COMPLIANCE

Credit Card Transaction Standard Updated

Version 3.0 of the Payment Card Industry Data Security Standard (PCI DSS) and Payment Activity Data Security Standard (PA DSS) became effective January 1, but organizations will have until at least December 31 to make the transition.

According to the PCI Security Standard Council, version 3.0 helps organizations make payment security part of their business-as-usual activities by introducing more flexibility and an increased focus on education, awareness, and security as a shared responsibility.

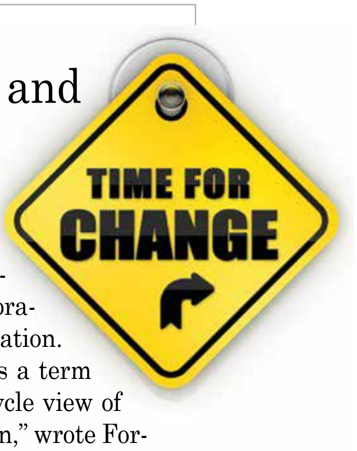
There has been some debate in the security industry about the effectiveness of the standard, particularly in light of major data breaches – such as the Adobe breach in October – by organizations that have been in compliance with the standard.

“Whatever your opinion, the new PCI DSS 3.0 appears to be moving from a security check box posture to a more holistic risk management approach,” said Bernard Zelmans, general manager for EMEA at security management firm FireMon, in an e-mail to *ComputerWorld UK*’s Lucian Constantine. “This will hopefully entail a more security centric approach to PCI compliance rather than the least common denominator approach of earlier versions of PCI.”

One area not addressed by the changes is mobile security. According to Michael Aminzade, a director at security firm Trustwave, “Merchants are struggling with how to protect mobile payment solutions and integrating mobile devices into their organizations. The Council released a best practices guide for mobile security more than a year ago, but it would be more beneficial to release additional guidance pertaining to mobile data security.”

RIM TRENDS

5 Trends Reshaping Records and Information Management



Changing technology and increased regulation have made it imperative that enterprise architecture and records management professionals work more collaboratively to protect and manage the enterprise’s information. That’s why information governance is “emerging as a term that better describes and supports a holistic, life cycle view of the creation, use and protection of digital information,” wrote Forrester’s Cheryl McKinnon in a recent *KMWorld* article. She went on to describe the top five trends that are reshaping the profession:

1. **Records management shifts to information governance.** Many businesses still lack confidence in their electronic records management programs, compliance initiatives, and e-discovery preparedness. Meanwhile, vendors are taking fresh approaches to addressing compliance, categorization, and retention requirements. The shift to a more comprehensive and proactive management of information across its entire business life cycle – rather than just at the end – has begun.
2. **Cloud and social platforms render “file and declare” ineffective.** As the shift to the cloud continues, McKinnon urges enterprise and information architects to realize that traditional records managers and records management systems are slow to make that leap. Furthermore, current records management systems tend to be already missing many forms of electronically stored information.
3. **Digital preservation forces itself onto the governance agenda.** “Digital records that have a long-term retention schedule are at risk when hardware devices, software applications and file formats decay or become obsolete,” wrote McKinnon.
4. **Open standards and open source change the sourcing landscape.** Between 2011 and 2012, several national governments directed their IT, records, and procurement managers to learn more about – and select – open-technology platforms.
5. **Auto-categorization becomes viable and approachable.** Opportunities to use auto-classification technologies for routine, high-volume, predictable electronic content are increasing as technology matures, McKinnon said.

CLOUD

Gartner: Cloud Will Be Bulk of IT Spending by 2016

Cloud spending is growing so fast that it will comprise the majority of new IT expenditures by 2016, according to an October press release from Gartner Inc. The IT research company further predicts that 2016 will see the private cloud give way to the hybrid cloud. By the end of the following year, Gartner expects nearly half of all large enterprises will have hybrid cloud deployment, meaning the enterprise will be both a user and provider of cloud services.

David Linthicum, chief technology officer and founder of Cloud Technology Partners, disagrees with part of this prediction. "Enterprises will use a variety of cloud models, including private and hybrid, resulting in a multicloud reality rather than a hybrid one. Already, enterprises are finding the cloud deployments that meet their requirements are more complex than private, public, or hybrid," he wrote in his October 29 *InfoWorld* blog.

In an earlier blog, Linthicum wrote that *multicloud* "add[s] more clouds to the mix, perhaps two or more public IaaS [infrastructure as a service] providers, a private PaaS [platform as a service], on-demand management and security systems from public clouds, private use-based accounting…" This is in contrast to a *hybrid cloud*, which he defined as "typically a paired private and public cloud."

In the more recent blog, he added that business – not IT – will drive cloud growth. Those in the business who want more cost-effective ways to provide IT services, decrease time to market, and increase agility will provide the impetus. The growth will be more around application development and application migration than infrastructure conversation and expansion, predicted Linthicum.

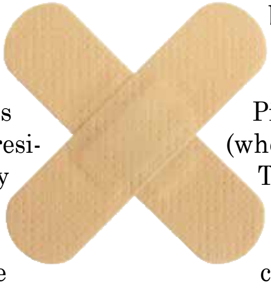
According to Chris Howard, research vice president at Gartner, the very real trends toward cloud platforms and "massively scalable processing" are giving companies and individuals more freedom to decide how they'll acquire or deliver IT services. Further, according to Howard, "Services delivered through the cloud will foster an economy based on delivery and consumption of everything from storage to computation to video to finance deduction management."

Along with the benefits mentioned above, there are several risks for organizations that use external cloud services, putting their information outside their immediate control. These risks need to be considered at the time of contracting and include:

- Ensuring 24/7 access to the information
- Ensuring the security of the information; the service provider's policies, controls, and staff training must meet the enterprise's requirements
- Ensuring that information is stored in a specific, physically identifiable location
- Ensuring there is an exit strategy if a provider goes out of business or the business relationship is terminated

INFO TECHNOLOGY

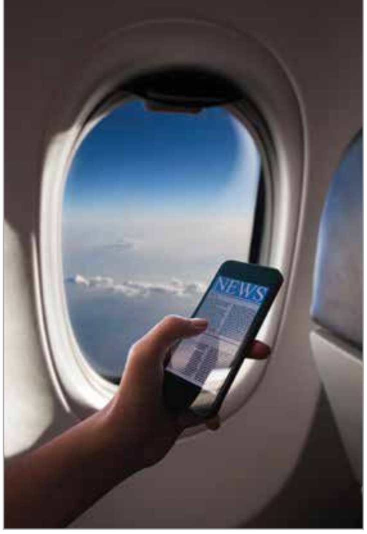
Computer, Heal Thyself?



One day, help desks and IT departments will be redundant as computers will be able to mimic the human brain and self-heal. At least that's the vision of Jeff Hawkins, the neuroscientist who founded the mobile computing companies Palm (where he invented the Palm Pilot) and Handspring (where he invented the Treo smart phone). Hawkins' latest endeavor is Grok, a company whose goal is to simultaneously create a theory of how the brain works and a computer algorithm to implement this theory. In other words, Grok is developing true artificial intelligence, machine intelligence software based on the brain's neocortex, which controls sensory perception, motor commands, and language, among other functions.

"It is basically machines that learn like the human brain learns," explained Hawkins in a recent article in *The Sydney Morning Herald*. "This is going to have as big an impact in the world as computers had. It is that big a concept."

The technology, which operates in the cloud, is in its earliest of early-stage development. It is available to Amazon Web Services customers to monitor server behavior and is being used by Phase 6, a language learning project based in Austria.



MOBILE DEVICES

Good News for Travelers

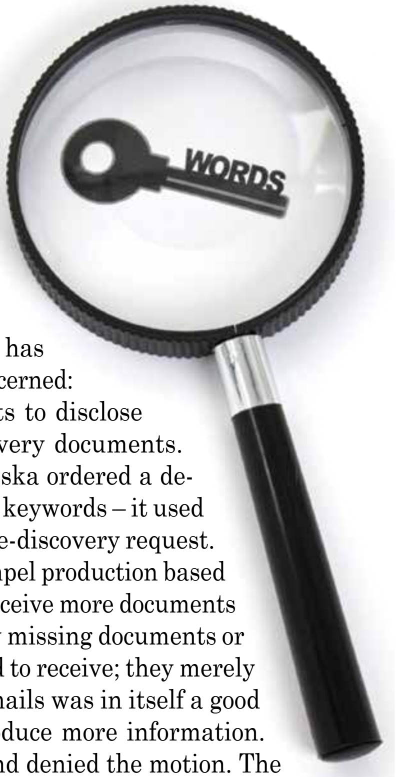
The next time you board an airplane you may not hear the request to turn off all electronic devices before taking off and landing. The U.S. Transportation Department's Federal Aviation Administration (FAA) has determined that airlines can safely expand use of portable electronic devices (PEDs) during all phases of flight.

According to the FAA, implementation will vary among airlines due to differences among fleets and operations. The agency expected many carriers would prove that their planes allow passengers to safely use their devices in airplane mode, gate-to-gate, by early 2014. Since the airlines must be approved by the FAA, the agency issued a tool to help carriers assess the potential risk of "PED-induced avionics problems" for their airplanes and operations. Specifically, carriers need to evaluate avionics as well as changes to stowage rules and passenger announcements. Each airline must also revise its manuals, checklists for crewmember training materials, carry-on baggage programs, and passenger briefings before expanding use of PEDs. It's up to each airline to determine how and when it will allow broader use of PEDs.

Yes, that means you will be able to read e-books, play games, and watch videos from gate to gate, with very limited exceptions. Electronic items, books, and magazines will still need to be stored in the seat back pocket during takeoff and landing. Additionally, cell phones should be in airplane mode or with cellular service disabled – no signal bars displayed – and cannot be used for voice communications, based on Federal Communications Commission (FCC) regulations that prohibit any airborne calls via cell phones. (The PED Aviation Rulemaking Committee recommended the FCC reconsider these regulations.) If your air carrier provides Wi-Fi service during flight, you may use those services, and you can continue to use short-range Bluetooth accessories such as wireless keyboards.

E-DISCOVERY

Prepare Yourself for Keyword Disclosure



An emerging trend in the courts has some attorneys increasingly concerned: courts are ordering defendants to disclose the keywords used to produce discovery documents.

Recently, a federal court in Nebraska ordered a defendant to report all the sources – and keywords – it used to perform searches in response to an e-discovery request. The plaintiffs had filed a motion to compel production based on the fact that they had expected to receive more documents than they did. They didn't point to any missing documents or even types of documents they expected to receive; they merely asserted the production of only 25 e-mails was in itself a good reason to order the defendant to produce more information. The judge didn't buy the argument and denied the motion. The court did, however, order the defendant to disclose the sources and keywords that were used.

This isn't the first instance of a court ordering the disclosure of search keywords. Last year, in a trade-secret theft case, a court in California issued a disclosure order despite defense counsel's contention that it would reveal sensitive trade secrets. The court again didn't buy into the argument. Thus, the trend seems to be that the plaintiff needs only to request the disclosure; a compelling reason is not required. Some trial lawyers contend this erodes the attorney-client privilege regarding work product.

One attorney, Ralph Losey, voiced just such an opinion on his blog *e-Discovery Team*: "[M]any lawyers have long considered the particular methods they used to find documents that are responsive to a request for production to be obvious work product. It was, after all, their own thought processes and legal techniques. If they used keywords to find the relevant documents, then they should not have to disclose what words they used. They argued that it would unfairly require them to disclose their theory of the case, their mental impressions of how to find relevant information."

E-DISCOVERY

Automated Legal Hold Tracking Lags, Survey Says

Most organizations are lagging in automating their legal hold management and tracking. The *Legal Holds and Data Preservation Survey 2013* revealed that 53% of organizations today use manual/written processes for tracking litigation holds, while only 34% have automated processes. One of 20 organizations still relies on verbal legal holds.

In many ways, automating the legal hold process has proved to be much more efficient and reliable than manual options, resulting in a higher satisfaction level with the current system/process. Survey results showed that such automation increases efficiency as well as the likelihood of issuing litigation holds. "When a litigation hold takes more effort, respondents are less likely to proactively implement one," explained David Steinberg, the founding partner of the Steinberg Group LLC, which conducted the survey.

Those using automated processes are also more likely to observe best practices. Compliance with sub-processes such as issuing reminders, requiring custodial compliance, following up with custodians, and sending release notifications was much more likely (85%) among automated users than manual ones (57%).

Overall, 62% of respondents expressed confidence in their current process, but those on manual processes were nearly 20 times more likely than automated users to indicate a "below standard" self-assessment. Similarly, automated users were 80% more likely to give their current system/process a favorable rating.

Training continues to be a problem area for most organizations. Although 70% of organizations train employees on legal holds, only 45% think the employees fully or mostly understand their preservation obligation.

The study surveyed 525 legal professionals responsible for overseeing the legal holds process, making it the largest study of its kind focused specifically on how organizations are currently handling legal data preservation.

CYBERSECURITY

Users Are Cybersecurity's Achilles Heel

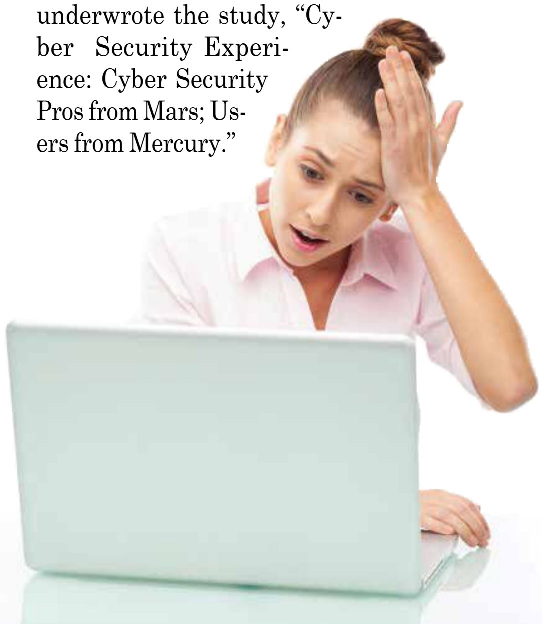
A recent study released by MeriTalk shows that U.S. federal agency cybersecurity professionals have become so focused on data security they fail to consider how the security measures will affect users. As a result, nearly a third (31%) of agency users said they use workarounds regularly to circumvent security measures they say are time consuming and hinder productivity. That explains why about half (49%) of federal security breaches are blamed on user noncompliance.

The survey found that very few federal cybersecurity professionals feel prepared for cyber threats. Nearly three-quarters (74%) said they are not prepared for an international cyber attack or to support secure access for mobile devices. Almost as many (70%) said they are not prepared for a denial-of-service attack or to secure cloud computing environments.

The activities that cybersecurity professionals said are the most likely to cause a security breach are the same activities in which end users encounter the most frustrating security measures: surfing the Internet, downloading files, accessing networks, and transferring files. E-mail, external websites, and Internet access via agency work stations are not only the most challenging end-user applications to secure, they are also the tools that more than 80% of end users rely on daily.

Dealing with security measures has reportedly become so burdensome that 20% of end users said they can recall an instance where they were unable to complete a work assignment on time because of a security measure. End users' responses to this study should make it clear to data security professionals that end user experience needs to be given higher priority.

"Without question, federal cyber security pros have a tough job, but they must start working with end users as partners instead of adversaries. It is a team game, and better support for users will deliver better results for security," concluded Tom Ruff, vice president public sector for Akamai, which underwrote the study, "Cyber Security Experience: Cyber Security Pros from Mars; Users from Mercury."



E-DISCOVERY

Transborder E-Discovery on the Rise

As if you didn't have enough to think about in being prepared for e-discovery, what if some of the information needed is stored in another country? It's up to you to ensure you won't run afoul of that country's privacy laws.

And some countries have much more stringent privacy laws than others. For example, European Union member states have based their data protection laws on the EU Data Privacy Directive, which closely regulates how and when personally identifiable information (PII) may be collected, processed, stored, and transferred by an organization. Those controls are much stricter than in the United States.

In addition, according to the global legal services firm Mayer Brown, "Several European countries have enacted blocking statutes designed to protect sovereignty and shield foreign nationals from intrusive U.S.-style litigation. Violations of these foreign laws may result in serious consequences for the organization, including criminal charges."

It's up to legal counsel and information governance professionals to ensure their organizations can meet both their U.S. and foreign legal obligations. Now – before litigation arises – is the time to evaluate those risks and implement the necessary standard controls. In a *Mondaq* article on the subject, Mayer Brown suggested the following steps:

- **Know your data and your legal obligations.** Involve local counsel and data privacy professionals in the litigation process to help minimize the risk. This is especially important given proposed changes to the EU directive, which include considerably steeper fines for violations.
- **Limit collection.** Consider implementing collection procedures that are specifically targeted at identifying relevant data from the outset, rather than employing a broad collection philosophy and relying on the review process to narrow the data for production.
- **Consider onsite, in-country review.** In some instances, it may be easier to collect and process data relevant to a U.S. litigation by conducting the review in the country in which the data resides with the goal of identifying the relevant information before it is transferred, minimizing the amount of PII at issue.
- **Consider redaction or anonymization.** Use of anonymization techniques or redaction of PII may address an organization's data privacy obligations.
- **Evaluate transfer options**. An organization retains responsibility for ensuring that PII is protected in accordance with the laws of its place of origin, even after the data is transferred to the United States. There are several options for such transfer, including the use of "Safe Harbor" vendors, employing the Hague Evidence Convention procedures, negotiating vendor contracts that include model contractual language or other provisions designed to ensure the data protection, or implementing strict protective orders.

PRIVACY

Online Privacy: A Global and Ageless Concern

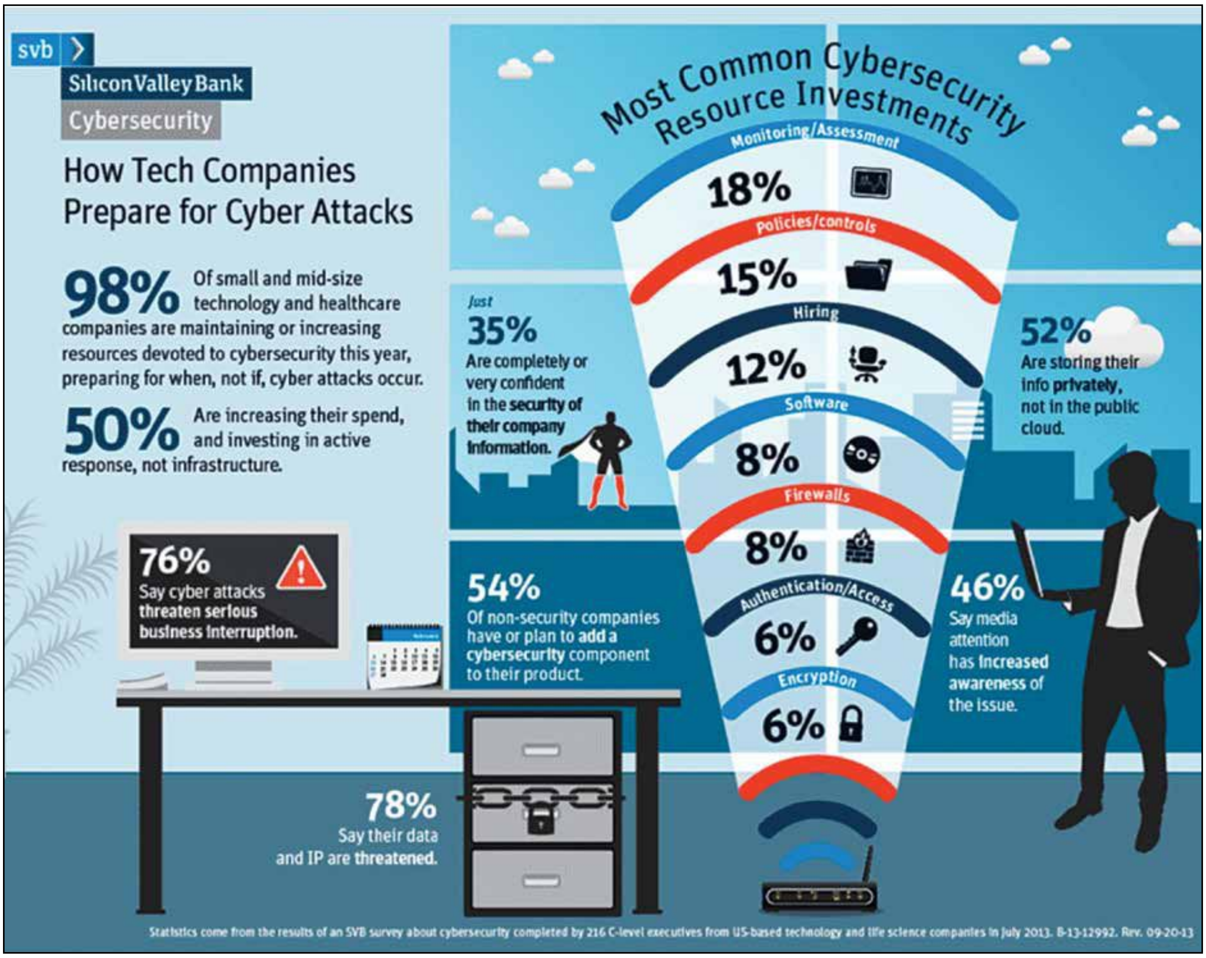
If you think teenagers and twenty-somethings don't care about online privacy, you are wrong. J.D. Power's research report "Consumer Concerns About Data Privacy Rising: What Can Businesses Do?" found that consumers believe they're losing control of their online privacy, no matter how old they are or where they live.

Findings showed that data privacy concerns increase with age. Almost 80% of 14-17 year olds said they were somewhat or very concerned about their online privacy, compared to 92% of people 67 years old or older. At least half of the people in these two age groups also report they usually or always set their social networks to private, compared to only 20% of pre-Boomers. Younger users also admitted to providing false information on websites. Nearly 30% of people 13-17 years old (Gen Z) and 18-35 years old (Gen Y) admitted to falsifying information. J.D. Power's Chief Research Officer Gina Pingitore pointed out that this could prove challenging for companies and market researchers.

The research also showed that privacy fears know no borders. The percentage of consumers in India who reported being highly concerned about privacy is equal to that of U.S. consumers (41%). Both countries were slightly lower than China, where 50% of consumers were highly concerned.

"For companies that value the use of online data as a source of consumer insight, it is important that they and the market research community work together to manage actual and perceived efforts to maintain privileged and confidential consumer privacy information," the researchers concluded.

In other words, privacy does matter, and it will continue to matter until consumers feel they have more control over how and where their information is used.



Source: Silicon Valley Bank Cybersecurity Impact on Innovation Survey, 2013

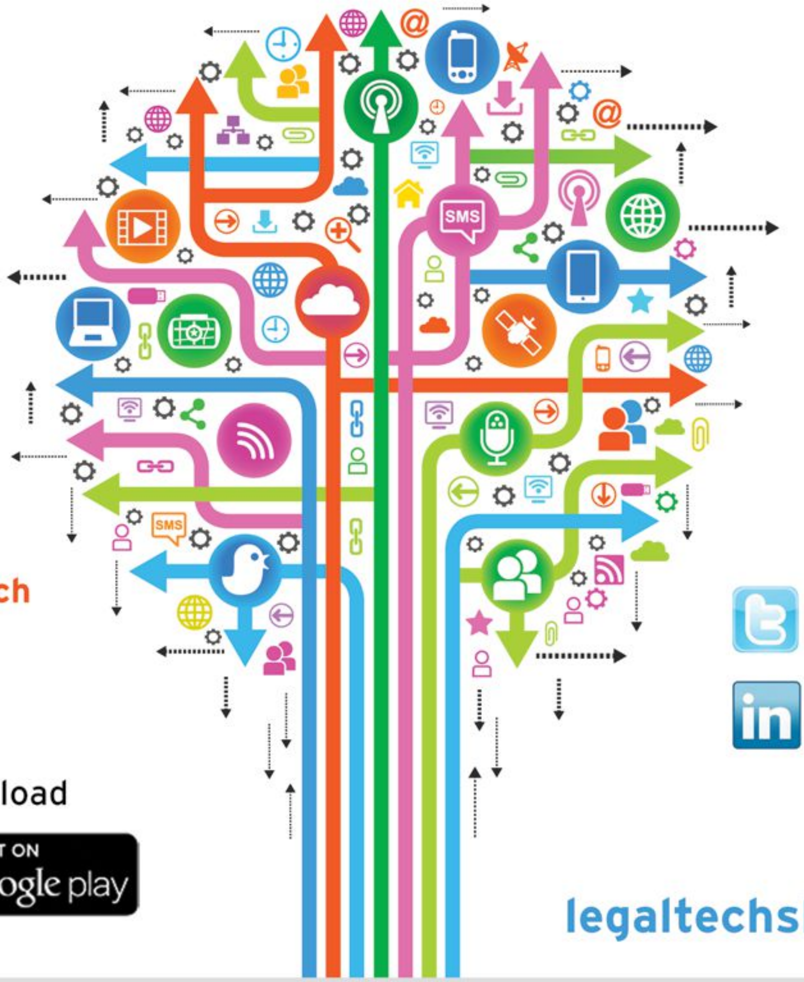
ARMA MEMBERS DISCOUNT: SAVE UP TO $170 OFF AN ALL-ACCESS PASS TO LEGALTECH! REGISTER TODAY!

LEGALTECH®

THE *MOST IMPORTANT* LEGAL TECHNOLOGY EVENT OF THE YEAR

FEBRUARY 4 - 6, 2014 | The Hilton New York

Connect. Network. Learn. Grow.



Customize your experience with the

NEW LegalTech 2014 App!

Now available for Download

Available on the App Store

GET IT ON Google play

Follow-Us
@LegalTechShow
#LTNY

Join Our Group
"LegalTech"

legaltechshow.com

EDUCATIONAL SPONSORS:

daegis The eDiscovery company. | discover ready | equivio zoom in. find out | FTI CONSULTING | TECHNOLOGY | hp | Autonomy | HuronLegal | ILDE Institute for Law Department Excellence

KIERSTED | KPMG cutting through complexity | Kroll Ontrack. | LexisNexis | nuix | PayneGroup | RECOMMIND | THOMSON REUTERS

UNITEDLEX | xerox

MATERIALS SPONSOR:

Workshare

IN ASSOCIATION WITH:

ARMA INTERNATIONAL | EDGE LEGAL MARKETING | i/+A International Legal Technology Association | KMWorld | NYSBA

ALM

INFO SECURITY

Google on the Hot Seat in EU

Changes to Google's terms of service have drawn fire from 14 European countries. On Nov. 11, Google started featuring names and photos of users in "shared endorsements," reported *PCWorld*. Thus, if a user follows a company on Google+, the user's name, photo, and endorsement could show up in the company's advertisements. When users signed up for a Google+ account, however, they were not informed that to use other Google services would mean releasing their information for commercial purposes outside the Google+ environment, according to privacy advocate Simon Davies.

That violates the European data protection law, stated Davies, who filed complaints with the data protection authorities of Norway, Sweden, the Czech Republic, Denmark, France, Spain, Italy, Slovenia, Austria, Belgium, Germany, Lithuania, the Netherlands, and Poland.

"On the basis of my initial assessment it appears that the changes will substantially violate Data Protection law," Davies wrote in the complaint. He requested that the authorities investigate and seek the immediate suspension of the changes pending the outcome of the investigation.

"The general position is that the ground rules shouldn't be changed half way through the match. Google acquired the data under one condition, and I'm asserting that it cannot change the purpose of that data after the fact," Davis said.

Although users have the right to opt out of shared endorsement programs in some companies, Davies stated that Google's opt-out mechanism creates another data protection issue. He said that opt-out mechanisms in principle do not deliver users' consent according to Europe's privacy watchdog, the Article 29 Working Party.

Google is also being investigated by data protection authorities over its policy changes that allow it to share personal data across all its products and services.

RISK MANAGEMENT

Survey Reveals Info Governance Gap in U.S.,UK Companies

Too many companies are relying on employees to self-manage their information, which may be putting them at risk. According to independent research published by Recommind, almost half (49%) of UK companies surveyed rely on employees to self-categorize data; that percentage is even higher (52%) among U.S. companies.

Interestingly, 75% of UK companies and 58% of U.S. companies claim to have an information governance policy in place, an indication that they at least understand the risks posed by their information. The over-reliance on employees to manage their own data, however, is a clear sign that they are not "tackling the issue head-on to proactively reduce risk," concluded the report. The research also found that of the U.S. companies surveyed, 82% agreed that some form of auto-categorization and tagging of data is a key component of effective information governance; 86% agreed that auto-categorization needs to be based on content and not just keywords. Only 24% of UK organizations said they knew how much data they hold. Thus it comes as no surprise that it takes an average of three hours for employees to retrieve specific information before they can begin to manage and analyze the data to understand its risks.

Attorney David Horrigan, an information governance analyst at 451 Research, pointed out that "[n]ot having a proactive [information governance] policy leaves companies open to substantial fines, litigation risk, security breaches, and compliance issues. This research shows that there are still too many organizations exposed to these unnecessary risks."

TRENDS

IDC: 3rd Platform Will Dominate in 2014

It's that time of year again. All the research analysts are issuing their predictions for 2014. The International Data Corp.'s (IDC) top-10 information and communications technology (ICT) trends, summarized in the following, were heavily influenced by the emergence of the "3rd platform" – the "emerging platform for growth and innovation built on the technology pillars of mobile computing, cloud services, big data and analytics, and social networking."

1. Worldwide IT spending will reach $2.1 trillion in 2014. It will be driven by 3rd Platform technologies, which will capture 89% of IT spending growth.
2. Emerging markets will return to double-digit growth of 10%, driving nearly $740 billion or 35% of worldwide IT revenues and, for the first time, more than 60% of worldwide IT spending growth.
3. Within the 3rd Platform, value will start to migrate "up the stack," from infrastructure as a service (IaaS) to platform as a service (PaaS) and from generic PaaS to data-optimized PaaS. Expect Amazon Web Services to roll out several PaaS offerings for developers and higher value services for businesses, forcing incumbent IT suppliers (including new-to-the-market Google) to urgently reconfigure themselves to fight for position.
4. The mobile device onslaught will continue in 2014 with sales of tablets growing by 18% and smartphones by 12%.

5. Cloud spending, including cloud services and the technology to enable these services, will surge by 25% in 2014, exceeding $100 billion. IDC expects to see a dramatic increase in the number of data centers as cloud players race to achieve global scale.
6. Spending on big data technologies and services will grow by 30% in 2014, surpassing $14 billion as demand for big data analytics skills continues to outstrip supply.
7. Social technologies will become increasingly integrated into existing enterprise applications over the next 12-18 months. In addition to being a strategic component in virtually all customer engagement and marketing strategies, data from social applications will feed the product and service development process.
8. Cloud-dedicated data centers will grow in number and importance, and the market for server, storage, and networking components will increasingly be driven by cloud service providers.
9. The 3rd Platform will deliver the next generation of competitive-advantage apps and services that will significantly disrupt market leaders in virtually every industry.
10. The 3rd Platform will continue to expand beyond smartphones, tablets, and PCs in 2014 to the Internet of Things. IDC expects to see new industry partnerships among traditional IT vendors, global telecom service providers, and semiconductor vendors to create integrated offerings.

PRIVACY

UN Adopts Internet Privacy Resolution

The United Nations (UN) General Assembly's human rights committee unanimously adopted a resolution to protect the right to privacy against unlawful surveillance. Germany and Brazil sponsored the resolution following the revelation of U.S. eavesdropping on foreign leaders, including Brazil President Dilma Rousseff and German Chancelor Angela Merkel.

According to Brazil's U.N. ambassador, Antonio de Aguiar Patriota, the resolution "establishes for the first time that human rights should prevail irrespective of the medium, and therefore need to be protected online and offline."

The Associated Press reported that the United States did not fight the resolution after successfully lobbying the "Five Eyes" Intelligence-sharing group – the United States, Britain, Canada, Australia, and New Zealand – to dilute some of the draft language. The key compromise dropped the contention that the domestic and international interception and collection of communications and personal data, "in particular massive surveillance," may constitute a human rights violation.

Despite the "watering down" of the language, the five major human rights and privacy groups – Amnesty International, Human Rights Watch, The Electronic Frontier Foundation, Access, and Privacy International – said the resolution will guarantee that the privacy issue stays on the front burner at the United Nations. The resolution directed the U.N. human rights chief to report to the Human Rights Council and the General Assembly on the protection and promotion of privacy "in the context of domestic and extraterritorial surveillance…including on a mass scale."

The unanimous vote assured the resolution's final passage by the 193-member General Assembly in December. (The final vote had not occurred as of press time.)

CLOUD

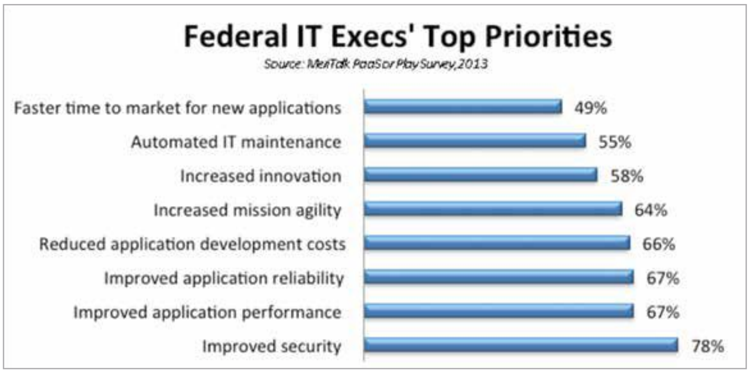
Cloud Computing Could Save Government $20 Billion a Year

A recent MeriTalk survey suggests that many U.S. federal IT professionals believe that the platform as a service (PaaS) functionality could cut federal IT costs by $20.5 billion a year by speeding up the development of software.

"PaaS or Play? Cloud's Next Move," which was underwritten by Red Hat Inc., reported on the survey of 153 federal IT professionals. The survey found that current software development is slow and expensive; the average duration for developing an application is 3.5 years.

Some 92% of the respondents believe that PaaS offers vital support for cloud computing and could reduce the development time significantly. The perceived advantages of PaaS include data center consolidation, shared services, improved agility and security, and better management of big data.

Currently, 12% of U.S. government agencies are using PaaS, 20% are transitioning to it, and 51% are considering the technology.



Source: Ponemon Institute, 2013

CAREERS
Employment Opportunities
NOW HIRING: We are seeking the most qualified workers to help our company continue to grow.

CYBERSECURITY

Cybersecurity Not Ready for Professionalization

The U.S. cybersecurity work force is too broad and diverse to be treated as a single occupation or profession, concluded a recent report from the National Research Council of the National Academy of Sciences titled "Professionalizing the Nation's Cybersecurity Workforce? Criteria for Decision Making." The researchers did, however, recognize that the cybersecurity field requires specialized knowledge and intensive advanced training; it's simply too young and diverse a discipline to introduce professional standards.

"Many aspects of the cybersecurity field are changing rapidly, from new technologies to the types of threats we face to the ways offensive and defensive measures are carried out," said Diana Burley, co-chair of the committee that wrote the report and associate professor of human and organizational learning at the George Washington University in Washington, D.C. "Premature or blanket professionalization strategies will likely hinder efforts to build a national cybersecurity workforce of sufficient quality, size, and flexibility to meet the needs of this dynamic environment."

The cybersecurity work force encompasses a wide variety of roles and responsibilities and requires an array of skills and abilities, including behavioral and management skills, as well as technical expertise. While there are indications that demand will continue to be high for cybersecurity workers, the evolving nature of the field makes it difficult to forecast the number of workers that will be required or the mix of knowledge and skills that will be needed, the report says.

There's no doubt that professionalization has its advantages, including enhancing the quality of the work force, but standardizing education or certification requirements also has disadvantages, particularly in a field where much of the work force is self-taught. Requiring formal education or training could actually deter potential employees from entering the field.

The report suggests that only specific occupations within the field should be professionalized based on how well-defined and stable they are and whether the benefits of professionalization would outweigh the costs.

In the meantime, companies and governments continue to train and encourage the development of cybersecurity experts from an early age.

CYBERSECURITY

Singapore Increases Cybersecurity Training for Youths

Singapore IT Security Authority (SITSA) hopes to increase public awareness about security threats while providing students with hands-on training based on real-world experience. The training will be provided through an advanced cybersecurity training facility in 2014, according to Masagos Zulkifli bin Masagos Muhammad, senior minister of state for Singapore's home affairs and foreign affairs, who spoke at the GovernmentWare 2013 conference.

In his opening speech to the conference, Masagos stressed the need to build a "sustainable national ecosystem," reported ZDNet. Such a system will include academic institutions and industry players working together to increase the country's cybersecurity talent pool.

Masagos also announced the release of a new interactive game, CyberShock, which is intended to raise public awareness of how national security includes cybersecurity. The game reportedly simulates the effects of a cyber attack on essential services such as power and public transportation, and participants play their part in helping to defend against the attacks.

INFO SECURITY

BYOD Brings Security Challenges

The bring-your-own-device (BYOD) trend poses serious security challenges for enterprises. A 2012 Trend Micro survey report "Mobile Consumerization Trends & Perceptions" revealed that nearly half of enterprises surveyed that allow employee-owned devices to connect to a company's network have experienced a data breach. Furthermore, 86% of the IT decision makers from the United States, United Kingdom, and Germany reported that smartphone data security is their number one concern when consumer devices are connected to corporate networks.

According to an October 13 *New York Times* article "Bolstering a Phone's Defenses Against Breaches," a handful of technology companies are trying to capitalize on the BYOD trend that people in charge of securing corporate networks say has become their biggest headache. In the past, the author wrote, they could mandate that employees use company-approved BlackBerry smartphones, which came with a tightly controlled network. However, with BlackBerry's future uncertain and an increasing number of employees requesting to use their iPhones, iPads, and Android-powered devices at work, IT managers have been forced to consider alternatives – and to deal with those alternatives' security threats.

Data security managers are struggling to keep tabs on sensitive information as employees import data to their personal devices and download mobile apps that have access to corporate assets. Experts and threat researchers warn that these applications have little or no safeguards. According to the article, in the 2013 "Application Security Testing Magic Quadrant" report, Gartner Inc. predicts that by 2015, 75% of mobile applications will fail basic security tests.

Businesses and government agencies are already finding that employees' mobile devices have become a crucial way for attackers to reach a network.

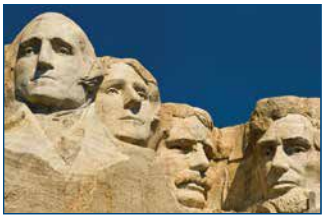
"An enormous amount of applications out there have been Trojanized," Scott Borg, the director and chief economist at the nonprofit group United States Cyber Consequences Unit, told the *New York Times*. "They have become one of the main stepping stones for getting into the enterprise."

Borg explained that the information collected from mobile Trojans "was the first step in 'spearphishing' campaigns, in which criminals use that data to tailor e-mails to employees with malicious links or attachments that, once clicked, give attackers a foothold into companies' systems."

In a recent press release, Gartner predicted that 30% of consumer product selection criteria will be based on requirements to secure new mobile computing platforms by 2015. The research firm encourages product managers to include all mobile device platforms alongside traditional desktops and laptops when assessing and deploying security measures. Pricing is especially important since consumers have shown they are less likely to pay for security programs for their mobile devices.

DIGITAL PRESERVATION

Building a Cyber Archive of the World's Monuments



Imagine if Mt. Rushmore or the ancient pyramids disappeared from the earth. How could they ever be replaced? Thanks to the efforts of the nonprofit CyArk (abbreviated from Cyber Archive), these and hundreds of other monuments are being digitally preserved using 3-D laser scanning technology, which can be used to reconstruct the damaged or destroyed monument.

CyArk is partnering with more than 170 organizations around the world to scan the 500 most at-risk places within five years, after which it will document another 500, and another 500 after that. The CyArk 500 project launched in October 2013; at that time 40 sites had been digitally preserved.

CLOUD

How Green Is Your Cloud?

Adoption of the cloud as a viable IT solution has grown exponentially during the past several years. In 2010, Forrester Research found that cloud investments were valued at $40.7 billion; by the end of 2013 it was expected to reach $150 billion as businesses of all sizes realize its increasing viability.

The rationale for moving IT services to the cloud centers on increasing efficiency and efficacy. Some also see it as an environmentally responsible choice; they consider the cloud to be a key feature of IT environmental sustainability.

According to the nonprofit association Business for Social Responsibility (BSR), cloud services are positive for sustainability: "The cloud encourages important clean-tech applications like smart grids and it also encourages consumers to use virtual services such as video streaming to replace resource-heavy physical products. The cloud also draws resources to where they are used most efficiently and its jobs tend to be cleaner and safer than those of more traditional industries."

Another nonprofit group, the Carbon Disclosure Project, estimated in a 2011 report that large U.S. companies that use cloud computing can achieve annual energy savings of $12.3 billion and annual carbon reductions equivalent to 200 million barrels of oil – enough to power 5.7 million cars for a year. Additionally, Pike Research predicted in its 2011 "Cloud Computing Energy Efficiency" report that data center energy consumption will drop 31% from 2010 to 2020 as a result of increased adoption of cloud computing.

On the flip side, data centers tend to have a sizeable carbon footprint. BSR stated that the majority of the top U.S. data centers are fueled by coal: it's inexpensive but dirty. To be environmentally sustainable, data centers need to draw their power from renewable energy sources.

Google has made significant investments in renewables and is using that energy to power 34% of its business. It recently entered into two 20-year agreements to purchase power from a wind energy developer with locations in Iowa and Oklahoma, two states in which Google operates large data centers. Recognizing the business opportunity presented by its impressive investment of more than $1 billion in renewable energies, Google formed Google Energy, a subsidiary that allows it to buy and resell electricity to wholesalers.

Yahoo and Facebook have made notable strides by locating to sites where they could secure large amounts of existing hydropower. Yahoo expanded its data center in Lockport, N.Y., which is drawing power from Niagara Falls; and Facebook built a 100% hydroelectric-powered operation in Lulea, Sweden, earlier this year.

It's likely we'll see more of these types of investments as more and more cloud services are powered by renewable energy.