TECHNOLOGY

2015's 10 Top Strategic Technology Trends

Technology research firm Gartner has identified the top 10 strategic technology trends for 2015 and beyond. Each of these factors will likely be very disruptive to the business, end users, or IT; require a major investment; or pose a risk if adopted late – affecting organizations' long-term plans, programs, and initiatives.

The trends cover three themes: "the merging of the real and virtual worlds, the advent of intelligence everywhere, and the technology impact of the digital business shift," explained David Cearley, Gartner vice president.

The top 10 trends are as follows:

1. **Computing Everywhere** – The focus will shift to mobile users as opposed to mobile devices only.
2. **Internet of Things (IoT)**– The combination of data streams and services created by digitizing everything creates four basic usage models – Manage, Monetize, Operate, and Extend – organizations can leverage.
3. **3D Printing** – Worldwide shipments of 3D printers are expected to grow 98% in 2015 and double in 2016.
4. **Advanced, Pervasive, and Invisible Analytics** – Organizations will need to focus on analytics as the volume of data coming from the IoT, social media, and wearable devices explodes in order to deliver exactly the right information to the right person at the right time.
5. **Context-Rich Systems** – "By understanding the context of a user request, applications can not only adjust their security response but also adjust how information is delivered to the user…"
6. **Smart Machines** – The application of deep analytics to an understanding of context will ultimately lead to a world of smart machines – an era that Gartner predicts will be the most disruptive in the history of IT.
7. **Cloud/Client Computing** – The focus will be on synchronizing content and applications across multiple devices.
8. **Software-Defined Applications and Infrastructure** – Computing will need to become more dynamic and less static in order to deal with the rapidly changing demands of digital business.
9. **Web-Scale IT** – Expect more organizations to begin thinking, acting, and building applications and infrastructure like Amazon, Google, and Facebook.
10. **Risk-Based Security and Self-Protection** – Once organizations realize that 100% secure environments are impossible, they can begin to apply more sophisticated risk assessment and mitigation tools.

MOBILE DEVICES

Smartphone Market, Challenges Continue to Grow

If you thought the demand globally for smartphones was declining, think again. According to a *cnet.com* article, the program director with research firm IDC's Worldwide Quarterly Mobile Phone Tracker said that global smartphone shipments are continuing to see "record-setting volumes." During the third quarter of 2014, they topped 300 million, a 25% increase over third quarter 2013.

As usage grows in general, so does the use of mobile devices at work. A 2013 IDC Global Solutions study found that 41% of respondents use their personal smartphone for business. This continues to present challenges to organizations with respect to e-discovery and data security.

CLOUD COMPUTING

Cloud Computing from the CIO's View

CIO magazine recently talked to some of the top CIOs about the challenges of cloud computing. Their leading concerns are legacy, vendor "lock-in," and security.

General Electric's chief operating officer for cloud, Chris Drumgoole, said most of its new apps (more than 90%) deployed today are in the cloud. But what's to be done about its 9,000 legacy apps? The company needs to assess each app and decide whether to move it, kill it, consolidate it with other apps, or allow it to remain on some sort of legacy system. Drumgoole said GE hopes to have made all those decisions by 2016.

Vendor lock-in can also be a major obstacle according to Dow Chemical's David Day, director of workplace services. Moving from one cloud app to another can be extremely complicated because the apps don't talk to each other. He advocates for better "orchestration tools," as well as standards to help smooth the way. On the positive side, Land O'Lakes CIO Mike Macrie said it is generally less expensive to switch providers in the cloud compared to on-premises.

CIOs still consider security a universal concern. "Security is one of the more complex problems to solve. To really put together an effective solution, you need to cobble together 5-6 solutions," says Randy Spratt, CIO and CTO at McKesson.

Humana's CIO, Brian LeClaire, said his company relies on "multiple tools and tactics" to protect its information and it assesses the provider's security framework before engaging with it. For example, the company looks at what tools the vendors use, their general approach to security, how they handle encryption, and their ability to ensure information remains in the continental United States. Fortunately, Sysco CTO Wayne Shurts said, cloud providers realize that legal and security issues are some of their biggest obstacles and have addressed many of these issues.

While some worry about security and risk in the cloud, others believe the cloud improves security because cloud vendors are more aware of the latest technology. Whirlpool CIO Michael Heim pointed out that security problems arise from how you manage the data, not where it's located. "The big challenge is that it's just different. You have people thinking in old models, not new ones," Heim observed.

The CIOs identified various other challenges they face, including "shadow IT," where employees purchase unauthorized cloud services. As more organizations have fine-tuned their cloud policies and services, this is not as big a problem as it was a few years ago, the article said.

"Transfer of brand risk" was also cited as a concern for some. An example of this is a client company's reputation being harmed by a cloud service outage. Some may recall just such an instance on Christmas Eve 2012 when Netflix went down because of an Amazon Cloud outage.

Finally, many CIOs questioned whether many cloud solutions are ready for major enterprises. Some see this as an opportunity to guide the vendor in its development and investments.

TECHNOLOGY

New Search Engine to Make Obsolete Formats Accessible

There could be good news on the horizon for accessing obsolete electronic file formats. The National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign is developing a new search engine named Brown Dog, which will convert defunct computer files into accessible formats, PBS NewsHour recently reported.

Kenton McHenry, a senior research scientist at the NCSA, explained that a user will be able to feed a file saved in an obsolete format into the cloud-based search engine, and it will transform the file into a format the browser can read. It will also be able to assign metadata to images that were previously unreadable, making them keyword searchable.

Development of Brown Dog is funded by a $10 million, five-year grant from the National Science Foundation as part of its Data Infrastructure Building Blocks program. McHenry told NewsHour that the search engine will likely be available on a limited basis and for testing in March 2015.

PRIVACY

Fortune 1000 Privacy Spending 2015 Forecast: Up 20%

A new benchmarking study launched to track privacy management and spending in Fortune 1000 companies found that enterprises spent $2.4 million on privacy in 2014. That number is expected to increase 20% in 2015, according to a report released by the International Association of Privacy Professionals (IAPP).

More than half (55%) of the participating enterprises considered their privacy programs to be mature or in the late-middle stage of maturity. One-third categorized their programs as being in the middle stage of maturity, leaving 9% in the early or "pre-stage" category.

Predictably, those with more mature programs reported higher privacy budgets and more privacy employees than those with less mature programs. Approximately 12% of companies spent $5 million or more on privacy, while 16% spent less than $500,000, reported *Law Technology News*.

Privacy hiring will continue to rise as privacy issues continue to plague companies of all sizes. Future budget estimates indicated one-third of companies expect to hire full-time and part-time privacy professionals in 2015. Those who can communicate meaningfully with legal, compliance, IT, and information security professionals will likely be in high demand, predicted IAPP President and CEO Trevor Hughes.

INFO SECURITY

Executives Say – But Don't Act Like – Data Security Is Vital

The majority of U.S. executives say data security is vital to their organizations, but their actions don't show it. In fact, it's estimated that only about a third of U.S. data is completely secure, and information security is low on the list of risks to businesses. According to NTT Com Security US, which conducted the survey, these findings "show an alarming disconnect between policy and behavior…among business leaders."

Even though 65% of respondents said data security is vital to their organizations and characterized consumer customer data as the most important, very few reported that all customer data is completely secure. Protection of intellectual property (IP) fared much better: 56% said their IP is completely secure. Respondents said they were more concerned about losing market share to competitors, the lack of employee skills, and decreasing profits than data security. This likely explains why only 10%-12% of their IT budgets is spent on data security.

The survey finding also showed that senior executives "fail to acknowledge long-term damage – both in terms of time and money – that a data breach might have on their business." Nearly three-quarters (72%) predicted there would be minimal long-term damage if data were lost in a security breach even though most of them realized that their organization would suffer reputational damage and loss of customer confidence.

As for the financial impact of a security breach, 40% of respondents said their organizations would suffer a direct financial loss, on average, by 5%. Yet, 16% expect no impact at all on revenue, with another 16% admitting they do not know what the financial implications would be.

As further evidence that many executives are out of the loop about the realities of data breaches, only 24% said they are kept up to date by the IT security team regarding data attacks and potential threats. NTT Com Security US concluded that these findings clearly show that business leaders need to be better educated about data security.

CYBERSECURITY

Europe's Biggest Cybersecurity Threat Isn't Hackers

The European Network and Information Security Agency (ENISA) learned valuable lessons when it conducted its largest-ever cybersecurity exercise a few months ago. The test involved more than 200 organizations and 400 cybersecurity professionals from 29 European countries simulating more than 2,000 separate cyber attacks, including denial-of-service attacks, website defacements, exfiltration of sensitive information, and attacks on critical infrastructure.

ENISA learned that the greatest threat Europe faces is not cyber espionage, cyber warfare, or cyber terrorism, but rather hardware and software failures. One of the major challenges to solving infrastructure weaknesses is that each country approaches it differently.

"The sophistication and volume of cyber-attacks are increasing every day. They cannot be countered if individual states work alone or just a handful of them act together," stated European Commission Vice President Neelie Kroes. The hope is that exercises such as Cyber Europe 2014 will help bring them together.

ENISA Executive Director Udo Helbrecht pointed out: "Five years ago there were no procedures to drive cooperation during a cyber-crisis between EU member states. Today we have the procedures in place collectively to mitigate a cyber-crisis on a European level."

INFO SECURITY

Payment Card Security Group Issues Best Practices

Organizations required to meet the Payment Card Industry Data Security Standard (PCI DSS) – which includes any organization that accepts, transmits, or stores payment card data – are required to have a formal security awareness program in place. The PCI Security Standards Council has made that task easier with the recent release of "Best Practices for Implementing a Security Awareness Program." The report repeatedly emphasizes the importance of training.

"Security awareness should be conducted as an ongoing program to ensure that training and knowledge is not just delivered as an annual activity, rather it is used to maintain a high level of security awareness on a daily basis," the report stresses.

The guidelines, which were developed by a group of numerous retailers, banks, and technology providers, focus on three key areas: assembling a security awareness team; developing appropriate security awareness content for the organization; and creating a security awareness checklist.

The first step is to assemble a security awareness team that includes representatives from a cross-section of the organization. This team will be responsible for developing, delivering, and maintaining the security awareness program. The guideline provides specific guidance for defining the team and its role.

Next, the team should work with business units to classify each employee's role and determine what training each needs based on the role and level of responsibility. The report provides sample role categories, potential content and metrics for each, and helpful references.

Recognizing that many people find checklists helpful in planning and managing programs such as this, the report includes checklists for creating, sustaining, and documenting a security awareness program that can be customized as appropriate.

The report concludes with two appendices: a checklist for mapping the PCI DSS requirements to different roles, materials, and metrics, and a sample table for recording how the organization is managing its security awareness program.

PRIVACY

EU vs. Google: The Saga Continues

The European Union has been investigating Google for the past four years, due primarily to complaints from Microsoft, Expedia, European publishers, and others, Reuters reported. During this time, Google has been the center of attention regarding privacy issues, requests to scrub search results when requested, copyright concerns, and taxes.

The latest in the saga: In late-November EU lawmakers voted to encourage anti-trust regulators to consider proposals to unbundle search engines from other commercial services. And since Google has an estimated 90% market share in the search industry, the resolution is asking to break up Google. The resolution is a non-binding one, but it is a clear and strong signal of Europe's concern over the growing power of U.S. tech companies.

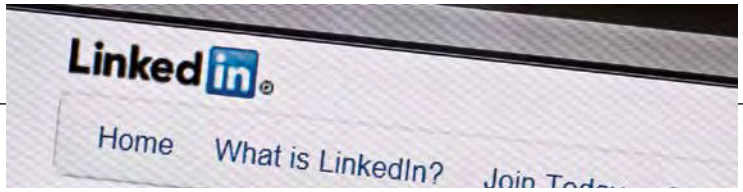
The lobbying group Computer & Communications Industry Association – whose members include Google, eBay, Facebook, Microsoft, and Samsung – opposes the resolution, calling it an "extreme and unworkable" solution.

"While clearly targeting Google, the parliament is in fact suggesting all search companies or online companies with a search facility, may need to be separated. This is of great concern as we try to create a digital single market," the group said in its official response.

The EU's new digital chief, Günther Oettinger, a vocal critic of Google's market dominance, surprisingly did not support the resolution to break up Google. In his words, such a move would be the "instrument of a planned economy, not a market economy."

Oettinger assumed his new role as digital chief at the end of October 2014. He is charged with delivering a single telecommunications market across Europe but has apparently made Google his first priority. Prior to taking office, Oettinger reportedly told the German publication *Handelsblatt* that Google should have to pay to use European intellectual property. German publishers have been wrestling with Google over the search giant displaying news snippets without compensating the publishers. Google responded, stating it would stop displaying snippets and instead include just a link and headline, a move some publishers decried as blackmail.

And if that's not enough, EU privacy watchdogs are demanding that Google extend the right-to-be-forgotten to all its sites, not just its European ones. The EU's supreme court a short while back issued a ruling directing Internet search engines to remove personal information that is "inadequate, irrelevant, or no longer relevant" if requested by the affected person. Google, the top Internet search engine in Europe, is complying, it says, by removing the results from the European versions of its website; the scrubbing has not extended to *Google.com*. Privacy advocates want that to change, putting them directly at odds with free speech proponents, who contend that allowing people to ask search engines to remove their information is essentially an attempt to whitewash the past.



PRIVACY

Court Claims LinkedIn Violates FCRA

A class action lawsuit has been filed against the professional networking site LinkedIn alleging that it violates the Fair Credit Reporting Act (FCRA), reports *Law Technology News*. The plaintiffs have taken issue with LinkedIn providing prospective employers and others who pay for premium services a report containing an individual's former employment history and "trusted references" without verifying the accuracy of the information.

According to the lawsuit, because LinkedIn provides reference reports for a subscription fee, it falls under the purview of the FCRA, which requires it to meet certification and disclosure requirements. The plaintiff's further contend that LinkedIn has failed to put procedures in place to ensure the accuracy of the information.

"Such secrecy in dealing in consumer information directly contradicts the express purposes of the FCRA, which was enacted to promote accuracy, fairness and the privacy of personal information assembled by credit reporting agencies," the claim says.

COPYRIGHT

China Gets Serious About Copyright

If China wants to create more of its own online content, it needs stronger protections for intellectual property (IP), according to the founders of Alibaba Group Holding and Tencent Holdings, China's Internet powerhouses.

Tencent Chief Executive Officer Pony Ma recently told the World Internet Conference in Wuzhen that improving copyright protections will help Chinese companies develop a mature business model for video, music, and animation, Bloomberg reported.

Respecting IP rights has long been a sore spot between China and the United States. In fact, China has been on a U.S. Trade Representative watch list for the past 25 years. Pony Ma says the country has come a long way during that time.

"China's Internet development in the past 18 years has evolved from total disorder that did not pay attention to intellectual property rights in the past to now, when it pays more and more attention. Although it didn't fully fix the problem, gradually it's improving."

In November, the country opened its first specialized court in Beijing to address IP cases. Additional courts are being set up in Shanghai and Guangzhou to handle cases on patents, trademarks, and computer software issues. This is all part of the government's efforts to make it easier for domestic companies to develop content for the country's 632 million Internet users, Bloomberg noted.

The government can't do it alone, however. Alibaba's Jack Ma, known as the country's richest man, pointed out that "[m]any problems cannot be solved by government. It's about society, education, culture. All of the stakeholders should come together to solve those problems."

Alibaba, Asia's largest Internet company, has taken strong measures to solve such issues regarding IP. In 2012 it was removed from the U.S. government's Notorious Markets list after cracking down on 87 million listings in its Taobao Marketplace that may have breached IP rules, Bloomberg reported. This has helped the company to build its credibility, making it much more attractive for distribution deals with such major players as Warner Music Group.

CLOUD COMPUTING

NIST Releases Final Cloud Computing Roadmap

The National Institute of Standards and Technology (NIST) has published the final version of the U.S. Government Cloud Computing Technology Roadmap in two volumes. The final documents reflect more than 200 comments received from around the world.

Volume I, *High-Priority Requirements to Further USG Agency Cloud Computing Adoption*, describes the purpose and scope of the roadmap. It focuses on five priorities: security, interoperability, portability, performance, and accessibility. It also presents 10 requirements for federal government cloud adoption, including developing international standards, security solutions, and clear and consistent categories of cloud services. Each requirement is accompanied by a list of priority action plans complete with target dates. Research teams from government, industry, and academia are working on the action plans.

Volume II, *Useful Information for Cloud Adopters*, introduces a conceptual model as well as technical use cases to provide more practical guidance to agencies. It offers a cloud computing taxonomy and identifies existing interoperability, portability, and security standards that apply to cloud computing. This volume also covers security challenges associated with cloud adoption.

Although NIST standards are developed for government agencies, they can be used by other organizations as well. NIST will continue its work in this area with the help of three new public working groups: Cloud Service, Federated Community Cloud, and Cloud Interoperability and Portability. The Cloud Computing Metrics group will continue to address gaps in metrics and metrology in cloud computing in accordance with requirement 10 presented in the first volume.

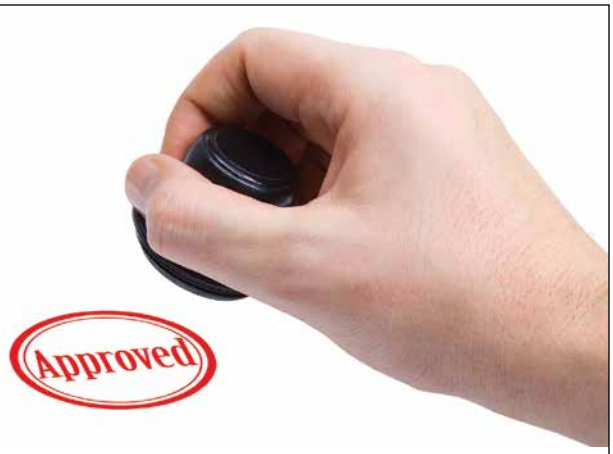
CYBERSECURITY

A Cybersecurity Threat Many Miss

As organizations tighten up their defenses against cyber attacks, there's one threat they are missing: their smaller-sized vendors.

"More and more, as the large companies put their defenses in place, the adversaries are going toward their suppliers," Sondra Barbour, Lockheed Martin's head of information systems, said at the recent Fortune Most Powerful Women Conference. Indeed, smaller vendors that can't afford expensive security measures and yet have links to some of their larger clients' sensitive data are becoming targets of sophisticated hackers.

Several of the executives talked about how their companies are creating increasingly elaborate cyber attack scenarios and running fire drills to help them prepare for future attacks. They said too many organizations don't put enough emphasis on such practice sessions and are paying a very high price.



E-DISCOVERY

Court Endorses Predictive Coding

Predictive coding appears to be growing in popularity throughout the legal community. Of course, there are some opponents who contend it is an unreliable and unproven technology that can result in excluding some documents appropriate to the case. Recent case law, however, indicates that courts approve of its use.

The U.S. Tax Court recently gave predictive coding a stamp of approval when it overruled the Internal Revenue Service's (IRS) objection to a petitioner's request for permission to use the technology to review documents. (See *Dynamo Holdings Ltd. v. Commissioner of the Internal Revenue Service*, 143 T.C. No. 9 [2014].) As noted by Bracewell & Giuliani's Daniel Meyers in a recent issue of the *JDSUPRA Business Advisor*, the e-discovery rules in the U.S. Tax Rules of Practice and Procedure are very similar to those in the Federal Rules of Civil Procedure (FRCP).

In the *Dynamo* case, Dynamo requested permission to use predictive coding to review volumes of data contained on backup tapes, explaining that a completely manual review would be time- and cost-intensive. The IRS suggested Dynamo produce all the files on backup; the IRS would sign a "clawback" agreement that would allow Dynamo to withdraw any protected documents. Not surprisingly, Dynamo was not comfortable with that option. Luckily for Dynamo, the court understood its reluctance.

The court decided that predictive coding was a "happy medium," and rejected the IRS' contention that predictive coding is an "unproven technology."

"Perhaps the most notable aspect of *Dynamo* was the court's emphasis on the need to be transparent and cooperative when using new review technology, such as predictive coding," Meyers suggested. The court was satisfied that Dynamo was attempting to be appropriately transparent.

A similar request to use the technology was denied by a District of Nevada case because "the record lacked the necessary transparency and cooperation among counsel." (*Progressive Cas. Ins. Co. v. Delany, 2:11-CV-00678-LRH, 2014 WL 3563467* [D. Nev. July 18, 2014])

This is one more very clear statement from the court regarding the importance of cooperation and transparency among all parties during the discovery process. The pending changes to the FRCP further reinforce that expectation.

E-DISCOVERY

Social Media Makes E-Discovery a Headache

There is no privacy when it comes to social media, and using it as a source can create e-discovery headaches, a panel of experts said during a session of the Advanced E-Discovery Institute on social media and privacy issues held in November, according to an article in *Law Technology News*.

"Social media, in so many ways, is like all of your worst e-discovery nightmares rolled into one," said Adam Cohen, a principal at Ernst & Young. Using it as a source amounts to "unlocking a door to every type of electronically stored information (ESI) imaginable" because there are so many different media platforms, formats, applications, locations, etc.

As with all document requests, social media requests should be justified, targeted, and discussed early in the case, advised Martin Tully, a partner at Akerman. Pinning down the information is a major challenge. It's doable – at least to some extent – but it's not easy. Forensic practices are sorely needed, said Cohen.

But the point remains: social media content is discoverable.

Organizations are obligated to preserve social media evidence just as they are other ESI. Failure to do so could present a spoliation problem, the top reason for disputes regarding social media, according to Magistrate Judge Kristen Mix, of the U.S. District Court for the District of Colorado. It's too easy to tamper with, delete, or modify postings. Cohen added that changes to social media posts are tracked, but he was unaware of any archiving tool on the market at that time that can capture deleted information.

Because of the expense of searching and producing ESI, it's critical that all parties put social media into perspective. As Tiffany Ferguson, a partner at Pugh, Jones & Johnson, pointed out, social media often turns up useful information but it's rarely the "smoking gun."

RISK MANAGEMENT

Guidelines on Data Breach Insurance Released

Commercial records and information management companies now have a resource to help them make sense out of industry-specific insurance coverage – especially for data breaches. That help is a new industry guideline published by PRISM International, "Risk Management and Insurance for the Commercial Records and Information Management Services Industry."

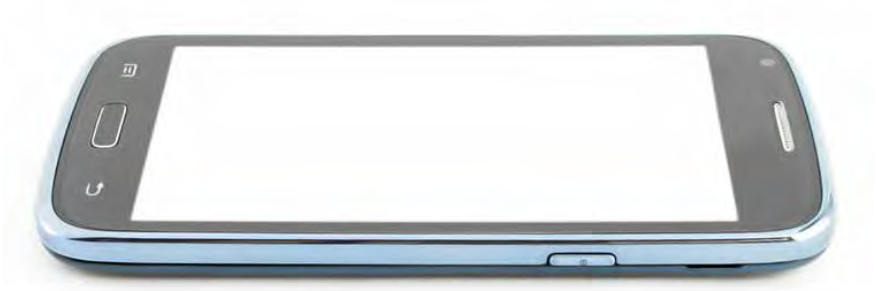
"Some types of coverage can be confusing. Making a mistake in coverage related to data breach can destroy a business," explained co-author Brian Jungeberg of Brightstone Insurance.

According to co-author Jim Booth, former executive director of PRISM International and now with Brightstone Consulting, the guideline contains results of an industry survey that measured commercial centers operators' depth of understanding of insurance policies and how many already had data breach coverage.

The survey results convinced Brightstone there is "an urgent need to correct the serious gap in data breach coverage. "Costs associated with a data breach can be greater than a fire," said Jungeberg. The guideline is intended to help operators create an effective risk mitigation strategy.

MOBILE DEVICES

Real Mobile Security Takes More Than a Policy



The use of mobile devices may be growing, but users are not necessarily getting smarter about the accompanying security issues. In 2012, a Symantec Threat Report revealed that 44% of adults were not aware of security solutions for mobile devices. As more people have begun using mobile devices, this number has only increased. In 2013 it rose to 57%. According to a special *ComputerWorld (CW)* report, this can be partly explained by the migration to smartphones by people who previously used feature phones with limited security requirements. They often aren't aware of the need to install security apps.

This is especially troublesome for organizations as employees increasingly are using their personal mobile devices to access corporate data. Couple this with the growing number of lost mobile devices. *CW* cited a *Consumer Reports* survey that determined 1.4 million smartphones were lost and never found in 2013, up from 1.2 million in 2012.

So how do organizations address this problem and safeguard their data?

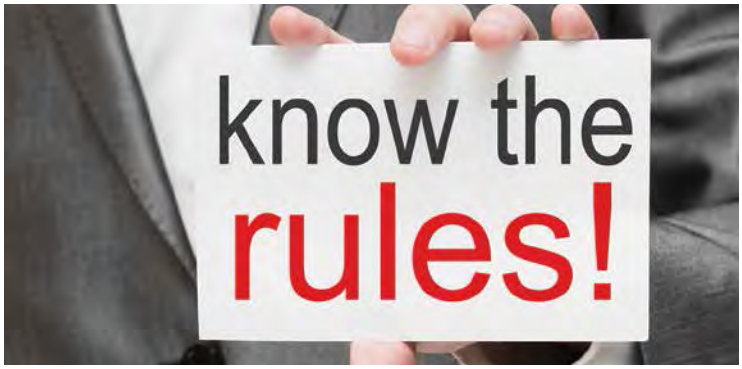
"To date there is really not a perfect way to secure a device from an employee," said Jamisson Fowler, vice president of IT at WellPoint, a health benefits company. "They are always prone to their own sets of mistakes, and there's not a tool out there to absolutely lock the device down."

The solution lies with better user training. Employees need to be continuously made aware of the dangers of bypassing corporate settings on their devices, of falling prey to phishing, of losing their devices and not promptly reporting the loss. But the training must be engaging, fun, and interactive to be effective.

One company has switched from a boring PowerPoint training tool to a Mario Brothers-like interactive game, the initial response to which has been very good. Other companies have taken a no-shame stance, assuring users that IT will not yell at them if they misplace their mobile devices and emphasizing the need to know of the loss as soon as possible because of the potential threat to the company's data.

Authentication and time-lock features are built into all current mobile operating systems to help deter unauthorized persons from using "found" smartphones. Additional solutions, such as fingerprint and iris scanners, are also available. Some even detect the shape of the ear to determine accessibility.

One thing is certain: having a policy is not enough. **END**



INFO SECURITY

FCC Jumps into Data Security Enforcement

The Federal Communications Commission (FCC) recently assumed the role of data security enforcer when it fined two telecom companies for allegedly storing personally identifiable customer data online without appropriate protection measures.

According to the FCC, the companies YourTel and TerraCom gathered sensitive information (including Social Security numbers) to determine eligibility but then failed to securely store or destroy the data once it was no longer needed. Instead, the information was stored on publicly accessible Internet servers until reporters for Scripps Howard News Service "stumbled" across it. As many as 300,000 customers may have been affected.

"This is unacceptable," stated the FCC's top enforcement official, Travis LeBlanc. He added that this may be the commission's first data security enforcement action, but it won't be its last. With 2014 having been marked with several high-profile data breaches, the FCC's growing interest in privacy cases is not unexpected.