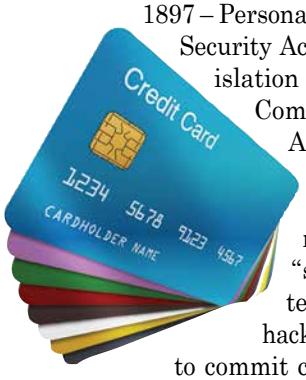
INFO SECURITY

Data Security Bills Await Action in U.S. Senate – Again

The recent Target and Neiman Marcus breaches have drawn a good deal of attention and provided extra fuel for the introduction of two bills in the U.S. Senate in early January.

Sen. Patrick Leahy (D-Vt.) cited the breaches when reintroducing S. 1897 – Personal Data Privacy and Security Act of 2014. The legislation would update the Computer Fraud and Abuse Act (CFAA) to allow the U.S. Justice Department to prosecute "significant" attempts of computer hacking and conspiracy to commit computer hacking. Key provisions in the bill include:



- Tough criminal penalties for individuals who intentionally or willfully conceal a security breach involving personal data when the breach causes economic damage to consumers
- A requirement for companies that maintain personal data to establish and implement internal policies to protect data privacy and security

The U.S. attorney general would also be required to report annually to Congress the number of criminal cases filed under the CFAA that were based solely on the defendant either accessing a nongovernmental computer without authorization or exceeding authorized access.

Leahy first introduced the bill in 2005 and has reintroduced it in the last four congressional sessions.

Less than two weeks later, Senators Roy Blunt (R-Mo.) and Tom Carper (D-Del.) introduced S. 1927 – Data Security Act (DSA) of 2014. This bill would replace a patchwork of state laws with a single set of requirements for public and private institutions to follow to prevent and respond to data breaches such as the one experienced by Target. The current bill builds on existing law such as the Gramm-Leach-Bliley Act of 1999.

If the financial establishment, retailer, federal agency, or other entity determines that sensitive information was compromised or may have been compromised, the DSA requires the organization to investigate the scope of the breach, the type of information compromised or potentially compromised, and whether the information could be used to cause an individual harm or to perpetrate bank fraud. If indeed the information was compromised and will cause harm, the organization must notify the appropriate federal government regulatory agency, law enforcement agency, and national consumer reporting agencies (if more than 5,000 individuals are affected), as well as the actual individuals whose information was breached.

Both bills are now in committee: Leahy's is in the Senate Judicial Committee (which Leahy chairs) and the Blunt-Carper bill is in the Committee on Banking, Housing and Urban Affairs.

CLOUD

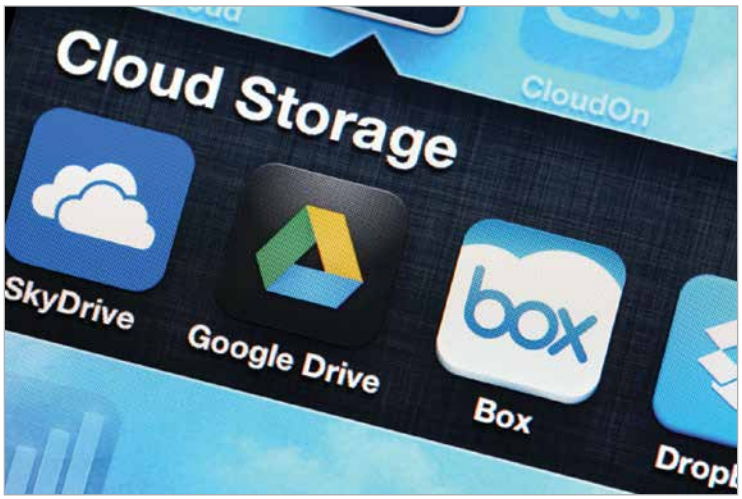
Deadline Draws Near for Cloud Vendor Accreditation

Cloud service providers have until June to be accredited by the Federal Risk and Authorization Management Program (FedRAMP) if they want to continue to service U.S. federal agencies. FedRAMP is a government-wide, standardized approach to cloud security assessments and the continuous monitoring of the assessments and authorization. Federal agencies are allowed to use only cloud products and services that have been accredited by FedRAMP.

Maria Roat, the program's director within the General Services Administration, advised providers and federal agencies in December to work directly with the FedRAMP office and to get the review process underway soon because the process is a lengthy one. Providers working directly with FedRAMP should expect the process to take four to five months to complete, while those going it alone can expect it to take six months, according to an article on *TalkinCloud.com*.

The new accreditation program is a "do once, use many times" framework that will eliminate previous redundancies. Each agency currently manages its own security risks and provides ongoing security assessments and authorizations for each IT system it uses, even if that system is being used by other agencies.

FedRAMP is mandatory for all low- to medium-risk federal agency cloud deployments and service models; private deployments intended for single organizations and implemented fully within federal facilities are excluded.



E-DISCOVERY

Cloud Can Complicate Discovery

As the cloud grows, so does the number of places where individuals and corporations can store information that may be discoverable. Dropbox and Google Drive, both of which provide cloud storage, are reportedly two of the most popular free applications downloaded on Apple and Android devices.

A subpoena sent directly to one of these application providers will likely meet a motion to quash based on Title II of the Electronic Communications Privacy Act (also known as the Stored Communications Act or SCA). In "Discovery Difficulties Presented by Cloud Computing" in *The National Law Review*, J. Michael Nolan III, of Jackson Lewis PC, cited *Crispin v. Christian Augigier Inc.*, in which "the court found … that the SCA was passed by Congress to prohibit electronic communication service providers, such as Facebook and Myspace, from revealing the contents of communications electronically stored to anyone other than the addressee or other intended recipient." The better option may be to subpoena the plaintiff or defendant app user to obtain electronically stored information in the cloud

Nolan also wrote that in the ongoing case of *Integral Development Corp. v. Tolat,* the court ordered the defendant to return any proprietary information he possessed on any storage medium, including Dropbox. Dropbox opposed the subpoena based on the SCA, so the court ordered that the Dropbox data be produced directly to the defendant's attorney, who in turn was ordered to turn it over directly to the plaintiff's forensic expert to determine whether any relevant information had been uploaded, transferred, or deleted from the Dropbox account.

Because viewing the file on an end-user's computer would have changed the metadata, there were two options for providing this information: 1) Dropbox could generate a complete forensic report that included information about who accessed the cloud account or 2) the information could be reconstructed by accessing each computer that had synchronized with the account – a very labor-intensive (and therefore costly) alternative. The court chose the latter.

INFO SECURITY

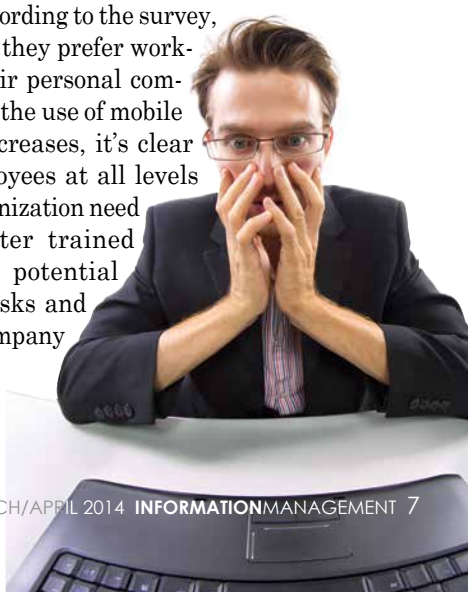
Senior Managers Behaving Badly

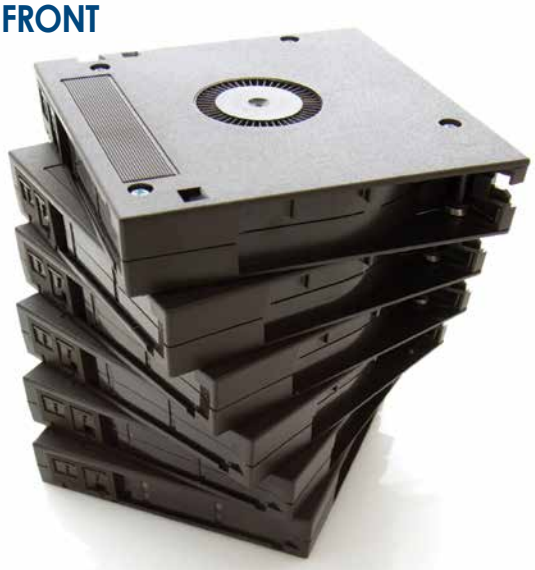
Oftentimes the biggest risk to your data's security comes from inside the company … from senior management.

"On the Pulse: Information Security Risk in American Business," a recent survey by digital risk managers at Stroz Friedberg, revealed that more than half of the respondents don't think U.S. companies are adequately securing their information (61%). Nearly three-quarters (73%) said a hacker could break into their employers' computer networks and steal their personal information.

Many respondents admitted to engaging in high-risk behaviors, such as uploading work files to their personal e-mail and cloud accounts (87%) and accidentally sending sensitive information to the wrong person (58%). Senior managers – who typically have high levels of access to valuable company information – were among the worst offenders. Indeed, 87% of senior managers said they upload work files to their personal accounts. More than half (51%) confessed that they have also taken files with them when leaving a previous job. These behaviors mean proprietary information could easily fall into the wrong hands.

The main reason senior managers upload work files to personal accounts, according to the survey, is because they prefer working on their personal computers. As the use of mobile devices increases, it's clear that employees at all levels in the organization need to be better trained about the potential security risks and current company policies.





INFO SECURITY

Data Backup and Migration Continue to Vex Enterprises

A new data management survey of 3,500 IT professionals revealed that even though the volume of data companies are managing is growing up to 40% annually, IT professionals lack confidence in their companies' data backup and migration processes. Almost 40% of the respondents said they've experienced data loss, and 83% either have no disaster recovery plan or are not entirely confident about their plan.

"We found that … companies are not protecting or backing up their data as often, for fears of security, manpower costs, or downtime," said Marty Gilbert, vice president of marketing for Vision Solutions, which conducted the survey. "Data recovery strategies are not evolving or being tested at nearly the rate they should be; with so many data breaches and disasters in the news, it's puzzling why corporations aren't moving at light speed to protect this data – the backbone of their business."

The survey also found that:

- Use of tape is the most predominant method of data backup (81% of companies) and is at a four-year high; meanwhile, software-based backup strategies are only inching up, barely above 50%.
- More than 60% of companies delayed a data migration, largely because of downtime (47%) and lack of resources (36%).
- Four out of five companies have never taken a complete business approach to migration or calculated the true cost of migration downtime.
- Only 39% of organizations test disaster recovery plans annually; 8% had no disaster recovery plan at all.

INTERNET

FCC Loses Battle for Net Neutrality

The U.S. Federal Communications Commission (FCC) may have lost the battle over "net neutrality" because of a recent court ruling, but it hasn't necessarily lost the war.

For some time, the FCC has been trying to ensure free and equal access to the Internet to all content providers, the same as it does for common carriers such as telephone companies. A U.S. appeals court, however, has ruled the FCC has been overstepping its authority because Internet providers are classified as broadband carriers, which are regulated differently.

The reaction to the court's decision has been varied: some have shrugged it off while others worry it could be the end of the Internet as we know it. Still others point out that even though the FCC lost this particular battle, it won an even bigger one because the court reinforced the commission's contention that Congress has given it the authority to regulate the Internet.

"While the court deemed that the FCC's Open Internet rules were based on faulty logic, it gave the agency a blueprint to revise its argument so that the rules would stick," summarized Maggie Reardon in a recent *CNet* article.

Judge Laurence Silberman of the U.S. Court of Appeals for the District of Columbia Circuit dissented in part to the court's ruling. While he agreed the FCC could not regulate broadband services under common carrier rules, he disagreed with the other justices' interpretation of the FCC's authority for regulation. He added that the court's decision grants the "FCC virtually unlimited power to regulate the Internet," which was not the intent of Congress when it passed the Communications Act.

FCC Chairman Tom Wheeler responded that the FCC's authority to regulate broadband networks had always been the intent of Congress, and he would make sure the agency does not use its powers gratuitously.

"No one got what they wanted out of this decision," said Harold Feld, senior vice president with Public Knowledge, a nonprofit whose mission is to preserve the openness of the Internet. "Confusion over the proper role of the FCC is greater than ever."

E-DISCOVERY

Some U.S. Courts Seeking Discovery Details

Several recent federal cases indicate that U.S. courts are becoming increasingly engaged in assessing the details of e-discovery, such as whether the correct search terms or custodians have been identified, according to Daniel J. Weiss, a partner at Jenner & Block, in a recent *Lexology* article. He cited the following three cases as evidence:

American Home Assurance Co. v. Greater Omaha Packing Co.: The court ordered a party that had produced very few e-mails to "disclose the sources it has searched or intends to search and, for each source, the search terms used."

Swanson v. ALZA Corp.: The court ordered a party to apply several search terms (including Boolean operators) to a database of collected electronic information and produce the results to the requesting party. The court also reviewed the requested search terms in detail and determined that about half of the terms should be applied even though more than 600,000 pages of electronic documents had already been produced.

Banas v. Volcano Corp.: The court reviewed a party's e-discovery effort and faulted the party for not searching the e-mail of several custodians.

INTERNET

Global Commission Tackles Internet Governance

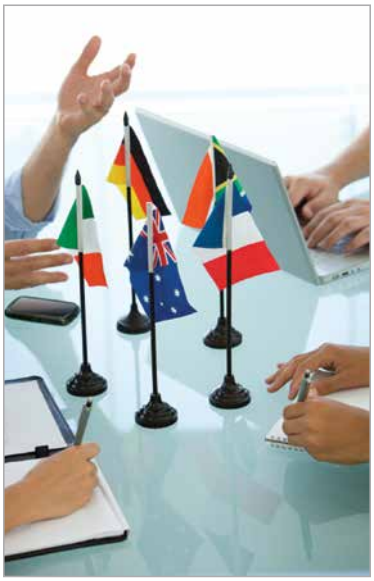
International concern over the reports of mass online surveillance by the United States and some of its allies was a hot topic of discussion in January at the World Economic Forum in Switzerland. In response, The Centre for International Governance Innovation and the Royal Institute of International Affairs (Chatham House), two independent global think-tanks, announced the launch of the Global Commission on Internet Governance.

The 25-member group, chaired by Sweden's foreign minister, Carl Bildt, is undertaking a two-year investigation into the various ways governments use Internet data. Its goal is to produce "a comprehensive stand on the future of multistakeholder Internet governance."

"In most countries, increased attention is being given to all the issues of net freedom, net security, and net governance," said Bildt. "The rapid evolution of the net has been made possible by the open and flexible model by which it has evolved and been governed. But increasingly this is happening as issues of net freedom, net security, and net surveillance are increasingly debated. Net freedom is as fundamental as freedom of information and freedom of speech in our societies."

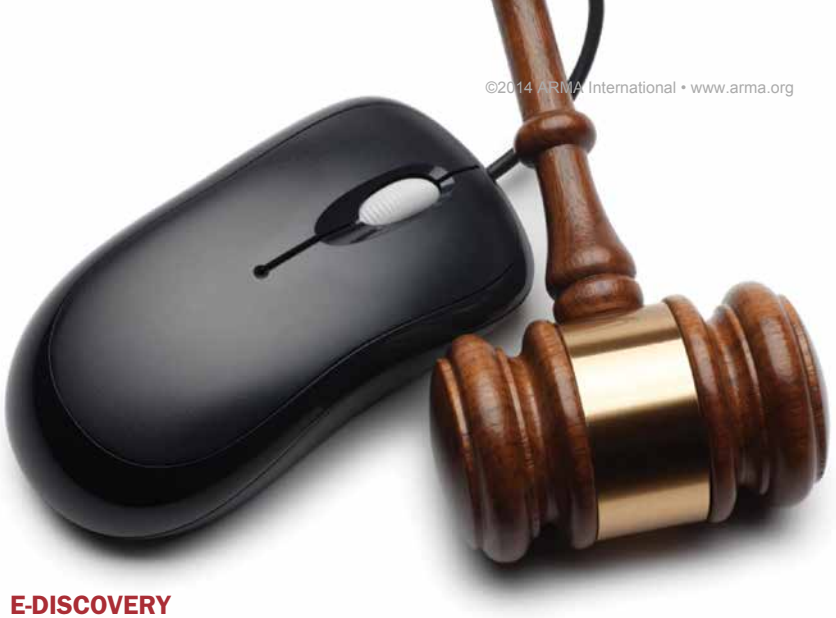
The commission will investigate a wide range of topics within four key themes:

1. *Enhancing governance legitimacy* – including regulatory approaches and standards
2. *Preserving innovation* – including critical Internet resources, infrastructure, and competition policy
3. *Ensuring rights online* – including establishing the principle of technological neutrality for human rights, privacy, cybercrime, and free expression
4. *Avoiding systemic risk* – including establishing norms regarding state conduct, cybercrime cooperation, and proliferation and disarmament issues



"Internet governance is too important to be left just to governments," said Patricia Lewis, research director of Chatham House's International Security Department. "The Internet is a fundamental part of the global economy and how we manage its future will be decisive in facilitating development for all."

The commission comprises technology experts from various sectors, as well as academics and policy and government specialists. Its members include Sir David Omand, the first security and intelligence coordinator for the United Kingdom and a former director of the UK's Government Communications Headquarters (a British intelligence agency), and Michael Chertoff, a former secretary of the U.S. Department of Homeland Security.



CLOUD

Copyright Violations Shut Down Cloud Storage Site

One of the most used file-sharing sites on the Internet, Hotfile, went dark in early December as a result of copyright infringement charges filed against it by the Motion Picture Association of America (MPAA). Hotfile was facing a possible $500 million fine had the case proceeded to court; instead the two parties settled for $80 million. The deal, approved by the U.S. District Court for the Southern District of Florida, required Hotfile to start using "digital fingerprinting" technology to filter copyright-infringing content or shut down its operations.

Implementing filtering techniques is a drastic step, but not an unusual one in the file-hosting business, reported *TorrentFreak*, an online publication focused on copyright and other issues related to digital file sharing. *TorrentFreak* noted that cyberlocker MediaFire uses digital fingerprinting technology and remains the most-used storage site on the Internet.

Hotfile, however, chose to shut down its operations rather than implement the filtering technology. It did so within hours of the settlement announcement and without first notifying its millions of individual and business users. Those users who hadn't backed up their virtual site to an alternate site were left adrift.

E-DISCOVERY

No Major E-Discovery Issues in 2013

Looking back, it was all quiet on the e-discovery front last year. "No earth-shattering opinions, no imprisoned spoliators, and barely a whimper from reported decisions related to parties' chosen form of production," observed Cecil Lynn, director of e-discovery and technology at eBay, and Lauren Schwartzreich, e-discovery counsel at Littler Mendelson, in a recent *Law Technology News* article.

"Perhaps the bench and bar are getting more sophisticated and technology savvy," they hypothesized. "Or perhaps the courts implicitly recognized the current state of flux, what with the proposed amendments to the Federal Rules of Civil Procedure (FRCP) that specifically address [electronic data discovery]. Or possibly, the industry is evolving from what was once considered cutting-edge and novel to what is emerging as best practices."

As in previous years, judges reinforced their expectation of cooperation with the electronic data discovery (EDD) competency. The Eastern District of Michigan went so far as to develop a "Meet and Confer Checklist and Model Order Related to the Discovery of Electronically Stored Information."

The courts also continued to focus on the parties' efforts to streamline discovery and consider the cost and burdens associated with their discovery requests, as well as on cost shifting, not only between parties but also for expenses incurred by non-parties. Even when the non-party and a party share an interest in the subject matter of litigation – a factor that weighs against cost shifting – one court held that the sheer volume of discovery tipped the balance in favor of shifting EDD-related expenses.

In 2012 many in the industry predicted there would be more movement in the use of predictive coding in 2013, but there was relatively little discussion of the use of technology-assisted document review. The authors noted that case law underscored that traditional keywords and document review may appropriately be used in conjunction with technology-assisted review.

"While 2013 did not produce any 'bombshell' e-discovery opinions," they concluded, "it did underscore that EDD standards are far from settled, including because of variances among circuits (and oftentimes individual judges). Whether the proposed amendments to the FRCP that address EDD will bring more uniformity to the field remains an open issue for 2014."

CYBERSECURITY

Financial Exchanges Unite Against Hackers

The World Federation of Exchanges (WFE) has decided it's time for the global financial exchanges to work together to thwart cyber attacks. The federation recently announced the formation of the Cyber Security Working Group, the exchange industry's first cybersecurity committee. Its mission is to help protect global capital markets by collaborating on best practices for protecting their infrastructures.

More than half the world's exchanges were victims of cyber crime in 2013, according to a paper published last summer by the WFE and the International Organization of Securities Commissions. Fortunately cyber attacks on stock markets have thus far focused on non-trading-related online services and websites and haven't come close to knocking out critical systems or trading platforms. Furthermore, most of the exchanges are confident in their protocols and preparedness.

That being said, 83% of the exchanges agree that cyber crime in securities markets should be considered a systemic risk because of its potential effect on confidence and reputation, market integrity and efficiency, and financial stability. The exchanges are united in their belief that a broader, system-wide response is needed.

Mark Graff, NASDAQ's chief information security officer, will chair the committee, which will include representation from more than a dozen exchanges and clearinghouses around the world.

CLOUD

China Is New Cloud Frontier

Many in the cloud industry are banking on China. In December, Amazon made headlines by announcing that it will extend its cloud-computing services – Amazon Web Services (AWS) – to China in 2014. *Xinhuanet.com* reports that AWS signed a memorandum of understanding with Beijing and Ningxia for jointly constructing and developing cloud services for Chinese clients. The business office will be located in Beijing and the data center in Ningxia. The AWS China deal is part of Ningxia's plan to build a cloud base that eventually will be able to house 1 million servers.

Amazon's entry into the China market sparked an impressive flurry of activity. Only hours before Amazon publicized its plans, Allyun – the cloud-computing arm of China's e-commerce giant Alibaba Group Holding – announced it was cutting its cloud service prices by as much as 35%. Shortly after Amazon's declaration, IBM said it would be teaming up with a local partner to provide cloud services to Chinese enterprises. The country's two largest mobile operators – China Mobile and China Unicom – announced earlier in December that they had begun construction of cloud computing facilities in Guizhou Province.

Although many Chinese companies currently offer cloud services, only Allyun comes close to AWS in size and is expected to feel the pressure of its entry in the Chinese market. Qian Lili, an analyst with Analysys International, told Xinhuanet that AWS China's arrival may not completely change the market landscape, but it will likely push out some of the small players. Other analysts contend the National Security Agency spying scandal could adversely affect AWS China's influence.

CYBERSECURITY

Kroll: Organizations Get Serious About Security in 2014

Kroll's recently released 2014 Cyber Security Forecast highlights seven trends that indicate changing tides in cyber standards and the need for organizations to take stronger actions to protect themselves from financial, legal, and reputational risks.

1. **Security frameworks such as the National Institute of Standards and Technology (NIST) Cyber Security Framework will become *de facto* standards.** "This trend will move the United States in the direction of the EU, where there is a greater recognition of privacy as a right," said Alan Brill, senior managing director at Kroll. Whether compulsory or unstated, these standards will drive decision-making in organizations that want to protect themselves from shareholder lawsuits, actions by regulators, and other legal implications.
2. **The data supply chain will continue to challenge even the most sophisticated organizations.** Contracting with third parties to store or process data will continue to be commonplace, making it imperative that companies closely vet their subcontractors as to their technical and legal roles and responsibilities in the event of a breach. This requires technical, procedural, and legal reviews.
3. **The malicious insider will remain a serious threat but will become more visible.** Kroll predicts that in 2014 a significant number – if not almost half – of data breaches will come at the hands of people on the inside. However, as the federal government and individual states add muscle to privacy breach notification laws and enforcement regimes, the hidden nature of insider attacks will become more widely known.
4. **Corporate board audit committees will take a greater interest in cybersecurity risks and how the organization plans to address them.** Data breaches pose significant threats to the organization's reputation, compliance efforts, and financial well-being, putting it squarely in the lap of corporate audit committees. "As corporate boards carry out their fiduciary responsibilities, they must also protect the company from possible shareholder lawsuits that allege the company's cyber security wasn't at a level that could be reasonably viewed to be 'commercially reasonable' and that incident response plans weren't in place to mitigate the risk," said Brill.
5. **Sophisticated tools will enable smart companies to quickly uncover data breach details and react faster.**
6. **New standards related to breach remediation are gaining traction and will have a greater impact on corporate data breach response.** Credit monitoring will no longer be the gold standard in breach remediation in 2014, as lawmakers, consumer advocates, and the public at large continue to question the relevancy and thoroughness of this as a stand-alone solution. The Federal Trade Commission and states like California and Illinois are already suggesting a risk-based approach to consumer remediation – one that matches remedy to individual risk based on the unique circumstances of a breach.
7. **As more organizations adopt the cloud and BYOD, they will be held accountable for implementing policies and managing technologies.**

E-DISCOVERY

Copyright Infringement on the Internet

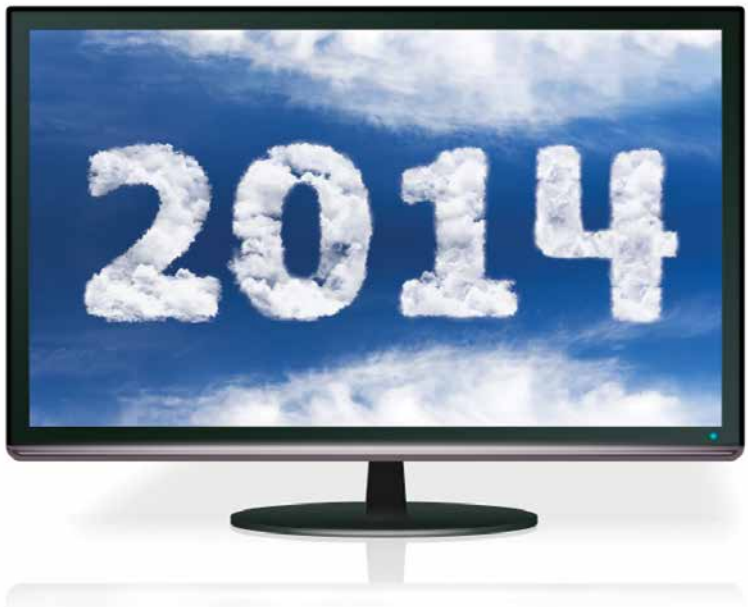
400%
the increase in copyright infringement cases from 2012 to 2013.

235M
Number of takedown requests Google received from copyright holders in 2013.

50M
Number of takedown requests Google received in 2012.

10M
Number of takedown requests Google received in 2011.

A significant number of the requests came from the music industry's anti-piracy groups BPI and RIAA (41.7 million and 30.8 million, respectively).



CYBERSECURITY

Prediction for 2014: Expect More Cybersecurity Challenges

Coalfire, an independent IT security business, welcomed the new year with its predictions for the top cybersecurity trends expected in 2014. Organizations should be prepared to identify or respond to the following emerging risks:

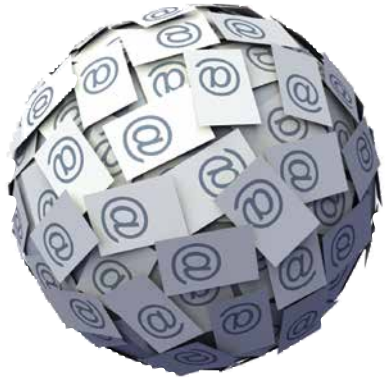
1. **There will be a significant security breach at a cloud service provider that causes a major outage.** Businesses must evaluate the risk within their third-party cloud service provider systems to protect sensitive information, including trade secrets and intellectual property.
2. **The migration from compliance to IT risk management will accelerate.** Risk and compliance management firms need to be more in tune with their clients' business needs – more proactive than reactive.
3. **Emerging threats will shift security programs from static boundary protection to more proactive monitoring and response programs.** Expect more virulent types of attacks that will be significant enough to require more proactive monitoring and response.
4. **There will be a significant increase in malware for Android phones, and malware will begin to affect iPhones, too.** Smartphones are woefully unprotected from malware as users harbor a false sense of security.
5. **The number of data breaches in health care caused by business associates (BAs) will increase dramatically because of the Omnibus Rule.** The Omnibus Rule required that all BAs be HIPAA compliant by September 23, 2013. Unfortunately, many organizations don't know they are BAs and are ignoring the requirements, increasing their vulnerability.

E-DISCOVERY

Court: 'Saved Everything' Defense Not Good Enough

If you think you don't need to issue a formal legal hold because your policy is to save everything, think again.

A California magistrate judge recently reminded a party of that. It seems the party neglected to issue a legal hold when it became apparent that litigation was likely. As it turns out, e-mails from key players were destroyed in the absence of a legal hold. The defendant later argued that it had a company-wide "no documents are to be deleted" policy that was equivalent to a legal hold. The judge disagreed.



"Although defendants argue that there was no need for a litigation hold because of their document retention policy, it is obvious that defendants' document retention policy did not prevent documents from being destroyed," the court said. "Further, defendants did not have a back-up system to prevent the destruction of documents…."

The court approved the adverse inference instructions and ordered monetary sanctions in the form of attorney fees and costs.

BYOD

Forrester: Act Now to Stamp Out BYOD Risks

If you can't beat them, join them." That adage fairly summarizes the results of a recent Forrester study of the legal implications related to a bring your own device (BYOD) policy, "Navigating the Legal and Compliance Applications of BYOD." According to a January 13 Forrester blog by David Johnson, a co-author of the study, technology attorneys participating in the study agreed that "once you learn that BYOD is happening in your organization, you have a legal obligation to do something about it, whether you have established industry guidance to draw on or not." In other words, you must take action to minimize the risk.

If only it were as easy as it sounds. As pointed out by Johnson:

- The more restrictions you put in place, the more incentive people will have to work around them and the more sophisticated and clandestine their efforts will be.
- There is no data leak prevention tool for the human brain, so arguably the most valuable and sensitive information walks around on two legs and leaves the building every night. Accepting this is important for keeping a healthy perspective about information risk on employee-owned devices.

Despite the challenges, organizations need to address the issue. Intellectual property misuse and accidental data loss are the top BYOD risks cited by Forrester. Patent, trademark, and copyright infringement may be very common, wrote Johnson, but they also are next to impossible to police with technical controls.

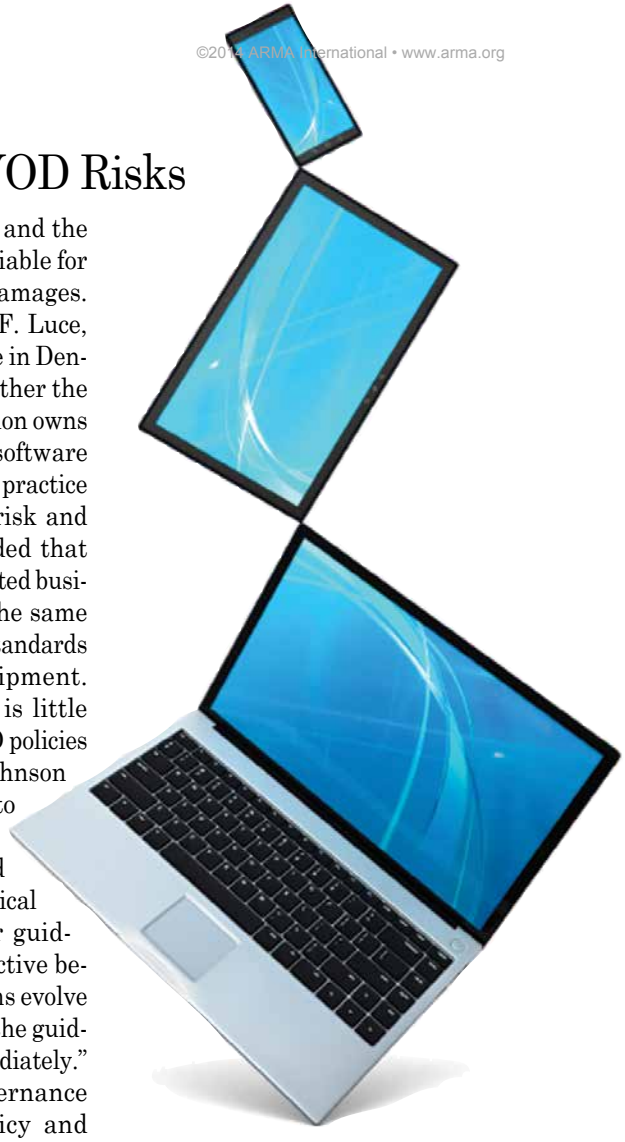
For example, Johnson wrote, if attorneys can prove that employees are using software that is not properly licensed for the organization's business purposes, it can be considered "willful and illegal misuse of someone else's property," and the organization can be held liable for past licensing fees and damages.

According to Charles F. Luce, Jr., partner at Moye White in Denver, it doesn't matter whether the employee or the organization owns the device on which the software is installed. Charles Gray, practice manager for Accuvant's risk and compliance business, added that any device used in a regulated business needs to adhere to the same regulations and industry standards as company-owned equipment.

Unfortunately, there is little specific guidance for BYOD policies and technical controls. Johnson noted that auditors tend to look to the U.S. National Institute of Standards and Technology's (NIST) technical control specifications for guidance, but "it's often subjective because devices and platforms evolve so quickly that it renders the guidance obsolete almost immediately."

Effective BYOD governance starts with a clear policy and education. Johnson stated that a signed BYOD agreement with each employee, along with adequate education on the risks and employees' responsibilities, are the absolute minimum controls that should be in place. He also recommends electronically enforcing policies for employees incapable or unwilling to do their part.

"A viable BYOD strategy addresses culture, responsibilities, education, policy, and technical controls. It recognizes the value that BYOD brings to employee engagement and performance and features a clear agreement between the organization and each BYOD employee that outlines what each is responsible for. Technology's role is to help foster safe behaviors, control information access, and verify ongoing compliance – all without getting in the way of creativity, productivity, collaboration, or other daily activities," Johnson wrote.



Forrester suggests creating a technology approach that promotes engagement while enforcing the policy. This means keeping employee-owned devices off of the corporate trust network while allowing access to information through secure proxies and interfaces. In regulated environments, it also means sensitive data is never stored on employee-owned devices, but in less stringent environments it can mean simply controlling access to systems of record such as customer databases to prevent anyone from walking away with a data dump.

CYBERSECURITY

NIST Presents Cybersecurity Standard

In February the U.S. Commerce Department's National Institute of Standards and Technology (NIST) released the first version of the "Framework for Improving Critical Infrastructure Cybersecurity." It was presented exactly one year after President Obama issued an executive order directing the agency to collaborate with industry to create a voluntary framework for managing cybersecurity-related risk.

According to NIST, the framework uses a common language to manage cybersecurity risk in a cost-effective way based on business needs without placing regulations on businesses. It focuses on using business drivers to guide cybersecurity activities and on considering cybersecurity risks as part of the risk-management process.

Per the executive order, the framework also provides guidance on how organizations can incorporate the protection of individual privacy and civil liberties into the program.

NIST has stressed that the framework is not a one-size-fits-all approach to managing cybersecurity risk. "Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances – and how they implement the practices in the framework will vary."

The framework is generally regarded as a good first step, but some don't think it goes far enough. Ann M. Beauchesne, vice president of national security and emergency preparedness for the U.S. Chamber of Commerce, stated: "[T]he Chamber believes that the framework will be fundamentally incomplete without the enactment of information-sharing legislation. Businesses need policies that foster public-private partnerships – unencumbered by legal and regulatory penalties – so that individuals can experiment freely and quickly to counter evolving threats to U.S. companies."

Greg Nojeim, director of the Center for Democracy and Technology's Project on Freedom, Security and Technology said: "The framework will be useful to companies and their privacy officers, because it will remind them that processes should be put in place to deal with the privacy issues that arise in the cybersecurity context. However, we are concerned that the privacy provisions in the framework were watered down from the original draft. We would have preferred a framework that requires more measurable privacy protections as opposed to the privacy processes that were recommended."

NIST noted that the framework "is a living document and will continue to be updated and improved as industry provides feedback on implementation." **END**