E-BUSINESS

EU Adopts Single-Market Digital Strategy

Europe cannot be at the forefront of the digital revolution with a patchwork of 28 different rules for telecommunications services, copyright, IT security and data protection," Commissioner for the Digital Economy and Society Günther H. Oettinger said recently. The European Commission (EC) agreed, and has made it a priority to eliminate barriers by implementing a Digital Single Market strategy. The EC set out the main areas where it will focus its work:

- Providing better access to digital goods and services
- Shaping the environment for digital networks and services to flourish
- Creating a European digital economy with long-term growth potential

Providing better access requires facilitating cross-border e-commerce; eliminating the discrimination resulting from geoblocking, which is denying use of online services based on geography; and modernizing copyright law to balance content creators' rights with users' rights.

The EC said value-added tax (VAT) arrangements also must be simplified to boost cross-border activities of businesses, especially small and mid-size organizations. The EC estimates that VAT-related costs due to different requirements are €80 billion (about $87 billion U.S.).

Creating an environment in which digital networks and services can thrive calls for a greater investment in infrastructure. To encourage that investment, the EC will update telecommunications and media rules to ensure they can accommodate new challenges and new players.

Providing a nurturing environment also requires better coordination of the spectrum among member states; the EC advocates a European approach to managing the spectrum "to promote a genuine single market with pan-European services."

In addition, the EC will look into the growing importance of online platforms (e.g., search engines, social media, app stores) while it pushes for swift adoption of the General Data Protection Regulation to ease consumers' distrust of online services for protecting their personal data. The Commission said 72% of European Internet users are concerned about using online services because of a lack of data security.

Standards are key to the long-term growth of Europe's digital economy. "[E]nsuring interoperability for new technologies [is] essential for Europe's competitiveness, they must be developed faster," the EC said. Cloud computing and the gold mine of big data are also critical. In short, the EC wants industry and consumers to make the most of the data economy.

The Digital Single Market strategy is expected to be unveiled in May.

IP

Canadians Tighten Restrictions on Counterfeits

Canada's recently revised Trade-marks Act (TMA) strengthens the protection of intellectual property (IP) and seeks to restrict importing counterfeit goods. The owner of a Canadian-registered trademark can now file a request for assistance application with the Canada Border Services Agency (CBSA); owners of registered or unregistered copyright can do the same, said Paul Tackaberry, counsel with Ridout & Maybee LLP.

The new section of the TMA specifies a procedure for CBSA's handling of complaints about suspected counterfeits. The IP owner has 10 days to start legal proceedings for infringement or the CBSA may release the goods.

STANDARDS

LG Electronics Receives Industry's First Safety Certificate

The British Standards Institute (BSI) recently awarded a certificate for personal information management systems to LG Electronics data centers in Korea, Europe, and North American. This marks the first time this certificate has been earned in the global electronics industry, reported *BusinessKorea*.

The BS10012 certificate – which is based on the BSI standard *Data protection. Specification for a personal information management system* – recognizes an organization's ability to systematically and safely manage its customers' information.

RIM

U.S. Government Recognizes RIM as a Profession

In March, the U.S. government formally recognized records and information management (RIM) as an occupational series for federal employees. The Office of Personnel Management (OPM) announced the final version of the Records Management Occupation Flysheet (0308) and the Qualification Standard, which created a new occupational series of RIM.

This action was mandated by the 2011 Presidential Memorandum on Managing Government Records. In response to the memorandum, NARA and the Office of Management and Budget implemented the Managing Government Records Directive, specifying how the presidential mandate would be met. The directive required OPM to establish a formal records management occupational series that consistently defines records management activities throughout the federal government.

ARMA International supported the directive's call for establishing this occupational series, and when the draft classification was released in December 2013, ARMA submitted comments on what it saw as weaknesses in describing the skills necessary to manage a modern information governance program. The association also asked that the National Archives and Records Administration (NARA) be given a greater role in developing the occupational classification. NARA appears to be pleased with the final version.

"We believe this will elevate the roles, responsibilities, and skill sets for agency records officers and other records and information personnel," stated NARA on its *Records Express* blog.

Upon announcing the change, the OPM said, "This is a part of the effort to reform records management roles, responsibilities, and skill sets. Over the years, the distinction between records management support work and specialist work has become more clearly defined."

Kimberly A. Holden, OPM deputy associate director, recruitment & hiring, said, "Establishment of this new series brings into focus the records and information management workforce using one occupational series to provide consistency in describing, classifying, and recruiting for records and information management specialists across the federal government."

This series comprises positions that supervise, lead, or perform RIM work, which includes planning, controlling, directing, organizing, training, promoting, and other activities involved in records creation, disposition, maintenance, and use. Agencies must apply the occupational series to covered positions by March 2016.

PRIVACY

UN Makes Right to Privacy a Priority

The United Nations Human Rights Council (UNHRC) has elevated the right to privacy and the freedom from excessive surveillance to a priority by appointing a privacy expert or *rapporteur*. This landmark decision, announced in March, is in direct response to the Edward Snowden leaks of U.S. National Security Agency surveillance information.

Although the right to privacy has long been part of international law, until now it has been low on the UN's list of priorities.

The rapporteur, expected to be appointed in June, will monitor, investigate, and report on privacy issues to the UNHRC. He or she will also advise governments on compliance and look into alleged violations, reported *The Guardian*.

The resolution, "The Right to Privacy in the Digital Age," notes that "the rapid pace of technological development enables individuals all over the world to use new information and communications technology and at the same time enhances the capacity of governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights."

Germany and Brazil spearheaded the resolution, which was passed without opposition.

MOBILE

Unsecured Mobile Apps Are Putting Organizations at Risk

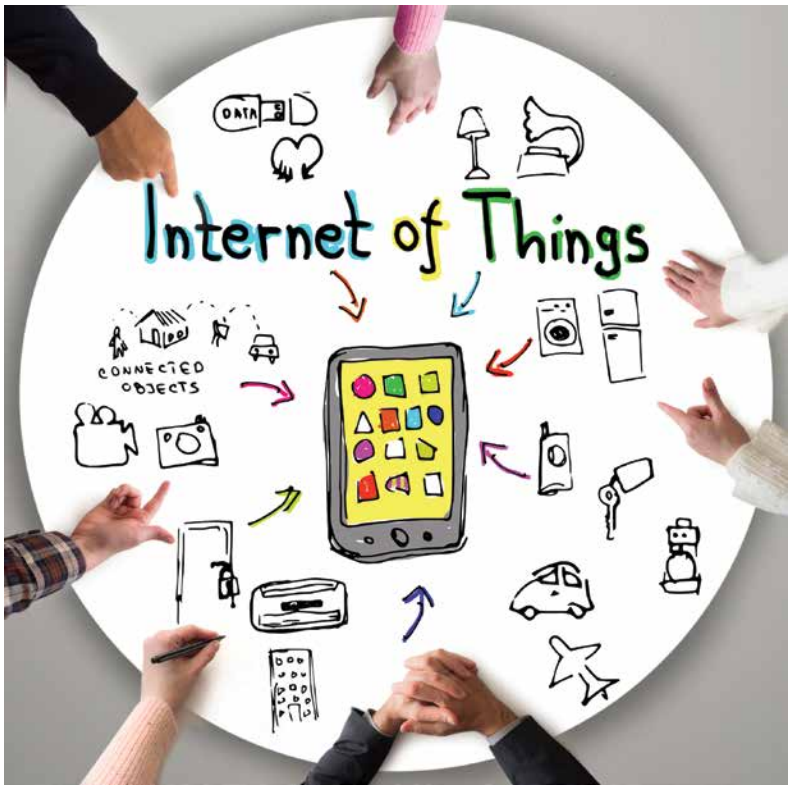
Malware targeting mobile devices is on the rise. In 2014, more than 16 million devices were infected, an increase of 25% over the previous year, reported Motive Security Labs, an offshoot of the French telecommunications company Alcatel Lucent. Threats such as Heartbleed and Not Compatible are coming to the forefront and targeting mobile devices.

While you might think that would be enough to convince companies to increase security for their mobile devices, such is not the case. Recent research conducted by the Ponemon Institute on behalf of IBM found that more than half of companies polled have no budget for mobile security.

The study revealed six reasons why mobile applications are insecure:

1. The "rush to release" can result in apps being released with vulnerabilities. Nearly 40% of the respondents said their organizations don't scan for vulnerabilities.
2. Mobile apps are often tested infrequently or too late. Most often, apps are tested in development or post-development. More than half of the respondents said they do not test apps.
3. Malware-infected mobile apps and devices are increasing in number perhaps because of a lack of resources; only 29% of respondents said their organizations have enough resources to prevent the use of vulnerable or infected apps.
4. Not enough is being spent on mobile app security. According to the report, an average of $34 million is spent annually to develop mobile apps, but only 5.5%, or $2 million, is allocated to their security.
5. Most organizations do not have sufficient mobile application security expertise.
6. Most organizations do not have policies that define the acceptable use of mobile apps in the workplace and thus are providing little or no guidance to employees.

On the brighter side, 60% of the respondents said their organizations consider mobile app security a high priority. Now seems a good time to put the policies and resources in place to prove it.



TECHNOLOGY

IoT – Some Call It 'Privacy Hell'

The Internet of Things (IoT), which includes anything with a sensor, processor, and connectivity to the Internet, continues to expand rapidly – Accenture predicted last year that 69% of consumers will own an in-home IoT device by 2019, while Gartner forecasted that 25 billion devices will be in use by 2020 – and that worries privacy and security experts alike.

"There are more devices and more types of devices, so this just gives you more ways for people to hurt you," security expert Josh Corman recently told *Fast Company's* Lauren Zanolli. "What we've done is blindly assume that [adding software and connectivity] is always good. And we're making really horrible, horrible choices."

Medical devices are a major area of concern for Corman, who pointed out that hacker-researchers have proved that high-tech medical equipment can be manipulated to cause harm. Then there are connected cars, home security and automation systems, and "smart" public infrastructure such as utility grids and traffic control.

He also raised a red flag regarding the data being collected about individuals' movements. According to the article, information collected by personal tracking and activity devices has already been admitted into court in personal injury cases; some believe it will soon be used in divorce cases as well.

"I think what will happen is that there is going to be enough people spied upon by ex-girlfriends or boyfriends, or distrust their government, or get hurt from IoT devices, and we're gonna realize we did too much," Corman predicted.

In January the Federal Trade Commission (FTC) issued a report providing best practices businesses should follow to protect consumers' privacy and security when developing IoT devices:

- Build security into the devices from the start.
- Train employees on the importance of security and ensure that security is managed within the organization.
- Ensure that outside providers can maintain appropriate levels of security.
- Consider a "defense-in-depth" strategy that uses multiple layers of security to defend against a particular security risk once it's been identified.
- Monitor devices throughout their life cycle and provide security patches to cover known risks.

The FTC also urged companies to limit the amount of consumer data collected and to dispose of it after a set period to limit the amount of data that could be breached and make themselves less enticing for hackers.

The FTC also published "Careful Connections: Building Security in the Internet of Things," a report that advises businesses on how to implement a risk-based approach to building security into products connected to the IoT.

"When you look at information security, the rules to build software are not like the rules to build a bridge," Lee Weiner, senior vice president of products and engineering at the security engineering firm Rapid7, told *Fast Company*. "If you want to build a bridge there are well-known structural codes. That is not the case in the software world. The only way those flaws get found is the equivalent of someone driving on that bridge with different types of vehicles."

PRIVACY

New Russian Data Residency Law Has Far-Reaching Effects

If you have business connections with Russia, be prepared for the new data residency law that will go into effect September 1. Essentially it requires businesses to record and process personal data of Russian citizens through databases in the Russian Federation.

Lothar Determann, an attorney at Baker & McKenzie, told *Legal Tech News* the law is farther reaching than some may realize, affecting companies that have:

- A subsidiary, branch, or representative's office in Russia
- Customers in Russia (such as an Internet or social media company)
- Customers who have customers or a presence in Russia (such as cloud providers)
- Suppliers in Russia (such as development centers)

"That means pretty much any company with an international business is affected to some degree," said Determann.

The effect on the company will depend on how significant its Russian ties are.

"Perhaps the greatest adverse effect is on Russian companies and Russian citizens," he suggested, pointing out that companies with headquarters or significant presences in Russia will lose access to advanced information technology products and services. Global providers would have to move databases and data centers to Russia, which they may not be able – or willing – to do, especially since the United States and the European Union have imposed trade sanctions against Russia for its activities in the Ukraine.

Determann said Russian companies may "have to return to locally hosted or on-premise solutions and incur implementation costs, find limited availability, face reduced technology quality and perhaps make do with offline work-arounds." Russian citizens, he added, could be forced to exclusively use locally hosted media and online services, which are closely controlled by the Russian government.

Assess whether employees and contractors have too much access to sensitive and confidential information in their workspaces and in offsite locations.

TECHNOLOGY

Say Goodbye to IE, Hello to Project Spartan

Microsoft recently announced that the browser included in Windows 10 will employ new technology code named "Project Spartan" instead of featuring Internet Explorer (IE). It's all part of Microsoft's effort to shed its old PC image as it strives to be a viable player in the mobile market.

"In the war of the future, which is mobile, they're losing," Tom Bedecarre, chairman of the digital advertising agency Akqa, told *The Science Times*. "Nobody's going to download Internet Explorer as their mobile browser."

IE had once been one of the most recognized technology brands, with more than a billion people around the world using it daily. Within three years of its release it overtook the top browser, Netscape. At one time, *The Science Times* reported, IE accounted for an estimated 95% of browser usage. Then along came Firefox, followed by Google's Chrome and Apple's Safari. Today, Microsoft's browser share has reportedly fallen to about 20%, equal to the share of Firefox.

IE won't be retired immediately, however. To help organizations that rely on software developed for IE, a new version will be released with Windows 10 alongside Spartan. This will provide legacy compatibility and time to migrate their software to the new platform.

INFO SECURITY

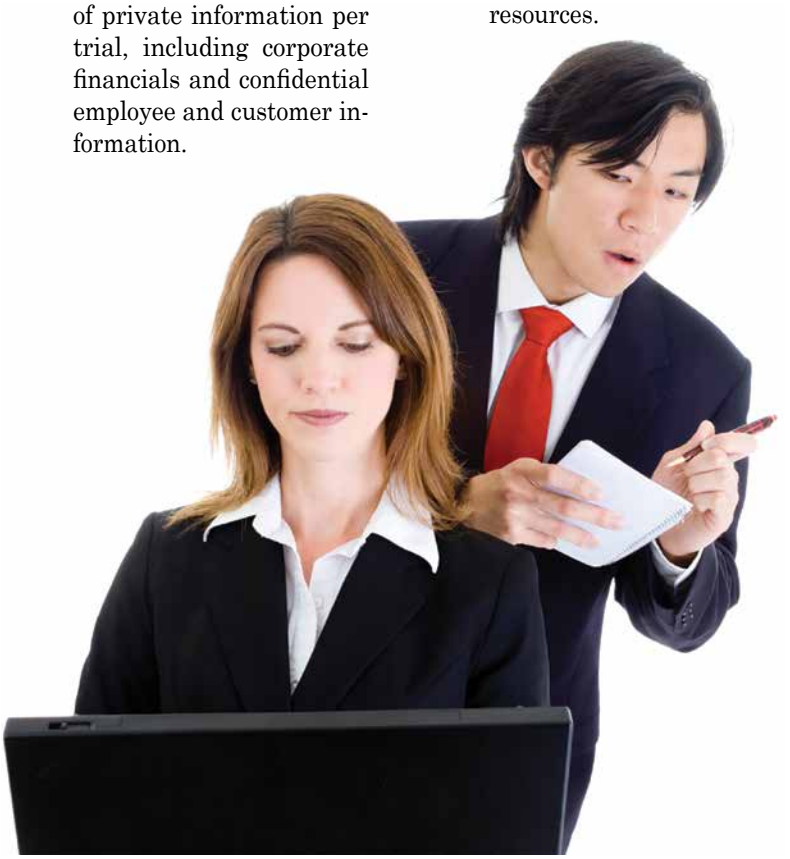
Low-Tech Hacking Works, Too

How easy is it to steal sensitive company information through "visual hacking?" 3M and the Ponemon Institute recently conducted a covert experiment in which an undercover visual hacker was sent into 43 offices at seven large corporations to obtain sensitive information only by using visual means. In 88% of the trials, the hackers were able to access sensitive information. The experiment demonstrated that:

- Visual hacking happens quickly. In 63% of the trials the hackers obtained high-level, sensitive corporate information in less than 30 minutes.
- Multiple pieces of information are hacked. The hackers saw up to five pieces of private information per trial, including corporate financials and confidential employee and customer information.
- Visual hacking goes unnoticed. The hackers were stopped in only 30% of attempts and even then had already obtained an average of 2.8 pieces of confidential customer information.

Protecting your organization's sensitive information is up to you. Some suggestions of where to start are:

- Assess the risk your office environment could be posing to sensitive information.
- Institute a visual privacy policy that outlines specific actions to prevent the display of important data in plain sight.
- Train employees to become more aware of what information might be desirable to visual hackers.
- Help senior management become more aware of the risks and ramifications of visual hacking and the need for additional prevention resources.
- Assess whether employees and contractors have too much access to sensitive and confidential information in their workspaces and in offsite locations.



PRIVACY

Court Scraps Netherlands' Data Retention Law

A judge in The Hague recently struck down the Netherlands' data retention law, saying that it breaches the privacy of telephone and Internet users. The Dutch law required telephone companies to store information about all fixed and mobile phone calls for a year and Internet providers to store information on customers' Internet use for six months, reported *The Guardian*. The intent was to make the data available for use by law enforcement.

The judge acknowledged that scrapping the data "could have far-reaching consequences for investigating and prosecuting crimes," but added that it did not justify the breaches of privacy. No deadline was set for disposition of the data.

Meanwhile, in Australia the government is considering a data retention package that would store certain types of phone and web data for two years, giving government agencies warrantless access to the information. The bill was introduced last fall but is reportedly closer to passing with bi-partisan support.

MOBILE

Move over Notebook PCs; Tablets Are Taking Over

Tablets are expected to overtake notebook PCs this year as the largest mobile computing category, according to new data from the market intelligence firm ABI Research. Tablets are expected to gain 52% of the market by the end of this year. In contrast, the market share of notebook PCs is expected to drop from 51% in 2013 to 48% by the end of this year.

Despite the rise of the tablet, there is still a market for notebooks, says ABI Research.

"Notebooks offer a combination of portability and productivity that has yet to be achieved by any other portable mobile computing device," said research analyst Stephanie Van Vactor. "Although laptops appear to be losing traction they're not going out of style and flat growth can be representative of several market conditions, including a longer lifecycle." The notebook PC category includes laptops, Chromebooks, and ultrabooks, the sales of which are still growing in some regions.

Although tablets continue to be popular, their adoption rate is beginning to slow. ABI Research's data shows Chromebooks and ultrabooks are experiencing a growing market that is expected to reach 47%, combined, this year.

INFO SECURITY

Study Says: Europeans Fear Their Data Isn't Safe

Most Europeans are not happy with how their data is being handled by businesses, according to "Symantec's 2015 State of Privacy" report. More than half (57%) of the participants said they are worried their data is not safe. Almost 60% reported they've experienced a data protection issue.

Surprisingly, these concerns do not appear to have prompted Europeans to change their behaviors. Internet purchases are continuing to increase, and only 25% said they took the time to read sites' terms and conditions. This may be due partly to the difficulty of finding those terms and conditions on some sites.

Despite these behaviors, Europeans generally realize their data has value and needs to be better protected, but 66% admitted they don't know what to do.

As Symantec pointed out in its report, it is clear that governments and businesses need to do more to educate people on how to protect their information, whether it's their banking details or their e-mails.

Phillip Carter, vice president for European enterprise infrastructure and software group at IDC, said, "Businesses should consider a channel to allow consumers to question how their data is being used and advocate more transparency. If businesses begin to act like trusted advisors and put privacy of consumer data at the heart of the business, the consumer is on a much better footing to feel more confident about their data."

The research showed that the responsibility for protecting information "is relatively equal across government, business, and consumers." The latter have indicated they are willing to pay for that protection in much "the same way that they would pay for travel or credit card insurance." Indeed, 50% said they would pay the same or more as they pay for credit card insurance, and 46% said they would pay the same or more as their phone bill.

"It is clear we are at a tipping point," concluded Symantec's Darren Thomson. "It is now that business and government leaders should act to ensure their customers and the public can trust them sufficiently to share accurate data. The opportunities with data shared, analyzed, and used in a secure and private environment are endless. The data potential could revolutionize how we live today."

PRIVACY

How Much Would You Pay for Privacy?

AT&T is about to find out how much customers in San Francisco will pay for a faster Internet and whether they will pay with their wallet or their privacy.

The company recently launched GigaPower, which it says is so fast customers can download 25 songs in less than a second, according to an article in *SFGate*. The service is priced at $139 a month or $110 a month; to get the lower price, customers must agree to allow AT&T to monitor their browsing habits through its Internet Preferences program. The plan is to compile the information to sell higher-priced personalized advertisements.

Sound familiar? This approach will pit AT&T against free Internet services such as Google and Facebook, which also use customers' online activities to sell customized advertising.

AT&T is targeting online gamers and users of video-chat services such as Skype, the article said. In other words, it will target users who have a high need for faster Internet speeds.

Predictably, the approach is drawing mixed reviews. Privacy watchdogs have expressed concern while others think it could work. Dan Marcec, spokesman for online advertising research firm eMarketer, told SFGate that people "generally don't have issues with advertising that they feel like they've raised their hands to receive."

It appears that this approach does not violate the Federal Communications Commission's net neutrality laws prohibiting Internet providers from charging users for access to faster speeds without their knowledge because customers must agree to opt in to the program.

TECHNOLOGY

New Messaging App May Replace E-mail

The new messaging app Slack is emerging as a possible replacement for e-mail. What makes this app different from other group chat apps is that it includes automatic archiving of all interactions, a good search engine, and strong device interoperability. It is hosted online, customizable, and reportedly easy to set up and maintain.

According to an article in *The New York Times*, Slack is "one of the fastest-growing business applications in history." After one year of operation, the app serves about a half-million workers "including at such large enterprises as Walmart, Comcast and *The New York Times* – as a partial replacement for email, instant messaging, and face-to-face meetings."

Stewart Butterfield, Slack's cofounder and CEO, told *The New York Times* that its user base is doubling every three months. He predicts there will be 2 to 3 million users by the end of the year.

The app is a reflection of Butterfield's vision for the office of the future. He believes that the trend is away from solo work and toward collaborative teams, which will require workers "to become adept at navigating complex team dynamics." Slack, says its co-founder, can provide the sort of "nuanced, intimate communication" not available with e-mail.

BYOD

Case Law Catches Up with BYOD

According to Amanda Tomney of DLA Piper, case law is finally catching up with the bring your own device (BYOD) movement. In a recent post to the legal firm's blog, *Labor Dish*, Tomney cited four cases related to the use of personal mobile devices in the workplace.

The first case dealt with partitioning work-related content from personal content. In *Rajaee v. Design Tech Homes, et al.*, the company remotely wiped the iPhone of a salesperson when he resigned. In so doing, all of his personal data was also deleted. The ex-employee sued the company for accessing personal information without authorization and for the damage caused by its deletion. The court rejected both claims for not meeting the requirements of the laws under which the suit claimed.

The upshot, according to Tomney, is that companies need to review their BYOD policies and ensure employees know the circumstances under which their personal devices may be wiped. Some companies are partitioning work-related content from personal content so when data is wiped, it occurs only on the corporate side of the wall.

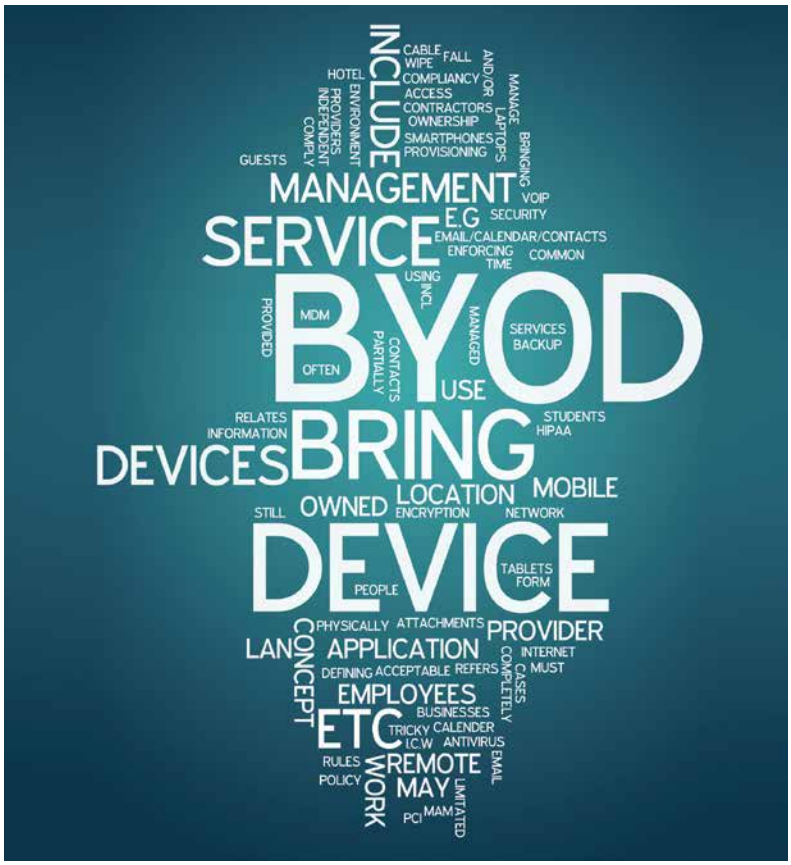
Another case raised the question of who should be allowed to use personal devices for work-related business. In *Mohammad v. Nwabuisi*, an employer was found liable for not compensating an employee for overtime work performed on the worker's personal device. Employers may therefore want to consider limiting BYOD to exempt employees. If non-exempt employees are allowed BYOD privileges, the company should ensure it has the policies and procedures in place for reporting all time worked, including time spent answering after-hours e-mail and calls.

The third case cited was *Cochran v. Schwan's Home Services Inc.*, in which the court determined that in accordance with state law, employers must reimburse employees who are required to use their personal devices for work, a reasonable percentage of their cell phone bill. The court further stated the reimbursement must be made even if employees do not incur any additional expense. Tomney warned that even in states without similar statutes the argument could be made that the absence of reimbursement is an "impermissible wage deduction."

Then there's the issue of litigation holds. "BYOD complicates the e-discovery process because electronic data that may fall within the scope of discovery requests can reside on devices besides those over which the company has control," wrote Tomney.

In *Small v. Univ. Med. Center of S. Nevada*, the defendant failed to issue a litigation hold addressing BYOD devices even though key employees confirmed they used their personal devices for work-related purposes. Consequently, the defendant lost more than two years of messages and other electronically stored information that were potentially relevant to the case. The e-discovery special master on the case called the defendant's conduct "a mockery of the orderly administration of justice," and called for an order of default judgment.

Concluded Tomney: "Yesterday's BYOD policy, in short, is as outdated as your uncle's flip phone."



CYBERSECURITY

Legal Departments Are Prime Targets for Hackers

High-profile breaches have led to scrutiny on third-party vendors' access rights to an organization's data. An area that hasn't received much attention, though, according to David White and Matthew Cohen, of AlixPartners LLP, "is the downstream transfer of corporate data in connection with litigation and regulatory matters to e-discovery vendors, outside counsel, experts, and opposing parties."

The authors said legal departments hold a company's most valuable and secret documents, making them a prime target for hackers. It's a security gap they urged organizations to address. In a recent *Metropolitan Corporate Counsel* article they wrote that contracts with outside vendors should ensure they are legally obligated to adequately protect the company's data and are fully liable for loss or inadvertent disclosure, and that the company has the right to audit and enforce these requirements.

The goal is to ensure the service provider's security meets or exceeds your industry's regulatory requirements.

The more difficult task is protecting information produced for others with whom there is no contract, such as opposing counsel and their vendors and experts. These concerns are typically addressed during the meet-and-confer process.

"The catch here is that while you, as the producing party, may be able to obligate receiving parties to protect your data as if it were their own, there are presently no mechanisms to audit or otherwise ensure those obligations are being met," the authors wrote. They added that the final disposition of information from all participants should be included in protective orders; derivative works should also be covered. **END**

INFO GOVERNANCE

Finding the Right Captain for Your IG Program

A successful information governance (IG) program that is truly enterprise-wide requires buy-in from all corners of the organization, particularly legal, records, information security, compliance, IT, and the business units. This way, everyone's needs will be represented.

It sounds good in theory, but then reality hits and the committee members become overwhelmed by their daily responsibilities, sending the IG initiatives to the back burners.

"Representation on the committee is rooted in the best of intentions, but it doesn't necessarily facilitate the process of actually getting things done," said attorney and IG expert Linda G. Sharp in a recent *JD Supra* article. "The true dynamic that has arisen typically consists of sprawling committees of individuals that already have a full-time job with little to no time to make committee meetings, much less make things happen."

Without a single person tasked with overseeing the initiative, many IG initiatives drag on for years with little or no real benefit to the organization. "Everyone is on deck to ensure they're not forgotten, but rarely is a dedicated captain at the helm," Sharp pointed out.

So who should that captain be? According to Sharp, it's an individual who understands a little bit of each of the organizational needs. The captain needs to understand the legal ramifications of litigation, the regulatory requirements of compliance, and a way to minimize the IT footprint. There must also be a focus on the needs of the business teams. That's why often the captain comes out of the legal, records and information management, compliance, and/or IT departments.

When's the last time you took a good look at your IG initiative's progress and its leadership? Has it grown stagnant? Do you have the right people in place? More important, do you have someone in place to truly own the initiative? Before you try to ramp it up, advised Sharp, "you need to take a critical look at who should be the 'owner' of it. In many businesses, the ship is afloat without a captain."