EHR

Report: Health IT Isn't Delivering

More than $81 billion. That's how much Rand Corp. researchers in 2005 estimated health information technology implementation would eventually save the United States by improving the delivery and efficiency of health care. In 2012, those savings had yet to be realized.

In a report published in the January 2013 edition of *Health Affairs*, Rand researchers blamed the slow progress on the "sluggish" adoption of health IT systems, the inoperability of health IT systems, and healthcare providers' failure to reengineer their care processes to take full advantage of health IT.

"The failure of health information technology to quickly deliver on its promise is not caused by its lack of potential, but rather because of the shortcomings in the design of the IT systems that are currently in place," said Arthur Kellermann, M.D., the study's senior author and the Paul O'Neill Alcoa Chair in Policy Analysis at RAND, a nonprofit research organization.

Jennifer Covich, CEO of the nonprofit member association eHealth Initiative, told *E-Commerce Times* that the study may be a bit harsh on the progress achieved to date. However, she said, "the study points out some valid factors that need to be addressed. For example, interoperability is a big problem and the federal government should play a lead role in dealing with that.

"Vendors may not be as far along in development as we would like, but to some degree they are in the same place as health providers in trying to figure out where they should be."

Stated Judy Hanover, research director at IDC Health Insights, "The supplier market in this space is immature, and there have been a lot of new functionality requirements for 'meaningful use' that have driven development of new functionality with minimal attention to usability. The platforms that today's EHRs [electronic health records] rely on make changes to support usability time consuming and expensive for vendors to make and implement in highly customized systems."

The Rand study's authors concluded that "a compelling vision is needed to guide further investments" in health IT. They suggested:

- Health information stored in one IT system must be retrievable by others, including doctors and hospitals that are a part of other health systems.
- Patients should have ready access to their electronic health information and be able to share it with providers of their choice.
- Health information technology systems must be engineered to aid the work of clinicians, not hinder it. Systems should be intuitive, so they can be used by healthcare providers without extensive training, and they should be easy to use across different healthcare settings.

CLOUD

Healthcare Cloud Spending Expected to Reach $6.8 Billion

The healthcare market's technology spending has grown aggressively over the past few years, a good percentage of it in cloud computing services. Researchers predict that the global healthcare industry will spend $6.8 billion by 2018, compared to an estimated $1.8 billion in 2011.

Research published in late January by Transparent Market Research revealed that North America is the fastest growing cloud computing market in the health industry today. This is largely attributed to the vast number of biopharmaceutical companies that are conducting research and development and relying heavily on IT to do it competitively.

Healthcare organizations are also major contributors as they implement electronic health records as affordably as possible. They are looking to increase competitiveness by cutting IT costs and are turning to cloud computing for solutions.

CLOUD

What to Expect in Cloud Computing in 2013

Cloud use in 2013 will get real," predicted Forrester Research's James Staten at the end of 2012. "We can stop speculating, hopefully stop cloud-washing, and get down to the real business of incorporating cloud services and platforms into our formal IT portfolios. As we get real about cloud, we will institute some substantial changes in our cultures and approaches to cloud investments."

Staten's comments were based on evidence that IT departments are no longer denying cloud use is happening in their companies and it is part of the IT budget.

"According to the latest *Forrsights* surveys, nearly half of all enterprises in North America and Europe will set aside budget for private cloud investments in 2013 and nearly as many software development managers are planning to deploy applications to the cloud," Staten wrote in his December 3 blog posting.

Here are some of the things Staten said we can expect in 2013:

- The industry will finally stop saying "everything is going cloud" and get real about what fits and what doesn't.
- Cloud and mobile will become one. "What's the value of a mobile app that doesn't call out through the Internet to back-end services? Not much," concluded Staten.
- Accurate cost-modeling will be much easier, thanks to new tools on the market.
- Developers will finally realize that development is not all that different in the cloud.

DATA SECURITY

UK Fines Sony $337K for 2011 Data Breach

They should have known better, stated the UK Information Commissioner's Office (ICO) in announcing it was fining Sony Europe £250,000 ($337,000 U.S.) for a violation of the Data Protection Act in 2011.

The penalty was assessed following a breach of Sony's PlayStation Platform in April 2011. More than 75 million customers' personal information – including names, addresses, account passwords, e-mail addresses, and dates of birth – was compromised, as were customers' payment credit card details.

ICO's investigation determined that the attack could have been prevented if software had been up-to-date.

"If you are responsible for so many payment card details and log-in details then keeping that personal data secure has to be your priority. In this case that just didn't happen, and when the database was targeted – albeit in a determined criminal attack – the security measures in place were simply not good enough," said David Smith, deputy commissioner and director of data protection.

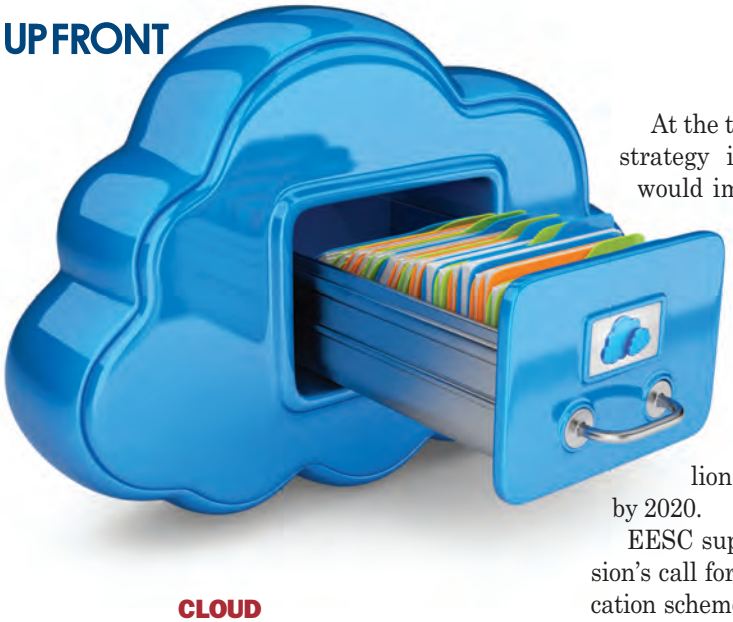
"There's no disguising that this is a business that should have known better. It is a company that trades on its technical expertise, and there's no doubt in my mind that they had access to both the technical knowledge and the resources to keep this information safe."

Interestingly, a California district judge threw out the Sony case saying, "There is no such thing as perfect security."

Since the hack, Sony has rebuilt the PlayStation Network Platform to be more secure. Sony told BBC News that it strongly disagreed with the ICO's decision and intended to appeal.

Smith acknowledged that the penalty was substantial, but said the ICO would make no apologies for that. "The case is one of the most serious ever reported to us. It directly affected a huge number of consumers, and at the very least put them at risk of identity theft."

On the upside, Smith cited a PR Week poll conducted shortly after the breach that revealed that 77% of consumers were more cautious about giving their personal data to other websites.



CLOUD

EU Considers More Aggressive Cloud Computing Strategy

The European Union (EU) is not doing enough to spur the development of cloud computing and the EU's role in that market. That was the central point made by the European Economic and Social Committee (EESC), the consultative body to the European Commission (EC), in its report to the commission in January.

Last September, the EC released a communication on "unleashing the potential of cloud computing in Europe." While the EESC agrees with the EC's intent, it contends the EC's approach does not go far enough in helping the EU realize that potential. Promoting its uptake isn't enough.

EESC members proposed an alternative strategy in which the EU would "help businesses and public administrations to become 'cloud active' by offering cloud-based services and make Europe 'cloud productive' by providing cloud infrastructure," stated EESC's Eric Pigal, according to *Computer Week*. Only then can the EU realize the cloud's potential.

At the time, the EC said the strategy introduced last fall would improve and increase the use of cloud computing in the EU and that the cloud could generate about €900 billion (about $1.2 trillion U.S.) and an additional 3.8 million jobs across the EU by 2020.

EESC supported the commission's call for an EU-wide certification scheme for cloud providers that would thereby create a technical standard. The committee also favors the EC's call for draft model conditions for cloud computing contracts in service level agreements and developing cloud-based public sectors.

On the other hand, the EESC took issue with the current strategy and the absence of concrete awareness-raising measures and warned against excluding the most vulnerable. "The commission should prioritize users with the lowest awareness and show small and medium businesses how they can benefit from cloud computing," said Pigal.

He also contended that special incentives are needed to encourage development of cloud services and infrastructure by European providers. "Under current market conditions, expanding the use of the cloud in Europe will inevitably strengthen non-European operators," Pigal warned.

EESC concluded that meeting the objectives of its cloud strategy will require targeted EU financing and national subsidies. The committee also stressed the need to kick-start European projects through competitive bidding.

U.S. LEG/REG

Warrantless Access to Cloud-Based Data Debated

Efforts to balance the needs of law enforcement and Americans' privacy are at the center of a U.S. Senate debate over proposed amendments to the 1986 Electronic Communication Privacy Act.

It all started in November when the Senate Judicial Committee considered a proposal that would allow law enforcement to access data in the cloud – including e-mail and Facebook posts – without first obtaining a search warrant. It immediately hit a wall formed by a coalition of technology firms, including Apple, Facebook, Google, and Twitter, which contended that electronic data should be treated the same way as hard-copy data.

Just prior to the close of the 112th session in December, the Senate Judicial Committee passed a revised version that would allow access, but only after law enforcement secured a search warrant for electronic data based on the traditional standard of probable cause before accessing data in cloud.

The current proposal before the Senate in the 113th United States Congress, which convened in January, would also require wireless carriers to store text messages for at least two years to aid law enforcement.

PRIVACY

Lebanese Up in Arms over Invasion of Privacy

Controversy arose at the end of 2012 in Lebanon when it was revealed the country's Internal Security Forces (ISF) demanded the content of all SMS text messages sent between September 13 and November 10 from providers such as Blackberry Messenger and Facebook. According to the Electronic Frontier Foundation (EFF), the information requested includes usernames and passwords.

The ISF's requests were submitted to the Ministry of Telecommunications. The minister of telecommunication, Nicolas Sehnaoui, immediately took to Twitter, reportedly to rally his supporters to spread the word and to fight to save individuals' Internet privacy.

ISF justified its request, reported EFF, by saying it would help generate leads in an investigation into a car bombing in Beirut that killed ISF's intelligence chief and another senior official. Rather than request the data for only those individuals suspected of being involved in the attack, the ISF apparently asked for all messages from all users — an estimated 3.7 million.

Not all the data requested by ISF is available from the Ministry of Telecommunications, said Sehnaoui; some of it would have to be provided directly by the service providers. The request was forwarded to Lebanon's Council of Ministers. It will be up to them to determine if the country's general security or its people's privacy are highest priority.

As of the writing of this article, no decision had been announced by the Council of Ministers.

EHR

HHS Moves Toward Safer Electronic Health Records

The U.S. Department of Health and Human Services (HHS) recently released its strategy for making electronic health records and other health IT safer for patients. The Health IT Patient Safety Action and Surveillance Plan was released for public comment at the end of last year.

At its foundation is the belief that health IT has the potential to greatly improve patient safety. To realize health IT's full potential, however, all interested parties — including the government and private sectors — must recognize that patient safety is a shared responsibility.

The plan's stated goal is to "inspire confidence and trust in health IT and health information exchange," by taking steps to use health IT to make care safer and continuously improve the safety of health IT. It prescribes a list of actions that are organized under three strategies:

- **Learn:** Increase the quantity and quality of data and knowledge about health IT safety
- **Improve:** Target resources and corrective actions to improve health IT safety and patient safety
- **Lead:** Promote a culture of safety related to health IT

"Though some in the field say it doesn't go far enough, others said the plan is an important step for an office whose primary role has been cheerleader for a technology that has the potential to dramatically improve health care in the United States but that may come with significant risks" wrote *Boston Globe*'s Chelsea Conaboy.

Public comments were due to HHS by February 4.

PRIVACY

Australia Passes New Privacy Law

In late December 2012, Australia passed the Privacy Amendment (Enhancing Privacy Protection) Bill 2012; it goes into effect in March 2014.

Most notably, the new law established the Australian Privacy Principles, the National Privacy Principles (applicable to the private sector), and Information Privacy Principles (applicable to the federal public sector) revised credit-reporting provisions; and expanded the powers and function of the Australian Privacy Commissioner, including the authority to seek civil penalties up to $1.1 million ($1.15 million U.S.)

Businesses were given 15 months to review their existing policies and procedures to ensure compliance with the new law.

Passage of the law occurred about the same time ABC News Australia reported that cybercriminals had hacked into the server and password system of a small medical clinic in Queensland and encrypted the center's patient medical records. The thieves then demanded $4,000 ($4,200 U.S.) to decrypt the data.

A Troubling Trend

This is just one more instance of a disturbing global trend in data security. Healthcare providers have become popular targets for this kind of cybercrime. The Third Annual Benchmark Study on Patient Privacy & Data Security, released in December 2012 by Ponemon Institute, reported that 94% of the U.S. hospitals surveyed had experienced at least one data breach in the previous two years; 45% had been attacked at least five times during that period.

According to Larry Ponemon, Ph.D., CIPP, and chairman and founder of Ponemon Institute, the vulnerability of patient information "is due in part to the recent explosion of employee-owned mobile devices in the workplace and the use of cloud computing services. In fact, many organizations admit they are not confident they can make certain these devices are secure and that patient data in the cloud is properly protected. Overall, most organizations surveyed say they have insufficient resources to prevent and detect data breaches."

The study confirmed that organizations are taking steps to detect data breaches, but most lack adequate budget and resources. Nearly half (48%) of the organizations surveyed said they are now conducting security risk assessments, but only 16% are conducting privacy risk assessments. Furthermore, 67% don't have controls to prevent and/or quickly detect medical identity theft.

PRIVACY

Georgia Congressman Tackles Health Security

Johnson

U.S. Rep. Hank Johnson (D-Ga.) released a discussion draft of the Application Privacy, Protection, and Security Act of 2013 in mid-January. According to the congressman's website, *AppRights.us*, "This bill would require that app developers maintain privacy policies, obtain consent from consumers before collecting data, and securely maintain the data that they collect."

The act would also require developers to provide consumers with a method to opt out of continued use of the app and decide the fate of their personal information already captured by the app. The consumer could direct the developer to delete any personal data to the extent practicable or cease collecting data altogether.

Johnson released the draft following on the heels of a meeting of the National Telecommunications and Information Administration (NTIA), which comprises mobile industry members and privacy advocates, to discuss a draft of proposed voluntary standards for disclosing how mobile apps use data.

The APPS Act draft provides a safe harbor provision for any developer who voluntarily adopts and complies with the code of conduct the NTIA is expected to release. Enforcement of the APPS Act would fall to the Federal Trade Commission (FTC). State attorneys general could bring suits against those who violate the regulations the FTC would enact to enforce the law.

As of this writing, it was unknown when the APPS Act would be introduced to Congress.

A TROUBLING TREND

Predictive Coding to Become an Ethical Obligation

Looking back over the reported electronic discovery opinions and notable e-discovery themes in 2012, it's clear that the big shaker and mover is technology-assisted review (TAR), or predictive coding.

"Across the entire electronic discovery reference model many notable e-discovery trends emerged in 2012, but none promises to change the status quo more than the line of opinions approving the use of technology-assisted review," said Michele Lange, director of e-discovery thought leadership and industry relations at Kroll Ontrack. "As courts in the last year progressively embraced advanced technologies, such as TAR, opinions from the bench showed increased scrutiny over procedural issues."

Indeed, the number of e-discovery procedural disputes doubled last year, while sanction cases dropped 10%, according to Kroll Ontrack's annual report on electronic discovery cases.

Howard Sklar, senior corporate counsel at Recommind Inc., observed in an article on Recommind's *The Core Perspective* that predictive coding has gone through three stages of adoption, each marked by legal developments.

- In the first stage, courts allowed the use of predictive coding in e-discovery.
- In the second, a dispute arose over electronic review of records because predictive coding wasn't used. Both sides eventually agreed on keyword search terms.
- In the third stage, a Delaware chancery judge required predictive coding without a request from the parties.

"In the future," Sklar contended, "we'll enter stage four: the decision by a state bar's ethics watchdog that failure to use predictive coding is ethically questionable, if not unethical. After all, purposefully using a less-efficient, less accurate, more expensive option is problematic." Stage four, he said, could happen any time given how fast we've gone through the first three stages.

Other Legal Trends of 2012

At the end of each year, Kroll Ontrack analyzes the 70 most significant state and federal judicial opinions related to the preservation, collection, review, and production of electronically stored information. In 2012, the decisions broke down into the following major issues:

- 32% of cases addressed sanctions regarding a variety of issues, such as preservation and spoliation, noncompliance with court orders, and production disputes.
- 29% of cases addressed procedural issues, such as search protocols, cooperation, production, and privilege considerations.
- 16% of cases addressed discoverability and admissibility issues.
- 14% of cases discussed cost considerations, such as shifting or taxation of e-discovery costs.
- 9% of cases discussed predictive coding.

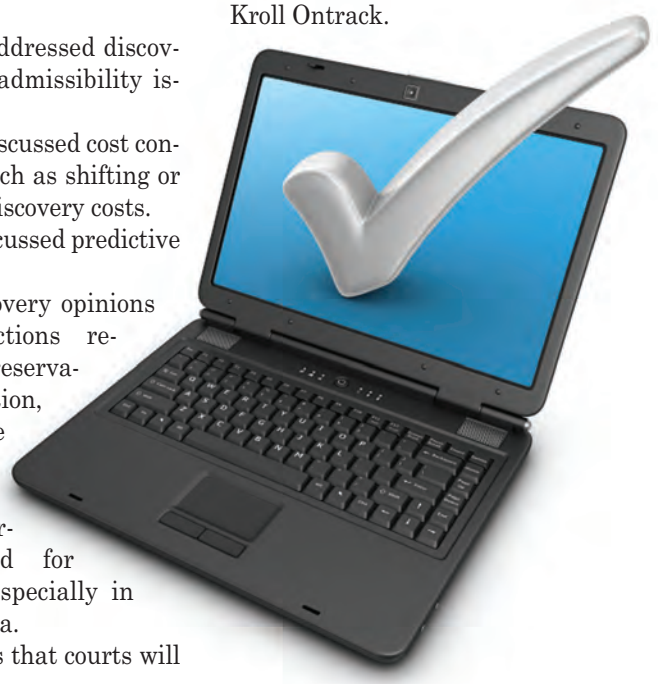
Many e-discovery opinions discussing sanctions revolved around preservation and spoliation, yet courts were all over the map regarding an appropriate preservation standard for e-discovery — especially in the era of big data.

Kroll predicts that courts will continue to fine-tune the most appropriate instances and best practices for TAR adoption in 2013. It also said it expects continued buzz regarding discoverability of social media and e-discovery cost allocation.

Some courts, such as in *Robinson v. Jones Lang LaSalle Americas, Inc.*, allotted broad discovery of social media data, finding that such data helped prove or disprove a party's allegations.

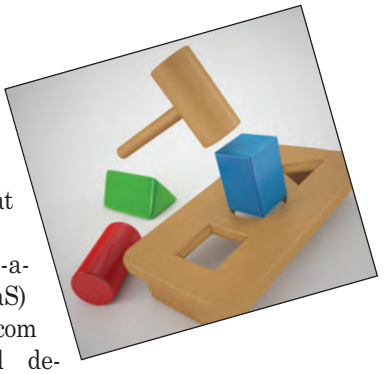
Conversely, the court in *Mailhoit v. Home Depot U.S.A. Inc.*, found that requests for social media data failed to satisfy the Federal Rules of Civil Procedure 34's "reasonable particularity" requirement and denied the bulk of the requests. Similarly, when it comes to which party pays for e-discovery costs, courts across the country have yet to settle on a standard.

"E-discovery cost allocation remains ripe for consideration by the Advisory Committee on Civil Rules in 2013 when evaluating amendments to the Federal Rules of Civil Procedure," concluded Kroll Ontrack.



CLOUD

Cloud Computing Creates Strange Bedfellows



Demands from large higher-end enterprises and other customers for complete, end-to-end services are prompting cloud service providers to form new partnerships. For example, as of this writing, AT&T had aligned with IBM and CSC with Sprint to offer a more comprehensive range of services.

"Alliances between vendors, such as AT&T/IBM and Sprint/CSC, will change the game in the coming year," said Ashok Kumar, associate director of custom research at Current Analysis. Kumar's prediction was based on the results of Current Analysis's recent Enterprise Cloud Adoption study.

In general, the research indicated that "enterprises are now moving beyond cloud experimentation to broader-based implementations," commented Bruce Page, vice president of custom research at Current Analysis. He said 64% of the responding enterprises reported they use the cloud, and the remainder expects to make the transition within the next two years.

The study also revealed that although software-as-a-service (SaaS) is the most common cloud deployment, infrastructure-as-a-service (IaaS) doubled in 2012. Further, security remains the most pressing concern both pre- and post-deployment. But the final decision most often (67%) resides with an enterprise's senior management, not the IT organization.

GOVERNMENT RECORDS

Cloud Computing, Social Media New Competencies for Fed CIOs

The recently published *2012 Clinger-Cohen Core Competencies and Learning Objectives* includes nine new competencies under the 12 core competency areas federal chief information officers need to effectively manage federal technology resources.

Published in December 2012 by the Chief Information Officers Council (CIO Council), these new competencies include:

- IT Governance
- Cybersecurity/Information Assurance Strategies and Plans
- Social Media
- Cloud Computing
- Information Accessibility

According to the report, the competencies and learning objectives are the basis for developing and implementing IT policies across the U.S. federal government. Educational institutions also use them to develop curriculum offered through programs under the CIO University Consortium umbrella. They can also be used as guidelines by individuals and organizations.

Twelve federal agencies, academic representatives from the CIO University Consortium, and members of the Industry Advisory Council helped review the changes drafted by the CIO Council's IT Workforce Committee.

IMAGING

3D Technology to Make Old New Again

An Austrian artist was awarded a £60,000 ($95,000 U.S.) commission by the Contemporary Art Society to turn classical and archaeological objects into digital and hologram forms using 3D scanners.

According to *The Independent*, artist Oliver Laric will scan all the works in The Collection and Usher Gallery — from classical sculptures to archaeological finds. His goal is to "[eliminate] historical and material hierarchies and to reduce all works to objects and forms."

The scans will be made available to the public to view, download, and use for free from the museum's website and other platforms, free from copyright restriction and available for social media and academic research alike. In addition, the artist will use the scans to create a sculptural collage for the museum, for which the digital data will be combined, 3D printed, and cast in acrylic plaster.

PRIVACY

Victoria Establishes Privacy and Data Security Office

Victoria (Australia) Attorney-General Robert Clark recently announced its plans to create an office of the Privacy and Data Protection Commissioner. The office intends to bring "together the skills and resources of the Privacy Commissioner and the Commissioner for Law Enforcement Data Security."

David Watts, the law enforcement commissioner, was tapped to lead the transition from two existing bodies into the one new entity. The new privacy and data protection commission is expected to spearhead the implementation of a new Victorian Protective Security Policy Framework for the government departments and agencies.

EHR

EHR Vendors to Feds: Slow Down!

Electronic health record (EHR) vendors have asked the U.S. government to slow down and focus on "encouraging and assisting providers to take advantage of the substantial capabilities established in Stage 1 and especially Stage 2, rather than adding new meaningful use requirements and product certification criteria."

The EHR Association, representing 40 EHR vendors, posed the request in its comments regarding the proposed Stage 3 requirements. The group stated its belief "that any meaningful use and functionality changes should focus primarily on interoperability and building on accelerated momentum and more extensive use of Stage 2 capabilities and clinical quality measurement." The vendors requested that Stage 3 be delayed at least three years so the focus could be on these areas.

They also encouraged the government to invest in quality measure alignment, infrastructure, and standards, and to focus on building on the foundation begun in Stage 2 without adding a significant number of new quality measures.

The government regulations take a one-size-fits-all approach, which has proved cumbersome for some healthcare providers. Unfortunately, there hasn't been time to examine what's working well.

"To keep moving ahead with such an aggressive strategy strikes me as foolish," Stephanie Reel, vice provost for information technology and chief information officer at Johns Hopkins University, told *Forbes*. "We don't know what's working, and what's not working."

"Our proposed alternative approach is offered in recognition that the public and private sector shifts to accountable care and value-based payment are now creating a business case for providers to adopt and use EHRs and other health IT, and to identify needed functionality to meet their varied technology requirements," stated the EHR Association in its comments.

Interoperability is a perfect example. It has never been a priority for vendors or hospitals. Now it's at the top of the list because payments are tied to care coordination. Vendors want to make sure standards for transmitting patient data between different platforms are adequate by testing them before they're set in stone. "We need the time to do it right," John Glaser, chief executive officer of Health Services at Siemens Healthcare, told *Forbes*.

Innovation could be the biggest casualty. Neither vendors nor providers have time to evaluate and plan improvements. Products become generic and patient care suffers.

As illustration, Reel noted that the time the IT department used to be spend working with physicians and others to create ways to improve patient care is now being spent ensuring they are meeting government rules.

"We're sacrificing innovation because of requirements to be compliant. The trade off is stark," she said.

E-RECORDS

Namibia Home Affairs Switches to Electronic Records

AllAfrica.com reported that the Namibia Ministry of Home Affairs and Immigration has "kissed manual record keeping goodbye." The ministry went live with its electronic document and records management system (EDRMS) just before the end of the year.

According to EDRMS project manager, Sarah Negumbo, from the prime minister's office, the project intends to ensure a risk-free electronic records and archival system for the public service in line with the National Archives Act of 1992.

"Records are not filed according to the filing system as per archives codes, making it difficult for records to be retrieved. Another aspect that the EDRMS implementation is addressing is the issue of security, because it was also discovered that some of the registries do not have security measurements in place in terms of preventing unauthorized access," Negumbo told *AllAfrica*.

The plan is to implement the system across all government offices, ministries, and agencies.

CLOUD

Singapore Claims Highest Understanding of Cloud

Forrester Research's recently published *VMWare Cloud Index 2012* found that Singapore companies rank highest in the Asia-Pacific (APAC) region for their confidence in their knowledge about cloud computing.

According to the report, 82% of Singapore respondents said they believed they had a strong understanding of cloud computing, which was higher than the APAC region's average response of 75%. This is the first time Singapore came out on top in this category; Australia had held that position the previous two years of the study.

In terms of cloud usage, the top three countries are Australia (58%), Singapore (51%), and India (50%), all significantly higher than the regional average of 42%. It's not surprising, then, to see that Singapore companies expressed the highest concerns in the region about data privacy and data residency.

In his briefing regarding the VMWare study results, Michael Barnes, vice president and research director of Forrester Research, noted that this may help explain why so many companies in Singapore reported an adequate understanding and awareness of cloud.

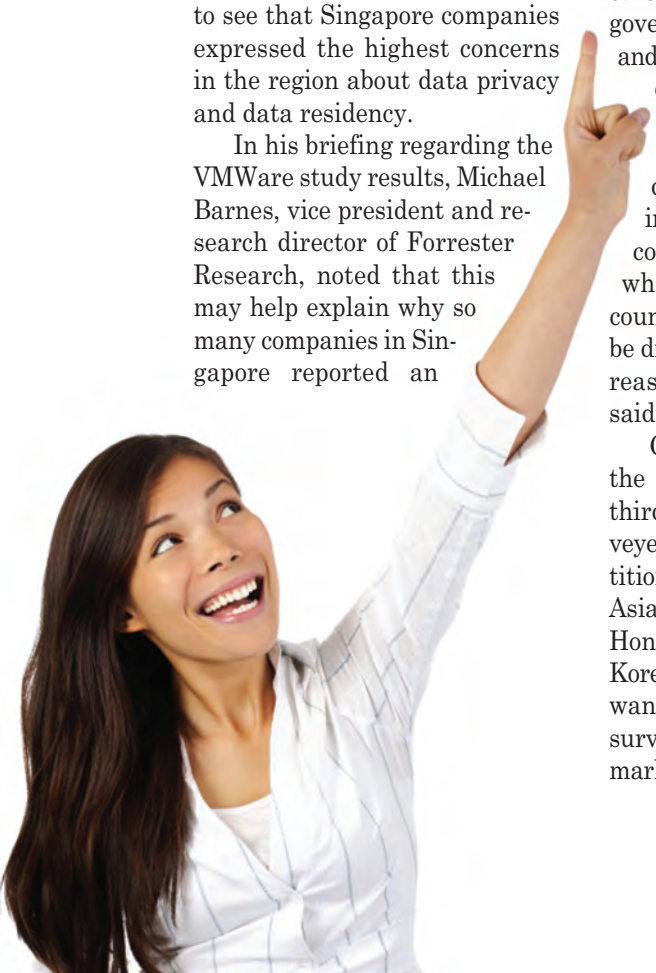
Respondents who believe they strongly understand cloud

1. Singapore: **82%**
2. Korea: **80%**
3. India: **79%**
4. Australia: **72%**
5. Hong Kong: **74%**
6. Taiwan: **72%**
7. China: **72%**
8. Thailand: **70%**
9. Indonesia: **70%**
10. Malaysia: **66%**

The Singapore government's "pro-cloud" stance is likely another contributor. Barnes said the governments in both Singapore and Hong Kong have consistently encouraged investments in local data centers.

"The government has done a remarkable job in luring datacenter investments to come into the country… whereas authorities in other countries or certain states could be discouraging cloud for various reasons, even jingoistic ones," said Barnes.

Commissioned by VMware, the cloud index study is in its third year. The 2012 study surveyed nearly 5,000 senior IT practitioners in 10 economies across Asia-Pacific: Australia, China, Hong Kong, India, Indonesia, Korea, Malaysia, Singapore, Taiwan, and Thailand. (Japan was surveyed separately by another market research firm.)



CLOUD

Ireland Gets Serious About the Cloud

Like many countries, Ireland is looking to the cloud for new growth opportunities. The government committed €5 million ($6.7 million U.S.) to fund a cloud computing technology research center.

The Irish Centre for Cloud Computing and Commerce (IC4), housed at Dublin City University, is meant to help speed up the development and adoption of cloud technology in Ireland. That means more jobs within the Irish IT sector.

"Cloud computing is already a significant part of the overall market for information technology and services and is now one of the fastest growing segments of the market. That why as part of the Government's Action Plan for Jobs we have specifically targeted this sector for jobs and growth in the coming years," explained Minister for Jobs, Enterprise and Innovation Richard Bruton.

According to its website, IC4 differs from other university-based research centers in that it is both multi-institutional and inter-disciplinary, including researchers from computing, business, and law. Its industry panel includes such recognizable players as IBM, Intel, Microsoft, and Fujitsu.

IC4's research agenda focuses on four broad, core research themes that the industry participants consider to be of equal importance; no distinction is made between server-side and client-side research. Those themes include:

- Architecture, including scalability and performance, reliability and resilience, interoperability, portability, and migration to the cloud
- Service lifecycle, including service delivery, service levels for a quality cloud service, and cloud service level assessment
- Business research, including business and organizational models, regulations for cloud services, and cloud as a competitive advantage
- Cloud security, including scalable and single/multi-tenant environments, data transfer in the cloud, mobile and security in the cloud, and risk management and disaster recovery

Outreach is key in 2013. IC4 has identified three major initiatives:

- Cloud Computing and Commerce Capacity Building Programme
- National Cloud Technology Incubator and CloudClinic Programme
- Cloud Technology Standards Observatory

DATA SECURITY

Microsoft, Symantec Take a Bite out of Cybercrime

Software powerhouse Microsoft announced in early February that its Digital Crimes Unit, in conjunction with Symantec, successfully took down the Bamital botnet. According to Microsoft, the botnet hijacked people's search results and took them to potentially dangerous websites that could install malware onto their computers, steal personal information, or fraudulently charge businesses for online advertisement clicks.

Microsoft filed a lawsuit January 31, supported by a declaration from Symantec, against the botnet's operators in order to sever all communication lines between the botnet and the malware-infected computers under its control. The court granted the requests, and technicians from Microsoft and Symantec, accompanied by U.S. federal marshals, seized data and evidence from the botnet through raids on data centers in New Jersey and Virginia.

Research conducted by Microsoft and Symantec showed that more than eight million computers have been attacked by Bamital during the last two years. Further, its search hijacking and click fraud schemes affected many of the major browsers, including Microsoft's Bing, Yahoo, and Google. In a proactive move, Boscovich added, owners of infected computers trying to complete a search query are being directed to an official Microsoft and Symantec webpage that explains the problem and offers guidance on how to remove Bamital and other malware from their computers.

BIG DATA

Big Data in 2013: What to Expect

Forrester Research's Mike Gautlieri recently shared his predictions for big data in 2013. He narrowed in on four key themes, but the underlying message for enterprises, he contended, is "opportunity."

1. **Companies will realize that "big data" means ALL of their data.** Some define big data by how it can be measured in terms of volume, velocity, and variety. The flaw in this definition, contends Guiltier, is that it is "not an actionable, complete definition for IT and business professionals. He suggests a more pragmatic definition: "Big Data is the frontier of a firm's ability to store, process, and access (SPA) all the data it needs to operate effectively, make decisions, reduce risks, and serve customers." Furthermore, it will continue to reside in all kinds of data architectures, including enterprise data warehouses, application databases, file systems, cloud storage, Hadoop, and others.
2. **The algorithm wars will begin.** Organizations are coming to realize that they "must use predictive and descriptive analytics to find no obvious information to discover value in the data." Advanced analytics, Gautier explains, uses advanced statistical, data mining, and machine-learning algorithms to dig deeper to find patterns that you can't see using traditional business intelligence tools, simple queries, or rules. He predicts that companies will rediscover the power of old algorithms and find competitive new ones.
3. **Real-time architectures will swing to prominence.** "Firms that find predictive models in big data must put them to use," says Gautlieri. This means employing technologies to make that possible, and mobile will continue to be a key driver. As a result, he predicts, "enterprise architects will step out of their ivory towers to once again focus on technology — real-time technology that is highly available, scalable, and performant."
4. **Naysayers will fall silent.** Big data isn't just a buzzword, it's real. According to Gautlieri, "It disrupts many who don't see anything new in it or don't see the tremendous opportunity firms have to harness it for competitive advantage." **END**