patriot Act and recent NSA PRISM project have added fuel to concerns over data risk within the cloud. Adrian Lawrence, a partner with the law firm Baker & McKenzie, warned that the Patriot Act, which grants wide-ranging powers to U.S. government agencies, could be applied outside the United States to any cloud service provider that is owned by, or a subsidiary of, a U.S. company. Lawrence said enterprises, cloud service providers, and insurers must take these types of issues into consideration sooner rather than later.

EHR

U.S. Doctors and Hospitals' EHR Use Is Up

In just three years, 40% of office-based physicians and 42% of hospitals in the United States have implemented at least a basic electronic health records (EHR) system, according to a report co-authored by the Robert Wood Johnson Foundation, Harvard School of Public Health, and Mathematica Policy Research.

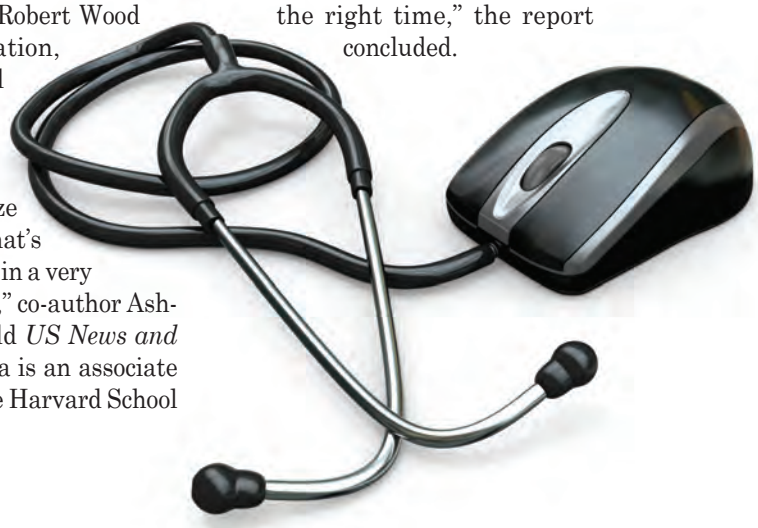
"Given the size of our country, that's amazing progress in a very short time period," co-author Ashish Jha, M.D., told *US News and World Report*. Jha is an associate professor with the Harvard School of Public Health.

The researchers credit three factors for driving the adoption of EHRs: society's increasing reliance on information technology, new federal funding to support the purchase of EHR systems, and future penalties for those who don't use EHRs.

"It's the right incentives at the right time," Jha said. "Doctors and hospitals have been thinking about buying electronic health records [systems] for some time. This is where our society is moving. But the finances have been a challenge. The federal incentives have been very well targeted. They were well designed to help push hospitals and doctors to adopt EHRs."

The study's findings weren't all quite as positive, however. For example, only 5% of the systems meet federal standards for exchanging that data with other providers to allow widespread physician access to a patient's records. The good news is that more healthcare providers are reportedly participating in initiatives that ultimately will connect their own electronic records systems to community-wide information exchanges.

Predictably, there are several improvements needed before EHR use can be optimized. "Even with improved functionality, high-quality patient education still depends on clinicians and educators with the time and skills to tailor the right materials to the patient at the right time," the report concluded.



MOBILE DEVICES

Mobile Safer than Desktops?

Yes, it could happen. By next year, mobile technology could actually be more secure than traditional computing.

This bold prediction was made by Marc van Zadelhoff, IBM vice president of strategy and product management, in a recent article in *USA Today*.

"Companies are adopting best practices that are rapidly enabling mobile computing to become more secure than traditional desktop computing," he said. "This is being led by chief information security officers who are driving change to ensure critical mobile security needs are addressed today."

Although mobile devices and tablets are primarily considered consumer products, they are increasingly being used for business purposes. Research conducted by Vertic, a digital ad agency, showed that tablet use in enterprises has grown nearly 50% annually since 2011. More than 96 million tablets are expected to have been shipped to enterprises by 2016. Further, 38% of senior executives were issued tablets in 2011.

Mobile usage has become a major driving force in IT over the past few years, a trend that is expected to continue in the near term. It has forced organizations to develop and expand policies that guide use and security of these devices. For example, a growing number of organizations now require employees to adopt solutions on their mobile devices that help keep personal data separate from corporate data.

Given the advances in mobile technology, van Zadelhoff concluded that security officers will have more finite control over mobile devices than they've had over traditional computers. "Going forward, mobile devices no longer have to be a security threat, but instead it can be seen as a 'do-over' in order to get it right," he said.

E-DISCOVERY

Gartner Predicts Growth, Consolidation in E-Discovery Market

Double-digit growth and continued consolidation are likely in the global e-discovery market over the next few years, according to Gartner Inc.'s *Magic Quadrant for E-Discovery*, published in June.

Gartner expects the market to grow by about 15% annually, from $1.7 billion in 2013 to $2.9 billion by 2017. This growth will be largely attributable to two factors: increasing volumes of litigation and regulatory investigation; and the growing volume of content and data that must be searched in support of these activities.

The majority of this market growth will reside with U.S. vendors, but the increasing awareness of e-discovery issues in Europe and Asia will drive growth there, eroding the U.S. share of the total market from 81% in 2012 to less than 70% in 2017. In addition, software vendors in adjacent markets, such as enterprise content management, will likely extend their offerings to include e-discovery functions, and vendors already in the e-discovery market will acquire additional capabilities from the content analytics or workflow sectors, for example.

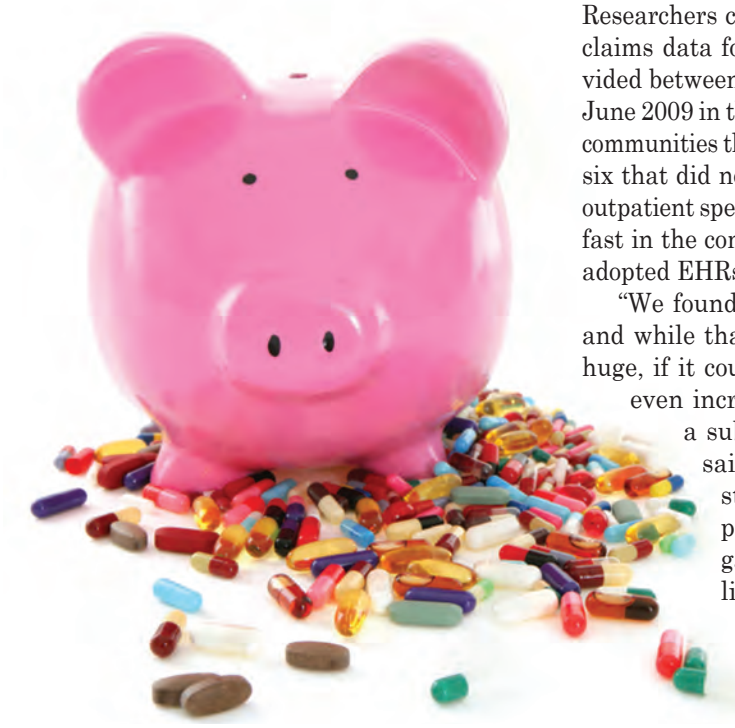
While revenues grow, the number of firms claiming to have e-discovery products and services is expected to shrink by 25% during the next two years. Most of that attrition is expected among service providers, not software vendors. Consolidation is already underway and is expected to continue, driven primarily "by the disintermediation of law firms, pricing pressure, and the need to develop economies of scale in data management," the report states.

Predicts Gartner: "The remaining legal-services firms will take one of two routes by becoming either large firms that are 'one-stop shops' but not technology developers, or large firms that are one-stop shops with proprietary technology for all aspects of the EDRM, not just the traditional hosting and review capabilities that have long sustained the industry. Although there is room for regional and specialist players, this is the part of the market that is consolidating and shrinking fastest. The larger players will need international presence in the form of data centers and local legal personnel to be competitive as the market opens up geographically."

EHR

Study Shows EHRs Do Lower Costs

A recent article on *Medical Xpress.com* indicates that doctors who use commercially available electronic health record (EHR) systems are seeing slower growth in healthcare costs, saving $5.14 per patient per month.



These savings were documented by a recent University of Michigan study of the impact of EHRs in community-based settings, including private practices and hospitals. Researchers compared insurance claims data for patient care provided between January 2005 and June 2009 in three Massachusetts communities that adopted EHRs to six that did not. They found that outpatient spending did not rise as fast in the communities that had adopted EHRs.

"We found 3 percent savings and while that might not sound huge, if it could be sustained or even increased, it would be a substantial amount," said Julia Adler-Milstein, an assistant professor at Michigan's School of Public Health and the study's lead author.

Most of the savings were in radiology. Adler-Milstein suspects doctors ordered fewer imaging studies because they had better access to patients' medical histories. This finding also contradicts the assertion that EHRs would actually raise costs because they make it easier to order tests, which is a key argument of critics who oppose using taxpayer dollars to fund EHRs.

The nine communities in the study had all applied to participate in the Massachusetts eHealth Collaborative's pilot, which gave funding and support for doctors' offices to convert their records.

"I think our findings are significant because we provide evidence to support the use of taxpayer dollars to invest in electronic health records," Adler-Milstein said. "We really have not had compelling evidence that proved that they would save money. It was assumed, but there are a lot of skeptics. This study helps clarify whether there are cost savings and what the magnitudes of those are in the near-term."

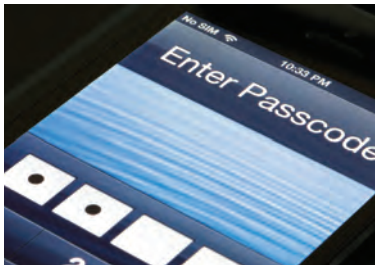
CYBERSECURITY

Online Security a Growing Concern for Insurance Industry

A recent study by Ernst & Young clearly showed that the global insurance industry takes cybersecurity very seriously. In fact, Ernst & Young expects it to be one of the top three issues facing the industry by 2015. It is currently ranked sixth.

Contributing factors cited by the report include the increasing availability of sophisticated hacking tools on the Internet; the growing pool of people capable of seriously breaching corporate security; the difficulty of developing a coordinated approach to Internet management, which offers an element of protection to criminals who route their attacks through multiple countries; the rising threat of state-sponsored cyber attacks; and the ease of staging distributed denial-of-service attacks.

"The key factor is to ensure an appreciation of cybersecurity as a due diligence and compliance issue, one that is recognized within the risk management function and regarded as a strategic risk at the highest corporate level. This is clearly a complex issue, but simple moves, such as regular CIO reports to the board and tracking cyber-attack incidents above a certain threshold in the company's key performance areas, can convey the seriousness with which it is taken at the top," the researchers concluded.



PRIVACY

Employees Don't Trust Employers with Mobile Data, Privacy

Use of personal mobile devices for sharing information on company networks has become commonplace. Most employees, however, don't trust their employers to protect their personal information.

A recent study of about 3,000 employees in the United States, United Kingdom, and Germany discovered that only 30% trust their employers to keep personal information private and not use it against them. Those in the UK were most trusting, with 34% saying they completely trust their employer, compared to 31% in the United States and 24% in Germany.

The survey further revealed confusion among the respondents as to what constitutes private information. Nearly 41% felt certain their employer could not see any private information on their mobile device. Only 28% thought the company could see their work e-mail and attachments.

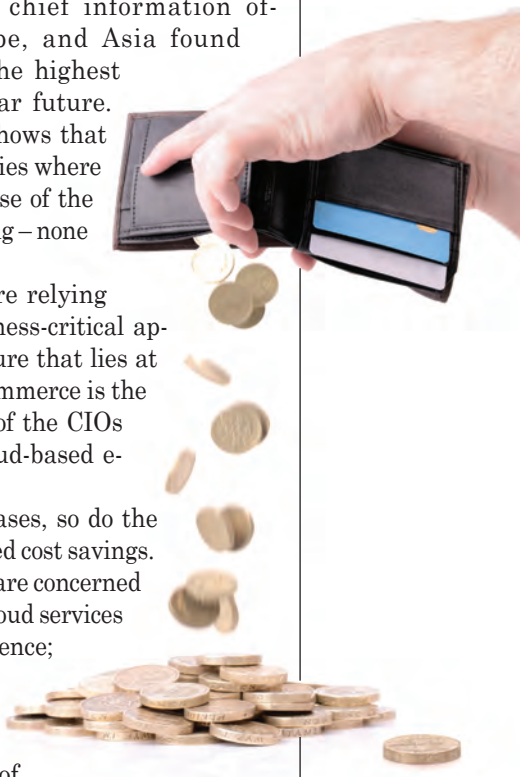
"The reality is that if these devices are used to get corporate email, employers can see work email and attachments on a mobile device as easily as they can on a PC. That's a gulf between expectations and reality," said Ojas Rege, vice president of strategy at security firm MobileIron, which sponsored the research.

"It's a new set of technologies, so there's immediately some level of confusion," Rege told *The Telegraph*. "Another thing is that IT departments are traditionally not very good at communicating; it's not their core competence."

He said the level of distrust among employees is due largely to a lack of transparency within organizations and the absence of clear policies around bringing mobile devices to work.

CLOUD

CIOs Cite Cloud's Hidden Costs as Chief Concern



A recent Compuware survey of chief information officers in the Americas, Europe, and Asia found that cloud computing will be the highest priority area for investment in the near future.

Current IT infrastructure spending shows that companies are exploiting cloud opportunities where they see them, which are primarily the use of the public cloud for backup, recovery, and testing – none of which directly affects the end user.

The study showed that companies are relying increasingly on the cloud to deliver business-critical applications and the supporting infrastructure that lies at the core of their business operations. E-commerce is the most commonly used cloud service; 81% of the CIOs are already using or planning to use cloud-based e-commerce platforms within the year.

As investment in cloud services increases, so do the stakes for the cloud to deliver on its promised cost savings. However, the majority of companies (79%) are concerned there will be hidden costs associated with cloud services prompted largely by poor end-user experience; 64% of the CIOs cited poor end-user experience as the most significant risk to managing the cloud.

Despite the business-critical nature of these cloud applications and the potential impact of poor end-user experience, the report revealed that 73% of companies are still using outdated methods to track and manage application performance. The most common tracking metric is simple availability or uptime, rather than more granular end-user metrics such as response time, page rendering time, and user interactivity time.

"The cloud is increasingly being used to deliver business-critical applications, so it is quite shocking that most companies are just waiting for problems to occur and then firefighting," said Thomas Mendel, managing director at Research In Action, which conducted the survey for Compuware. "The fact is that most traditional monitoring tools simply don't work in the cloud. Effectively monitoring and managing modern cloud-based applications and services requires a new approach designed to work in today's complex, hybrid, and dynamic environments. Failure to do so could have a hugely detrimental impact on reputation, customer loyalty, and revenues."

CYBERSECURITY

Hackers Attend Summer Camp

Maybe you've heard of Space Camp, but how about hackers' camp? The U.S. Cyber Challenge (USCC) is conducting four regional camps this summer to provide specialized cybersecurity training to some of the brightest young talent in cybersecurity.

The camps feature workshops led by college faculty, top System Administration, Networking, and Security Institute instructors, and cybersecurity experts from the community. The workshops and presentations focus on topics ranging from intrusion detection, penetration testing, and forensics. Campers can also participate in a job fair where they can meet USCC sponsors and discuss potential employment.

Cybersecurity experts who can bring a fresh perspective to the profession are in top demand in the private and government sectors. It's estimated there are as many as one million openings in this highly specialized job market in the United States alone.

USCC's program is working to find 10,000 of America's best to fill the ranks of cybersecurity professionals. Other countries see the need as well; France, for example, has conducted similar cyber challenges, according to the BBC News.

Academic institutions have increased their efforts to meet the need for cyber professionals, but the demand is still much greater than the supply, according to Diane Miller, who directs Cyber Patriot, a national high school cyber-defense competition that's presented by Northrop Grumman and the Air Force Association. "Everybody is scrambling to find that exceptional talent," Miller told BBC News.

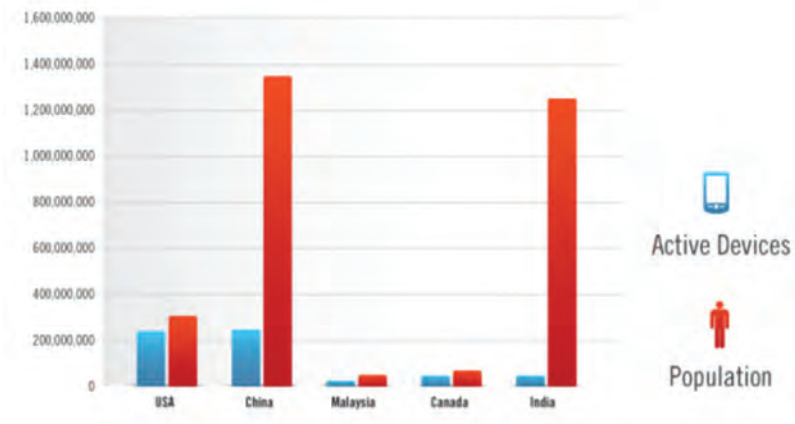
Some worry that this type of training could be turned against organizations and the government. Samuel Schneider, a representative of the global IT security organization (ISC)2, takes a different view: "The earlier we reach them, the less risk they are at . . . going out and performing illegal or illicit activities."

Headded that this is an excellent opportunity to "indoctrinate or incorporate a new security mentality into children."

MOBILE DEVICES

World Market Means Big Growth for Mobiles

The latest forecast from International Data Corp. (IDC) predicts a 33% increase in the number of smartphones shipped in 2013 alone. That equates to about 959 million phones, compared to nearly 723 million in 2012. Furthermore, this trend will likely continue for many years given the growing market in less-developed countries. With increasing demand from poorer markets come lower prices. IDC reports that smartphone average selling prices (ASPs) have declined to $372 in 2013, down from $407 in 2012 and $443 in 2011. The ASP is expected to drop as low as $309 by 2017, thanks largely to the continued emerging market demand.



CLOUD

Spare Cloud Computing Capacity to Be Traded on German Stock Exchange

Beginning the first quarter of 2014, Deutsche Börse, the operator of the Frankfurt stock exchange and Eurex derivatives exchange, will start trading in its spare cloud computing capacity. Buyers and sellers of at least one terabyte in cloud-computing data space – the size of the average external home hard drive – will be able to match supply and demand through a new platform run by the exchange, with real-time prices.

International Data Corp. has predicted an annual growth rate of up to 40% in Europe's cloud infrastructure over the next seven years as it attempts to catch up with developments in the United States and Asia. The *Wall Street Journal* reported that Deutsche Börse and Zimory, a Berlin-based software developer that does not provide cloud capacity, recently formed Cloud Exchange AG in hopes of being a "catalyst" for that growth.

Buyers of cloud capacity apparently will be able to choose the location and jurisdiction of the servers, as well as stipulate how long they want to rent the cloud capacity. They also will be able to migrate between vendors, choose the safety level they want for their data, and choose their disaster recovery measures and data speed.

The article added that a group of up to 20 "early adapters" is working on the details to ensure the marketplace can go live with enough liquidity early next year.

Other commercial cloud marketplaces exist but are affiliated with specific vendors.

EHR

Despite EHR Growth, Australian Doctors Resist Letting Patients See Records

The use of electronic health records (EHRs) in Australia grew 62% from 2011 to 2012 – and the initial results have been encouraging. According to a survey by Accenture, 83% of Australian doctors are actively using electronic medical records (EMRs) and roughly 70% reported improved quality of diagnostic and treatment decisions as a result of sharing the EMRs. Indeed, most (77%) Australian doctors believe sharing health records electronically helped reduce medical errors in 2012.

Australia's personally controlled electronic health record (PCEHR) scheme has had a slow start despite support by government and prominent healthcare CIOs. When it comes to providing patients control over their personal EHRs, Australian doctors are more resistant than doctors in other countries. Fewer than one-quarter of Australian doctors believe patients should have full access to their records; 65% believe patients should have limited access; and 16% say they should have no access. Australia ranked second highest of the eight countries surveyed in the proportion of doctors who say patients should have no access to their records.

"The shift to patient-centered care has long been talked about, but we're now entering a new stage with the rise of the digital citizen and availability of electronic health records," said Leigh Donoghue, managing director of Accenture's health business in Australia and New Zealand.

"The combination of smartphones, faster broadband, mobile access to the PCEHR system, and a growing array of mobile health applications will trigger fresh demands from consumers for more active participation in managing their own care. To meet changing consumer expectations, Australian doctors' views on patient access will need to evolve," said Donoghue.

CYBERSECURITY

Medical Device Manufacturers Tackle Cybersecurity

It appears medical devices are not immune to the risks associated with cyber attacks. After all, many medical devices contain configurable embedded computer systems that can be vulnerable to breaches.

Although the U.S. Federal Drug Administration (FDA) is not aware of any targeted devices or of any injury or death as a result of a cyber attack, it said it has become aware of cybersecurity vulnerabilities and incidents that could directly impact medical devices or hospital network operations.

"Over the last year, we've seen an uptick that has increased our concern," said William Maisel, deputy director of science and chief scientist at the FDA's Center for Devices and Radiological Health. "The type and breadth of incidents has increased."

He said officials used to hear about problems only once or twice a year, but "now we're hearing about them weekly or monthly."

The Department of Homeland Security (DHS), which is working with the FDA to reduce these vulnerabilities, recently received reports from two researchers that found potential weaknesses in 300 medical devices produced by about 50 vendors, an official told *DelawareOnline*.

The FDA has been working closely with DHS and other agencies and manufacturers to identify, communicate, and mitigate vulnerabilities and incidents as they are identified, but the agency is asking device manufacturers to do more.

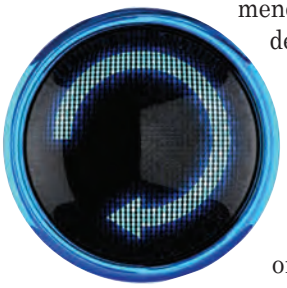
Specifically, the FDA recommends that manufacturers "review their cybersecurity practices and policies to assure that appropriate safeguards are in place to prevent unauthorized access or modification to their medical devices or compromise of the security of the hospital network that may be connected to the device. The extent to which security controls are needed will depend on the medical device, its environment of use, the type and probability of the risks to which it is exposed, and the probable risks to patients from a security breach."

The FDA has similarly requested that healthcare facilities evaluate their network security and take steps to protect the hospital system. That includes restricting unauthorized access to the network and networked medical devices; ensuring appropriate antivirus software and firewalls are up to date; monitoring network activity for unauthorized use; and working with the device manufacturer if they detect a security problem.

The FDA is working on guidelines – to be available this year – that will allow it to block approval of devices if manufacturers don't provide adequate plans for protecting the devices and updating their security protections over their commercial lifetimes.

MOBILE DEVICES

NIST Publishes BYOD Guidance



The National Institute of Standards and Technology (NIST) finally updated its 2008 *Guidelines on Cell Phone and PDA Security* to reflect the tremendous growth of mobile devices. The new *Guidelines for Managing the Security of Mobile Devices in the Enterprise* recommends using centralized device management at the organization level to secure both agency-issued and individually owned devices used for government business.

Centralized programs manage the configuration and security of mobile devices and provide secure access to an organization's computer networks. Many agencies currently use this type of system to manage the smartphones they issue to staff. The new NIST guidelines offer recommendations for selecting, implementing, and using centralized management technologies for securing mobile devices.

Other key recommendations include instituting a mobile device security policy, implementing and testing a prototype of the mobile device solution before putting it into production, securing each organization-issued mobile device before allowing a user to access it, and maintaining mobile device security.

GOVERNMENT RECORDS

Revisiting the '70s: More Watergate Records Released

"All the News That's Fit to Print"

The New York Times

LATE CITY EDITION

VOL. CXXIII ... No. 42,566 NEW YORK, FRIDAY, AUGUST 9, 1974 15 CENTS

NIXON RESIGNS

HE URGES A TIME OF 'HEALING'; FORD WILL TAKE OFFICE TODAY

'acrifice' Is Praised; Kissinger to Remain

By ANTHONY RIPLEY

The 37th President Is First to Quit Post

By JOHN HERBERS

POLITICAL SCENE SHARPLY ALTERED

Rise and Fall

Appraisal of Nixon Career

JAWORSKI ASSERTS NO DEAL WAS MADE

The U.S. National Archives and Records Administration (NARA) has released additional records that had been sealed since the criminal trial of seven men involved in the Watergate burglary (*U.S. v. Liddy, et al.*) in the 1970s. NARA released 36 folders of documents totaling approximately 950 pages upon an order from the U.S. District Court for the District of Columbia.

All trial records have been "unsealed," but NARA said it is still required to withhold personal privacy information, grand jury information, and illegal wiretap information, as appropriate.

Newly unsealed records include the names only of those overheard by the bugs installed in the break-ins at the Democratic National Committee headquarters at the Watergate. They also contain the pre-sentence reports for the Cuban burglars. NARA said such records of living persons are not usually released publicly, but the court stated in its opinion that "the public's interest in clarifying the historical record and further identifying the facts that led to the resignation of President Nixon outweigh their individual privacy interests."

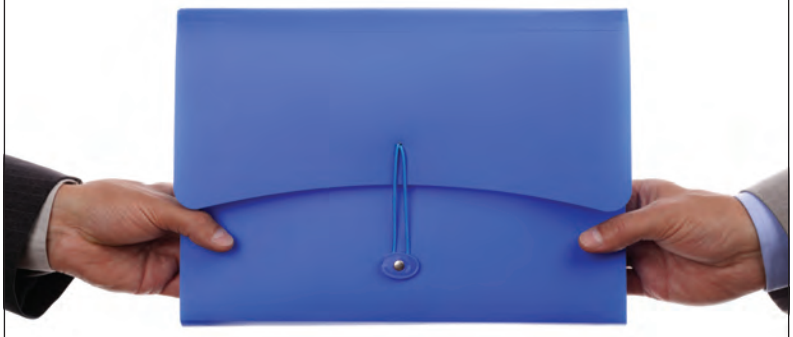
FACTOID

52% of U.S. physician groups planning to implement electronic health record (EHR) systems do not plan to replace their current practice management system with an integrated practice-EHR management system.

Source: 5th Annual U.S. Ambulatory Electronic Health Record & Practice Management Study, released by HIMSS Analytics

E-DISCOVERY

New Service Concept in E-Discovery Technology Emerges



As e-discovery technology moves beyond litigation into the realm of investigation, the volume of data continues to grow, making it difficult for many corporate legal departments to keep up. They are searching for a solution that is agile, up-to-date, and economical – a solution that provides control over their data, said Lynn Frances, a legal technology analyst, in her recent article in *Metropolitan Corporate Counsel*.

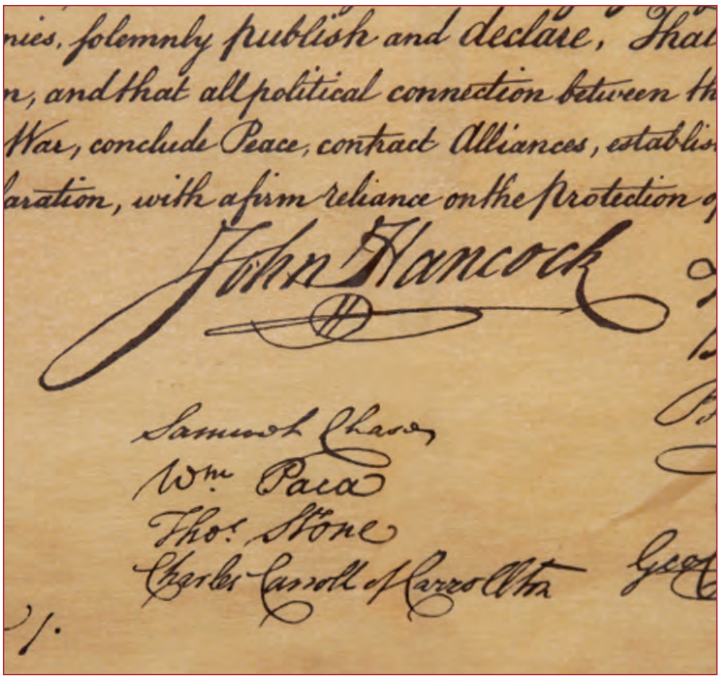
Historically, legal departments that wanted to maintain tight control over their data have kept it in-house. Some built such large litigation support departments that they could have been fully operational e-discovery services companies. When technology wasn't changing as quickly, the in-house model was a valid option for those that could afford the up-front investment, according to Frances.

Predictably, the do-it-yourself (DIY) solution wasn't viable for smaller organizations that couldn't afford the investment in technology and personnel or that chose to focus on their core business. They chose outsourcing as the solution.

In the outsourcing model, corporations relinquished control of their data, workflow, and protocol to outside counsel and e-discovery service providers. "Unless they established their own case-tracking and analysis systems in-house, general counsel, whose cases were spread among various service providers, lacked the business intelligence that the DIY departments enjoyed," Frances wrote.

Because of the tremendous changes the field has seen in the last several years, the cloud is a third option that offers the benefits of the other two models. In the cloud model, the initial and ongoing investments in software, infrastructure, and security lie with the service provider. This allows the client to determine what portions of the processes will be run in-house and places the final control of the data in the organization's hands. Of course, to provide assurance on data security, a cloud-based offering that hosts legal data must be housed in a highly secure environment with verified security protocols.

"This type of model was not possible in the legal industry just three years ago because attorneys were uncomfortable with the cloud as a legal data environment," noted Frances. Indeed, a 2011 survey of in-house counsel found that only 29% of the responding companies used cloud technology. That number has changed drastically: the 2013 Corporate Counsel Survey showed that four out of five respondents reported a good experience with cloud-based computing.



ARCHIVES

Attention U.S. History Buffs: Founders' Papers Are Online

If you haven't yet discovered the new *Founders Online* website, launched this summer by the U.S. National Archives and Records Administration (NARA), now may be a good time to do so. The site, which was still in beta at the time of printing, features correspondence and other writings of George Washington, Benjamin Franklin, John Adams, Thomas Jefferson, Alexander Hamilton, and James Madison.

For the past 50 years, through its National Historical Publications and Records Commission, NARA has invested in documentary editions of the original historical records of the Founding Era. Dedicated historians and experts in editing historical documents have collected copies of original 18th and 19th century documents, transcribed them, provided annotations, and produced hundreds of individual volumes – all of which eventually will be fully searchable and available for free on the *Founders Online* site.

Founders Online will include thousands of documents, replicating the contents of 242 volumes drawn from the published print editions. As each new print volume is completed, it will be added to this database of documents.

The site launched with 119,000 searchable documents, fully annotated. All of the unpublished and in-process materials (about 55,000 documents) will be posted online over the next three years. Researchers will be able to view transcribed, unpublished letters as they are being researched and annotated by the editors and staff. Altogether, some 175,000 documents are projected to be on the *Founders Online* site. **END**