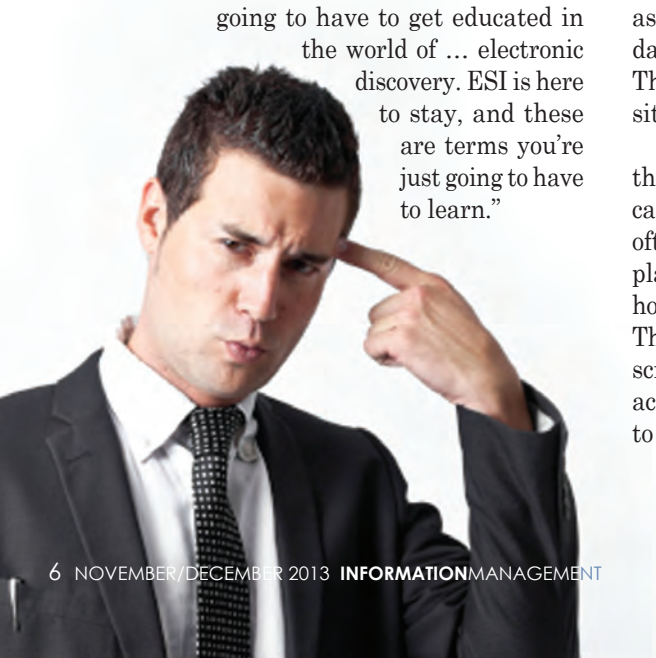
E-DISCOVERY

Court: Ignorance About E-Discovery Is No Excuse

For years attorneys have been advised to become better educated about the ins and outs of electronically stored information (ESI). Failure to do so has recently cost one California attorney $165,000.

According to an article in *Lexology, a California appellate court recen*tly imposed the monetary sanction against an attorney who didn't follow directions well when instructed to allow forensic examinations of her computers during a class action suit. When ordered to produce the records in question in their "native format," the attorney promptly converted the records into PDF and deleted the original Word documents. The trial court then ordered the forensic examination of the attorney's computers, which the attorney refused to allow.

During the discovery dispute, counsel for the attorney reportedly told the court she "[didn't] even know what 'native format' means." The court responded: "You'll have to find out. I know. Apparently [opposing counsel] knows. You're going to have to get educated in the world of … electronic discovery. ESI is here to stay, and these are terms you're just going to have to learn."



CLOUD

Think Cloud, Re-think Disaster Recovery

Add business continuity to the list of considerations if you're deciding whether to move to the cloud. Using it for even the basic purpose of data backup could significantly improve your organization's ability to recover from a disaster.

While most large companies have a backup strategy, many are not sending their data offsite — or far enough offsite — to mitigate geological or meteorological risks, according to Richard Cocchiara, CTO and managing partner of consulting for IBM's Business Continuity and Resiliency Services. "Cloud gives them the ability to store data someplace remote, store it online, and to typically recover faster than from tape," he recently told *Network World*.

Cocchiara said that companies with sophisticated disaster recovery architectures and strategies may benefit from the cloud from financial and control perspectives, for example, because they can test cloud disaster recovery more often. These companies, though, often face the challenge of creating an integrated strategy of processes, architecture, and reporting that is necessary to demonstrate their business continuity capability to auditors, he said.

The cloud levels the playing field for small and medium-sized businesses (SMBs), which are not likely to be able to afford the same protection as larger companies. For example, SMBs typically don't have secondary data centers; they usually rely on tape backups that are stored locally. The cloud enables them to back up data or replicate servers to a remote site and to network to that site when there's a disaster.

Cocchiara reminded all companies, regardless of size, to make sure their business continuity plan is in the cloud so it will be accessible in case of a disaster. "I know it seems like a nit, but you'd be surprised how often business continuity plans are lost in a disaster," he said. "Those plans are critical and if they're stored on a system in the primary center, how are you going to run the recovery if you can't get to that system? The cloud gives them the ability to store those plans and the notification scripts on a server they can access from their laptop anywhere they can access the cloud. And for a business continuity manager, that's critical to their success."

E-MAIL

NY Court Rules E-mail Signatures Valid

A U.S. state of appeals panel recently ruled that signing your name to an e-mail is comparable to physically signing a printed document. This is the third appeals panel to support the validity of e-mail in contractual negotiations.

"Given the widespread use of e-mail as a form of written communication in both personal and business affairs, it would be unreasonable to conclude that e-mail messages are incapable of conforming to the criteria of CPLR [Civil Practice Law and Rules] 2104 simply because they cannot be physically signed in a traditional fashion," New York Appellate Justice Sandra Sgroi wrote in *Forcelli v. Gelco Corporation*, 27584/08. CPLR 2104 states that "an agreement between parties or their attorneys relating to any matter in an action…is not binding upon a party unless it is in a writing subscribed by him or his attorney." It also requires the agreement be "signed" by the party or the attorney.

The *Forcelli* case centered on the enforceability of an e-mail that summarized an apparent agreement to settle a claim from an automobile accident. The official settlement documents, mailed the following day, pointedly referenced the e-mail confirmation. During the time it took to return the signed documents, the court granted the defendant's motion to dismiss the complaint. But the plaintiff argued the agreement had been reached several days prior to the court's decision, as evidenced by the e-mail.

The defendant claimed the agreement was not actionable until the official documents were suitably signed and returned. The court disagreed, concluding it was clear from the contents of the e-mail and the follow-up documents referencing that e-mail that an agreement was reached.

Sgroi pointed out that the close of the letter reinforced this finding because it clearly indicated the author of the e-mail "purposefully added her name to this particular e-mail message, rather than a situation where the sender's e-mail software has been programmed to automatically generate the name of the e-mail sender, along with other identifying information, every time an e-mail message is sent."

Food for thought when composing that next business e-mail message.

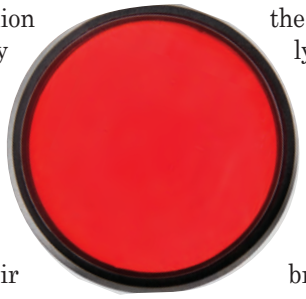
CYBERSECURITY

Cybersecurity: The Gap Between Fear and Action

An amazing 97% of businesses with annual security budgets totaling more than $1 million are concerned they are vulnerable to targeted malware attacks and other sophisticated cyber-crime and cyber-espionage tactics. Their level of concern was revealed in a survey of 200 C-level executives at U.S.-based companies conducted by Opinion Matters, on behalf of ThreatTrack Security. The survey further reported that 33% of the companies — including roughly half of all financial services firms and manufacturing companies that participated — have experienced a targeted cyber attack.

Unfortunately, these executives' fears have not necessarily translated into taking protective action. For example, 42% said they do not have an incident response team in place, and 47% said they are not using advanced malware analysis tools. Most (82 %) financial services firms are concerned about sophisticated attacks to their networks, but only half of them use an advanced malware analysis tool, like a sandbox.

Consumers share some of these basic fears. A companion survey reported that 75% of consumers are concerned about the security of their personally identifiable information. And for good reason, since nearly half (47%) of them said they had been notified at some point that their information had been compromised by a breach.



PRIVACY

Student Safety or Privacy Invasion?

A school district in Southern California is monitoring students' posts on social media sites in an effort to stop cyber-bullying and other teenage issues, according to a recent article in the *Los Angeles Times*. Glendale Unified School District reportedly hired Geo Listening in 2012 to track posts by its estimated 14,000 middle school and high school students after two teenagers committed suicide.

The school district has restricted the monitoring to publicly available pages. Further, the district did not supply Geo Listening a list of current accounts. Instead the company uses "deductive reasoning" to link public accounts to students, according to Chris Frydrych, founder and chief executive of Geo Listening. (He declined to elaborate when asked what constituted "deductive reasoning.")

Response to the program on and off campus has been mixed. Many believe that it and other efforts like it walk a fine line between balancing safe and supportive schools with student privacy and free speech. But the Glendale District program "is sweeping and far afield of what is necessary to ensure student safety and intrudes deeply into students' privacy and conduct outside of school," contends Brendan Hamme, an attorney with the American Civil Liberties Union of Southern California.

PRIVACY

Another State Increases Social Media Privacy Protection

Washington is the latest state to pass legislation banning employers from requesting employees' user names and passwords for their personal social media accounts. According to *Corporate Counsel*, the new law also prohibits employers from requiring their employees to:

- Open their accounts so the employers can view their postings
- Add them as friends
- Change their personal settings to make their accounts more public

If the employer is investigating a worker's alleged misconduct or if a worker is accused of making unauthorized transfers of proprietary information, the employer can ask the worker to voluntarily provide his or her log-on information, but the employer cannot require it. The law does not apply to social media sites and platforms used primarily for work purposes.

Some employers contend they need access to their employees' personal social media accounts to protect proprietary information, to meet federal financial regulations, and to minimize legal risk. Lawmakers are siding with the opposition, which calls such attempts an invasion of employees' privacy.

The National Conference of State Legislatures reports that since 2012, the following states have passed such laws: Arkansas, California, Colorado, Delaware, Illinois, Maryland, Michigan, Nevada, New Jersey, New Mexico, Oregon, Utah, Vermont, and now Washington. Legislation has been introduced or is pending in the remaining 36 states. Some states have similar laws protecting students at U.S. colleges and universities.

HR

UnitedHealth Recalls EHR Software

One of the clear advantages of electronic health records (EHRs) is they help to eliminate some common medical mistakes. For example, a study published in the June 2013 *Journal of the American Medical Informatics Association* reported that more than 17 million medication mistakes are avoided in the United States each year because hospitals are using computerized systems for ordering prescription drugs, thereby reducing the risks resulting from sloppy handwriting and dangerous drug combinations.

But what if an error is caused by a software glitch?

The UnitedHealth Group Inc. recently recalled software used in hospital emergency departments in more than 20 states because certain versions failed to print information about medications and failed to add data to patients' charts. Such notes typically contain directions about diet and use; failure to include them could lead to serious injury or death.

This is not the first recall of Picis software (the software manufacturer purchased by UnitedHealth Group in 2010), according to Bloomberg. A database maintained by the Food and Drug Administration (FDA) recorded six recalls since 2009. Unlike medical device manufacturers, makers of EHR software are not required to report safety issues to the FDA.

"It's admirable that the vendor reported this," said Ross Koppel, adjunct professor of sociology and medicine at the University of Pennsylvania, "but realize that this is one of the more obvious errors. Most are not as obvious and go unreported." He explained that some companies require hospitals to sign non-disclosure agreements, and practitioners are often unaware of the technology's role in errors.

PRIVACY

California Sets Pace on 'Do Not Track' Regs

Many privacy advocates are looking to California to blaze the trail for a national Do Not Track law. The state's Online Tracking Act requires websites to inform users whether and how they honor "do not track" signals transmitted by a consumer's browser. It also requires sites to tell users when advertisers and data brokers are tracking their online movements. At press time, the bill was waiting for Governor Jerry Brown's signature.

Privacy advocates have been frustrated by the lack of progress in Congress and the World Wide Web Consortium (W3C) on standards for online tracking and hope the California bill will stir the pot.

"I'm hoping the California bill will set off a digital data stampede for other states to begin regulating privacy," Jeff Chester, executive director for the Center for Digital Democracy and a member of the W3C Tracking Protection Group, recently told *Politico*. "It's not clear there is going to be a standard for Do Not Track from the W3C. It's likely to be a very weak standard."

The technology industry has mixed feelings about the legislation. Michael Beckerman, president of the Internet Association (whose members include Google and Facebook), stated: "The Internet is an area that is evolving every day. The users should have the power of choice here, not government regulations. California should not start the precedent of states or even the federal government regulating this since it's about the relationship between users and Internet companies."

According to the *Politico* article, the trade group TechAmerica initially opposed the bill for "trying to codify a definition of online tracking and lacking nuanced options for firms to describe how they respond to 'do not track' signals." The group dropped its opposition and adopted a neutral stance toward the amended version that passed the state legislature.

It remains to be seen whether the U.S. Congress or W3C will make headway on more far-reaching standards before the end of the year.

EHR

Wyndham Stands Up to the FTC

Hotel operator Wyndham Worldwide Corp. is fighting back in a data breach lawsuit filed in June 2012 by the Federal Trade Commission (FTC) against the company and three of its subsidiaries.

The lawsuit alleges that Wyndham failed to implement reasonable information security measures

and consequently experienced three major data breaches in two years. Hundreds of thousands of credit and debit cards were ultimately compromised, and there were fraud losses of more than $10.6 million.

The FTC accused the hotel operator of unfair trade practices and of deceiving customers into thinking their cardholder data was adequately protected when it wasn't. Other companies facing similar charges have opted to settle with the FTC, accepting fines as high as $10 million (as in the case of ChoicePoint) and comprehensive bi-annual audits.

Wyndham has questioned the FTC's authority to sue companies on behalf of consumers for cybersecurity breaches and lax or misleading data security policies. The U.S. Chamber of Commerce and several other organizations joined the battle by seeking permission to file for a dismissal, accusing the FTC of holding breached entities like Wyndham to unfair and arbitrary standards. *ComputerWorld* reported the groups also alleged that the FTC is forcing businesses into lengthy data breach settlements and imposing costly fines for violating security standards the agency hasn't formally promulgated.

A federal court judge in New Jersey agreed to allow the groups to file for the dismissal.

The Wyndham lawsuit is considered a landmark case because it's the first time the FTC has had to go to a federal court because a breached entity refused to settle.

The Chamber of Commerce *et al.* contend the agency routinely punishes businesses for failing to have reasonable security standards, yet it has never specified what constitutes reasonable standards. And because previous cases have been settled out of court, there has been no clear precedent for courts and legal counsels to reference.

There is also the question of whether Congress intended the FTC to actually regulate data security. Chris Hoofnagle, director of information privacy programs at the University of California Berkeley Center for Law & Technology, filed an amicus brief supporting the FTC, noting the agency's enforcement actions have been the only effective means of holding companies accountable for failing to protect consumers' data.

"Congress, in creating the FTC and in empowering it to police unfair and deceptive trade practices, explicitly gave the agency power to determine what is unfair and deceptive," he told *ComputerWorld*.

Security consultant Paul Rozenweig, founder of Red Branch Law & Consulting, believes a Wyndham victory would disable the FTC to broadly enforce cybersecurity standards.

EHR

NIST Solicits Feedback on Cybersecurity Framework Draft

In accordance with an executive order issued by President Barack Obama in February, the National Institute of Standards and Technology (NIST) has been working diligently to develop a cybersecurity framework that will provide a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" to help organizations manage their cybersecurity risk.

The latest draft of the preliminary framework was discussed with industry representatives in a dedicated workshop in September. NIST was expected to release a full preliminary draft in October for public review, followed in February 2015 by the final 1.0 version.

The finished framework will guide organizations on managing cybersecurity risk in a manner similar to financial, safety, and operational risk. It will focus on supporting cybersecurity improvement using industry-known standards and best practices.

According to NIST, "The framework provides a common language and mechanism for organizations to: 1) describe current cybersecurity posture; 2) describe their target state for cybersecurity; 3) identify and prioritize opportunities for improvement within the context of risk management; 4) assess progress toward the target state; 5) foster communications among internal and external stakeholders." It is not intended to replace an existing business or cybersecurity risk management process and cybersecurity program. Instead it provides guidance for improving or for establishing a program, if necessary.

The framework, which closely resembles a maturity model, comprises three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profile.

The Framework Core contains cybersecurity activities and references that are common across critical infrastructure sectors. The core presents standards and best practices in a manner that allows for communication and risk management across the organization. The core consists of five functions — identify, protect, detect, respond, recover — that can provide a high-level, strategic view of an organization's management of cybersecurity risk.

Part two is the Framework Implementation Tiers, which demonstrate the implementation of the core functions and categories and indicate how cybersecurity risk is managed. These tiers range from "partial" (tier 0) to "adaptive" (tier 3), with each tier building on the previous one.

Finally, part three is the Framework Profile, which conveys how an organization manages cybersecurity risk in each of the core functions and categories by identifying the subcategories that are implemented or planned for implementation. Profiles are also used to identify appropriate goals for organizations.

The NIST proposal has been criticized for not providing "measurable cybersecurity assurance." Ralph Langner, a renowned Germany-based consultant on industry control systems (ICS) security, contended the "fundamental problem of the [framework as it is currently written] is that it is not a method that, if applied properly, would lead to predictable results."

According to *CSO*, Langner is not alone in this belief. Joe Weiss, managing partner of Applied Control Solutions, said the framework draft takes a "useless 'high-level approach' that favors self-regulation over mandates."

In response, NIST has said the early phases were intended to obtain feedback from the industry to help flesh out the framework. However, it likely will not become a prescriptive standard.

DATA SECURITY

Photocopiers Can Pose Data Security Risk

Time to trade in that photocopie? Be sure to wipe its memory first.

Affinity Health Plans recently settled a case filed by the U.S. Department of Health and Human Services (DHHS) and was fined for potential Health Information Portability and Accountability Act (HIPAA) privacy and security violations. Affinity agreed to pay $1.2 million in fines because it failed to clear the hard drive of one of its leased photocopiers, which was later purchased by CBS.

Affinity self-reported the breach after *CBS Evening News* advised it that the copier's hard drive contained confidential patient medical information. Upon researching the breach, Affinity estimated that as many as 344,000 patients may have been affected. And this wasn't the first photocopier Affinity had returned without erasing the hard drive.

The DHHS' investigation found that Affinity had not included photocopier hard drives in its definition of electronic protected health information in its risk assessment as required by the HIPAA Security Rule. It also determined Affinity had violated the HIPAA Privacy Rule by failing to implement policies and procedures to scrub internal hard drives before returning photocopiers to its office equipment vendors.

In addition to the $1.2 million settlement payment, Affinity was directed to make its best effort to track down and scrub all the hard drives on photocopiers it previously leased that are still in the leasing agent's possession.

PRIVACY

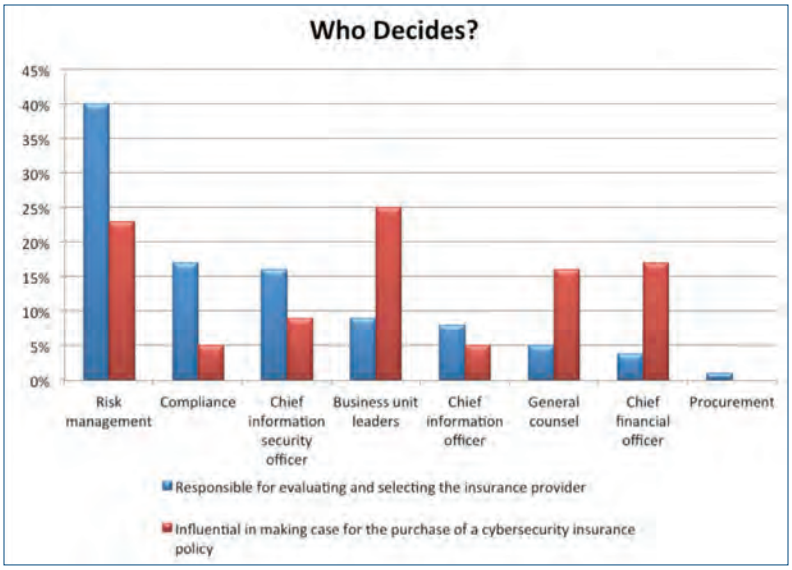
Tips for Complying with HIPAA Omnibus Rule

September 23 marked the compliance deadline for the Health Insurance Portability and Accountability Act (HIPAA) Omnibus Rule that makes business associates accountable for any misuse or failure to safeguard protected health information (PHI).

In a September press release, Karen Carnahan, president and COO of Cintas Document Management, said such HIPAA violations could result in penalties of up to $1.5 million each and that non-compliant companies "risk long-term damage to their reputation and brand."

To help achieve compliance under the Omnibus Rule, Cintas offers these tips:

1. Retrain employees on the updated policies and procedures addressing privacy, security, and PHI breaches.
2. Inventory vendors and look closely at their associates and subcontractors who handle PHI.
3. Update your business agreements. The Department of Health and Human Services has posted a sample version of a revised business associate agreement on its website.
4. Review internal policies and procedures to ensure they reflect the changes made to the HIPAA Privacy Rules. Revisions should reflect changes to the definition of PHI and to the rules governing patient access to records; disclosures to third parties; research; marketing; fundraising and the sale of PHI; notifications to those involved in a patient's care; and other rules governing decedents and immunizations.
5. Update breach policies and procedures.
6. Determine if notice is required for a breach. Under the Omnibus Rule, if there is a breach, it is presumed the covered entity or business associate must give notice unless it can demonstrate a low probability that PHI has been compromised or unless a regulatory exception applies.
7. Review breach notification procedures.
8. Encrypt or destroy PHI.
9. Review your Security Rule gap analysis to ensure it considers the changes made by the Omnibus Rule.
10. Update your HIPAA privacy notices to reflect the changes made by the Omnibus Rule.



Source: Ponemon Institute, 2013

CYBERSECURITY

Rising Data Breech Costs Drive Cybersecurity Insurance Sales

Increasing costs related to data breaches are prompting enterprises to purchase cybersecurity insurance. A new study from Ponemon Institute revealed that 31% of the respondents already have the specialized insurance while 57% of those without it plan to purchase a policy.

Most (70%) of the companies that have purchased a cybersecurity insurance policy have learned first-hand just how costly a breach can be. The respondents reported the average financial impact on companies suffering a breach was $9.4 million. The average potential risk of future incidents was estimated to be $163 million, due largely to the anticipated loss of confidential business information.

From a business perspective, 41% of the respondents consider cybersecurity risks to be greater than other insurable business risks such as natural disasters and business interruption. More than a third (35%) said cybersecurity risks are equal to other insurable business risks.

Many of the policies that have been issued cover expenses incurred during and after a breach. For example, 86% of the policies cover notification costs, 73% cover legal defense costs, 64% cover forensics and investigative costs, and 48% cover replacement of lost or damaged equipment. Fewer than one-third (30%) of the policies cover third-party liability.

Even though insured respondents felt the cost of the insurance was fair given the risk, high premiums were cited as the main reason others had not purchased a policy to date.

Policies typically cover the most common and costly incidents, including human error and negligence, external attacks by cyber criminals, system- or business-process failures, and malicious or criminal attacks from inside. Not surprisingly, the industry sectors with the highest insurance adoption rate were technology and software (41%)

E-MAIL

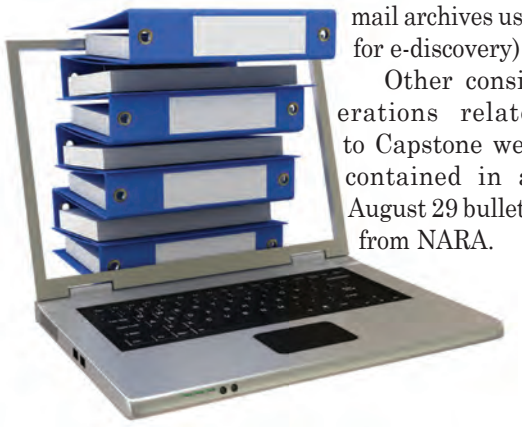
NARA Implements New Plan for Preserving E-mail

The National Archives and Records Administration (NARA) has offered federal agencies a new, more simplified and automated approach to managing e-mail: Capstone.

The Capstone approach allows an agency to categorize and schedule e-mail based on the work and/or position of the e-mail account owner. For example, the agency could determine that records from the accounts of officials at or near the top of an agency should be preserved as permanent. All other e-mail accounts would be considered temporary and preserved for a set period of time based on the agency's need.

Advantages of using the Capstone approach include:

- Reduced reliance on print-and-file, click-and-file, drag-and-drop, or other user-dependent policies
- Optimized access to records in response to discovery or Freedom of Information requests
- A practical approach to managing legacy e-mail accounts
- Reduced risk of unauthorized destruction of e-mail records
- Technologies are leveraged for other purposes (e.g., e-mail archives used for e-discovery)



Other considerations related to Capstone were contained in an August 29 bulletin from NARA.

PRIVACY

Privacy Groups Oppose Proposed Google Settlement, Facebook Policy Changes

A privacy advocates have asked a U.S. court to decline a proposed $8.5 million settlement with Google in a class action lawsuit over search privacy. Their primary point of contention: it does not require Google to change its business practices.

The lawsuit, filed in October 2010, stated that Google allegedly transmitted user search queries to third parties without users' knowledge or consent in order to increase ad revenue. The plaintiffs contended that when a user clicks a link from Google's search results page, the owner of the website would receive from Google the user's search terms, which could contain the user's real name, contact information, credit card numbers, and Social Security number. Those queries could also include highly personal and sensitive information such as confidential medical information, according to the complaint.

The $8.5 million settlement would not provide a monetary award to the individuals who were part of the class that filed suit, but would be used to pay settlement-related expenses, with the remainder going to organizations that would promote public awareness, research, development, and other initiatives related to protecting privacy on the Internet. At the time of filing, the proposed recipients included World Privacy Forum; Carnegie-Mellon; Chicago-Kent College of Law Center for Information, Society, and Policy; Berkman Center for Internet and Society at Harvard University; Stanford Center for Internet and Society; MacArthur Foundation; and AARP Inc.

In addition, the settlement required Google to notify users of its conduct so "users can make informed choices about whether and how to use Google Search." Google agreed to include the required disclosures on its FAQs webpage.

Privacy organizations, including the Electronic Privacy Information Center, Consumer Watchdog, Patient Privacy Rights, the Center for Digital Democracy, and the Privacy Rights Clearinghouse, contested the settlement, urging the presiding judge not to accept the proposed settlement. They criticized the agreement because it doesn't require Google to change its business practices and the proposed relief does not benefit the class members. Further, the group contended the entities that would receive the settlement funds were not, in fact, "aligned with interests of the purported class members."

Many of the aforementioned privacy organizations also weighed in on a similar matter involving Facebook. The groups petitioned the Federal Trade Commission (FTC) to stop Facebook from changing two of its governing policies, saying the changes compromise users' privacy.

PRIVACY

Student Safety or Privacy Invasion?

A school district in Southern California is monitoring students' posts on social media sites in an effort to stop cyber-bullying and other teenage issues, according to a recent article in the *Los Angeles Times*. Glendale Unified School District reportedly hired Geo Listening in 2012 to track posts by its estimated 14,000 middle school and high school students after two teenagers committed suicide.

The school district has restricted the monitoring to publicly available pages. Further, the district did not supply Geo Listening a list of current accounts. Instead the company uses "deductive reasoning" to link public accounts to students, according to Chris Frydrych, founder and chief executive of Geo Listening. (He declined to elaborate when asked what constituted "deductive reasoning.")

Response to the program on and off campus has been mixed. Many believe that it and other efforts like it walk a fine line between balancing safe and supportive schools with student privacy and free speech. But the Glendale District program "is sweeping and far afield of what is necessary to ensure student safety and intrudes deeply into students' privacy and conduct outside of school," contends Brendan Hamme, an attorney with the American Civil Liberties Union of Southern California.

E-DISCOVERY

Comments Sought on Proposed Amendments to FRCP

A draft of preliminary changes to the rules regarding electronic discovery in federal civil suits is now open for public comment. The proposed amendments to the Federal Rules of Civil Procedure (FRCP) were prepared by the Committee on Rules of Practice and Procedure of the U.S. Judicial Conference. Among other things, the changes address scheduling orders, scope of discovery, document production, and sanctions.

The importance and expectation of cooperation was established in the current rules. The proposed changes would facilitate and encourage that cooperation. For example, they would require that the parties meet face-to-face or by other means of direct, simultaneous communication and would allow them to schedule those conferences earlier. This would likely significantly increase the involvement of the courts early in cases, explained Bennett Borden and Amy Frenzen of Drinker Biddle & Reath LLP in a recent *Modaq* article.

A great deal of the discussions regarding the changes have centered on the duty to preserve, how and when it is triggered, and its scope. The new rules would strengthen the court's ability to limit discovery based on proportionality by moving this under the section about scope.

Bordon and Frenzen pointed out that this would also affect preservation, because "it would allow a party to make and defend preservation decisions based upon the proportional benefit of the information compared to the burden of preserving as well as producing it."

In addition, the new rules regarding discovery sanctions would add a layer of protection to preservation decisions. Sanctions would be imposed, in most situations, only if the party's failure to preserve or produce documents was "willful or in bad faith" and "caused substantial prejudice in the litigation."

This proposed amendment protects reasonable preservation and provides clearer guidance on which sanctions can be imposed, whereas the imposition of sanctions currently varies widely among circuits.

Public hearings have been held in Washington, D.C., Phoenix, and Dallas. Comments on the proposed changes may be submitted to *www.regulations.gov/#!docketDetail;D=USC-RULES-CV-2013-0002* until February 15, 2014. The target effective date for the final rules is December 15, 2015.

INFORMATION SECURITY

Survey: Industrial Firms Underestimate Their Data Risk

Manufacturing and distribution executives have become more aware of the risks associated with business information and data, especially as social media becomes more widespread. Yet more than two-thirds believe their data is at little or no risk, according to a research report from the consulting firm McGladrey. Given that their controls are often insufficient or ineffective, this raises the question of whether the executives fully understand their exposure.

Roughly 70% of small and midsize organizations said their data was at little or no risk, as did 56% of larger companies. Attackers, though, don't seem to care much about size.

"Financially motivated attackers will take any data they can find," wrote Corbin Del Carlo, McGladrey's director and regional leader of security and privacy services. "One company's Internet footprint looks the same as another to anyone interested in finding something of value, whether it's credit information, personnel information, intellectual property such as engineering drawings or processes, technology, or other industrial assets. Size does not matter; information does."

How one defines "at risk" may be telling. Some respondents told the surveyors they defined risk by whether "things are running." In other words, as long as their intranet and website were up, they were fine. Some admitted they were still running on technology from the 1980s and were reluctant to make the sizeable investment to bring them into the 21st century. Others were forced to make the investment because they had been breached.

McGladrey found that one of the best practices that thriving companies share is investing in new or upgraded information technology, allowing them to develop innovative products, decrease cycle time, and increase productivity. Investing in software can also give companies a competitive advantage by enabling executives to access corporate performance information they can translate into actionable plans. **END**

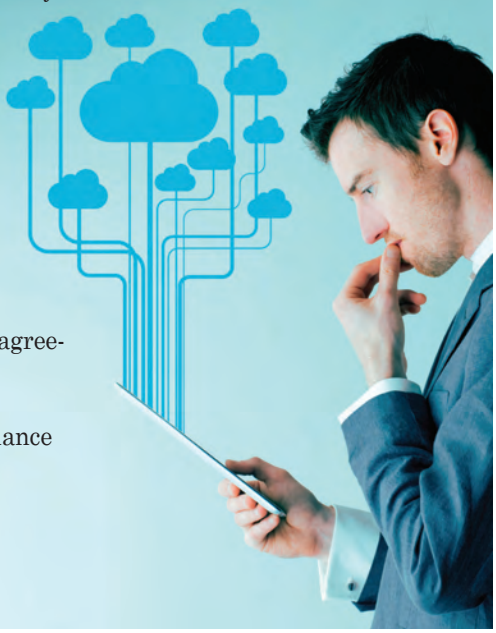
CLOUD

Data Security Top Concern for IT, Business Execs

For the past 50 years, through its National Historical Publications anResults of Saugatuck Technology's "2013 Cloud Survey" of 218 IT and business executives across organizations of all sizes revealed that data protection and security is their top concern related to using cloud-based services. This is consistent with the survey results for most of the past seven years.

Here are the top 11 cloud concerns, according to the survey:

1. Data security/privacy
2. Data/transaction integrity
3. Regulatory compliance
4. Integrating cloud-based data or workflow with existing enterprise applications
5. Cloud provider transparency (e.g., uptime, service level agreements, computer resource location)
6. Ability to customize cloud solutions
7. Dependable delivery of required high availability/performance
8. Viability cloud providers
9. Return on investment for cloud not yet verified
10. Provider lock-in
11. Cross-border data restrictions



CYBERSECURITY

Cybersecurity – An IT Issue or Compliance Issue?

Increasingly, cyber attacks on financial institutions are focusing on interrupting service to users. Consequently, distributed denial of service (DDoS) attacks have become a notable headache for many financial institutions. They are also a reminder of looming responsibility for the organizations' compliance departments, wrote Compliance Complete's Emmanuel Olaoye in a recent Reuters article.

DDoS attacks have become so problematic that the Depository Trust Clearing Corp. (DTCC) considers them one of the three types of attacks that pose a systemic risk to the financial system. (DTCC settles the majority of securities transactions in the United States.) Because regulators are asking more questions about security for such attacks, some contend cybersecurity is becoming a compliance issue. As such, compliance departments may need to become more involved instead of relegating the issue to IT.

Science Applications International Corporation's chief cybersecurity technologist, Gib Sorebo, advises compliance professionals to speak to their IT or information security colleagues when a regulation is introduced so they know whether the organization has the technical capability to comply with the rule.

"The first conversation is understanding what the firm needs when compliance requirements come down," said Sorebo. "It is a lot easier if you have that conversation first about what is doable and not doable."

The role of compliance in cybersecurity likely will continue to change as regulators increase their focus on security. Sorebo predicts compliance departments will need a more extensive cybersecurity program instead of one that is more narrowly focused on protecting customer information. "The compliance officer is going to have to define the overall compliance ecosystem he or she has to have to operate in," he said. "They must certainly be prepared to address, at a minimum, how they are addressing all those compliance obligations." **END**