

SC

MAGAZINE
Spotlight

This Spotlight issue of *SC Magazine* explores the exploding market of cloud services and tools, and the effect this new paradigm is having on enterprise defense.

SHINING THE “SPOTLIGHT” ON THE:

CLOUD

INCLUDING:

P10 At your service

Understanding how your cloud vendor defines security and the assurance protocols it employs is essential.

P16 Safe passage

With cloud computing becoming popular for e-commerce, what are the security and privacy concerns moving forward?

P22 Ahead in the cloud

IlliniCloud provides the technology backbone that helps school districts in Illinois manage critical IT functions

Leverage the power of the cloud. SECURELY.



The cloud is a dangerous place for sensitive data. We make it safer.

The cloud brings risk.

Websense security for cloud-based apps

How can you harness the power of cloud apps securely? Effective data loss prevention (DLP) is a critical element. Websense® TRITON™ solutions combine web and email security with industry-leading DLP to identify, discover, fingerprint and help protect your data everywhere.



Get a free DLP whitepaper at www.websense.com/cloud-security

The cloud brings security.

Websense Security-as-a-Service

Our Websense Hosted Security lets you leverage the cloud for:

- Lower hardware, software, bandwidth, and maintenance costs
- Flexible hosted and hybrid configurations
- Reliable and secure - 99.999% uptime SLA and ISO27001-certified*

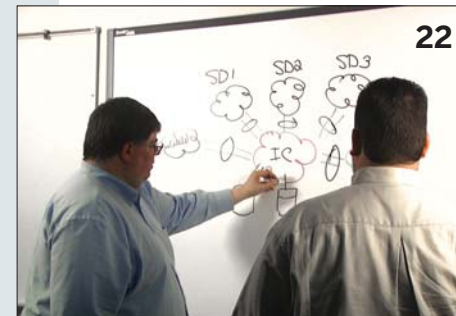


Watch a free demo at www.websense.com/saas

With Websense, you can stay a step ahead of the threats. From our roots in web filtering, we've been analyzing and classifying content for more than 15 years, and we now offer must-have web, email, and data security that closes the gaping holes left by traditional security products.

*See terms and conditions for specifics.

© 2011 Websense Inc. All rights reserved. Websense is a registered trademark of Websense, Inc. in the United States and certain international markets. Websense has numerous other registered and unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners. Photo credit: NOAA/DOC.



REGULARS

- 5 Editorial** Welcome to our special Spotlight edition on the cloud.
- 6 DataBank: Cloud gauge** Some graphs and data bites on the use of cloud services and tools, and their effect in the workplace.
- 8 News Update** As cloud deployments grow at a rapid pace, so too does the need for security standards that apply to these new environments.

FEATURES

- 10 At your service**
Understanding how your cloud vendor defines security and the assurance protocols it employs is essential.
- 16 Safe passage**
With cloud becoming popular for e-commerce, what are the security and privacy concerns moving forward?
- 19 Cloud query**
A number of leading cloud experts explain how their companies provide secure and cost-efficient solutions to their customers.
- 22 Ahead in the cloud**
IlliniCloud provides the technology backbone that helps several school districts in Illinois manage critical IT functions.
- 24 Remote options**
Can cloud providers be trusted with your most sensitive data? We find out.



Cover illustration by Marc Tobin

This Spotlight issue of SC Magazine explores the exploding market of cloud services and tools, and the effect they are having on enterprise security.

SC Magazine™ (ISSN No. 1096-7974) is published 12 times a year on a monthly basis by Haymarket Media Inc., 114 West 26th Street, 4th Floor, New York, NY 10001 U.S.A.; phone 646-638-6000; fax 646-638-6110. Periodicals postage paid at New York, NY 10001 and additional mailing offices. POSTMASTER: Send address changes to SC Magazine, P.O. Box 316, Congers, NY 10920-0316. © 2011 by Haymarket Media Inc. All rights reserved. Annual subscription rates: United States: \$98; Canada and Mexico: \$110; other foreign distribution: \$208 (air service). Two-year subscription: United States: \$175; Canada and Mexico: \$195; other foreign distribution: \$375 (air service). Single copy price: United States: \$20; Canada, Mexico, other foreign: \$30. Website: www.scmagazineus.com.



WHAT IS SCWC 24/7

SC Magazine has created a free virtual environment that is open year-round. Each month we host an event focused on a subject that you as an IT security professional face on a regular basis.

THIS MONTH



Sept. 20 eConference on data security

Many leading CSOs at various conferences this year touted the need for organizations to have their security controls follow and protect their most important data assets, rather than the network. So, just how is this best achieved and what policies, plans and technologies can help?

ON DEMAND

IPv6
As many of the newest operating systems and network devices stand at the ready for IPv6 – given that most implement the latest protocol by default, gaping holes can easily be introduced to the network.

Social networking

Beyond the ability for cybercriminals to enlist social networking sites to cull pertinent details, such sites still are rife with malware and social engineering attacks. What can companies do to protect their end-users and their own critical data as staff access their profiles? We discuss best practices and other tactics and tools.

Securing the cloud

Enterprise end-users are becoming more reliant on cloud computing applications and virtualized environments to enable the quick sharing of information.

FOR MORE INFO

For information on SCWC 24/7 events, please contact Natasha Mulla at natasha.mulla@haymarketmedia.com.

For sponsorship opportunities, contact Mike Alessie at mike.alessie@haymarketmedia.com. Or visit www.scmagazineus.com/scwc247.



SC MAGAZINE EDITORIAL ADVISORY BOARD 2011

- Rich Baich**, principal, security & privacy, Deloitte and Touche
- Greg Bell**, global information protection and security lead partner, KPMG
- Christopher Burgess**, senior security adviser, corporate security programs office, Cisco Systems
- Jaime Chanaga**, managing director, CSO Board Consulting
- Rufus Connell**, research director - information technology, Frost & Sullivan
- Dave Cullinane**, chief information security officer, eBay
- Mary Ann Davidson**, chief security officer, Oracle
- Dennis Devlin**, chief information security officer, Brandeis University
- Gerhard Eschelbeck**, chief technology officer and senior vice president, engineering, Webroot Software
- Gene Fredriksen**, senior director, corporate information security officer, Tyco International
- Maurice Hampton**, Qualys; formerly information security & privacy services leader, Clark Schaefer Consulting
- Paul Kurtz**, partner and chief operating officer, Good Harbor Consulting
- Kris Lovejoy**, vice president of IT risk, office of the CIO, IBM
- Tim Mather**, director, information protection, KPMG
- Stephen Northcutt**, president, SANS Technology Institute
- Randy Sanovic**, former general director, information security, General Motors
- * Howard Schmidt**, cybersecurity coordinator, White House; president and chief executive officer, Information Security Forum
- Justin Somaini**, chief information security officer, Yahoo!; former chief information security officer, Symantec; former director of information security, VeriSign
- Craig Spieziele**, chairman, Online Trust Alliance; former director, online safety technologies, Microsoft
- W. Hord Tipton**, executive director, (ISC)²; former CIO, U.S. Department of the Interior
- Amit Yoran**, chief executive officer, NetWitness; former director, Department of Homeland Security's National Cyber Security Division
- * emeritus

WHO'S WHO AT SC MAGAZINE

- EDITORIAL**
- EDITOR-IN-CHIEF** Illena Armstrong illena.armstrong@haymarketmedia.com
- EXECUTIVE EDITOR** Dan Kaplan dan.kaplan@haymarketmedia.com
- MANAGING EDITOR** Greg Masters greg.masters@haymarketmedia.com
- SENIOR REPORTER** Angela Moscaritolo angela.moscaritolo@haymarketmedia.com
- TECHNOLOGY EDITOR** Peter Stephenson peter.stephenson@haymarketmedia.com
- SC LAB MANAGER** Mike Stephenson mike.stephenson@haymarketmedia.com
- DIRECTOR OF SC LAB OPERATIONS** John Aitken john.aitken@haymarketmedia.com
- SC LAB EDITORIAL ASSISTANT** Judy Traub judy.traub@haymarketmedia.com
- PROGRAM DIRECTOR, SC CONGRESS** Eric Green eric.green@haymarketmedia.com
- CONTRIBUTORS** Stephen Lawton, Deb Radcliff, Jim Romeo
- DESIGN AND PRODUCTION**
- ART DIRECTOR** Brian Jackson brian.jackson@haymarketmedia.com
- VP OF PRODUCTION & MANUFACTURING** Louise Morrin louise.morrin@haymarketmedia.com
- SENIOR PRINT AND DIGITAL CONTROLLER** Krassi Varbanov krassi.varbanov@haymarketmedia.com
- SC EVENTS**
- SENIOR EVENTS MANAGER** Natasha Mulla natasha.mulla@haymarketmedia.com
- SENIOR EVENTS COORDINATOR** Anthony Curry anthony.curry@haymarketmedia.com
- EVENTS ASSISTANT** Maggie Keller maggie.keller@haymarketmedia.com
- U.S. SALES**
- ADVERTISING DIRECTOR** David Steifman (646) 638-6008 david.steifman@haymarketmedia.com
- EASTERN REGION SALES MANAGER** Mike Shemesh (646) 638-6016 mike.shemesh@haymarketmedia.com
- WEST COAST BUSINESS MANAGER** Matthew Allington (415) 346-6460 matthew.allington@haymarketmedia.com
- NATIONAL ACCOUNT MANAGER - EVENT SALES** Mike Alessie (646) 638-6002 mike.alessie@haymarketmedia.com
- ACCOUNT EXECUTIVE** Dennis Koster (646) 638-6019 dennis.koster@haymarketmedia.com
- SALES/EDITORIAL ASSISTANT** Roo Howar (646) 638-6104 roo.howar@haymarketmedia.com
- UK ADVERTISEMENT DIRECTOR** Mark Gordon 44 208 267 4672 mark.gordon@haymarketmedia.com
- LICENSE & REPRINTS ACCOUNT EXECUTIVE** Malika Toure (646) 638-6101 malika.toure@haymarketmedia.com
- EMAIL LIST RENTAL**
- EMAIL SENIOR ACCOUNT MANAGER** Frank Cipolla, Edith Roman Associates (845) 731-3832 frank.cipolla@epostdirect.com
- CIRCULATION**
- GROUP CIRCULATION MANAGER** Sherry Oommen (646) 638-6003 sherry.oommen@haymarketmedia.com
- SUBSCRIPTION INQUIRIES**
- CUSTOMER SERVICE:** (800) 558-1703
- EMAIL:** Haymarket@cambeywest.com
- WEB:** www.scmagazineus.com/subscribe
- MANAGEMENT**
- CEO OF HAYMARKET MEDIA** Lee Maniscalco
- DEPUTY MANAGING DIRECTOR** Tony Keefe

A mix of sun and clouds

Maintaining effectiveness, while being efficient and cost-conscious is still a driving force behind many a business decision. To save money often can mean a much-needed boost to the bottom line. A tarrying, manic economy that keeps many executives guessing has made sure such thinking still leads the day.

It's almost expected, then, that cloud services, which offer such benefits to organizations as reduced cost, scalability, flexibility, mobility and more, would be espoused wholeheartedly by any money-savvy CEO. The resulting main worry for their CISOs and other technology experts is securing all the corporate information stored in and exchanged through the cloud. After all, the lower total cost of ownership the cloud offers is quickly negated when critical business data is exposed or stolen because it proved easy pickings to persistent cybercriminals.

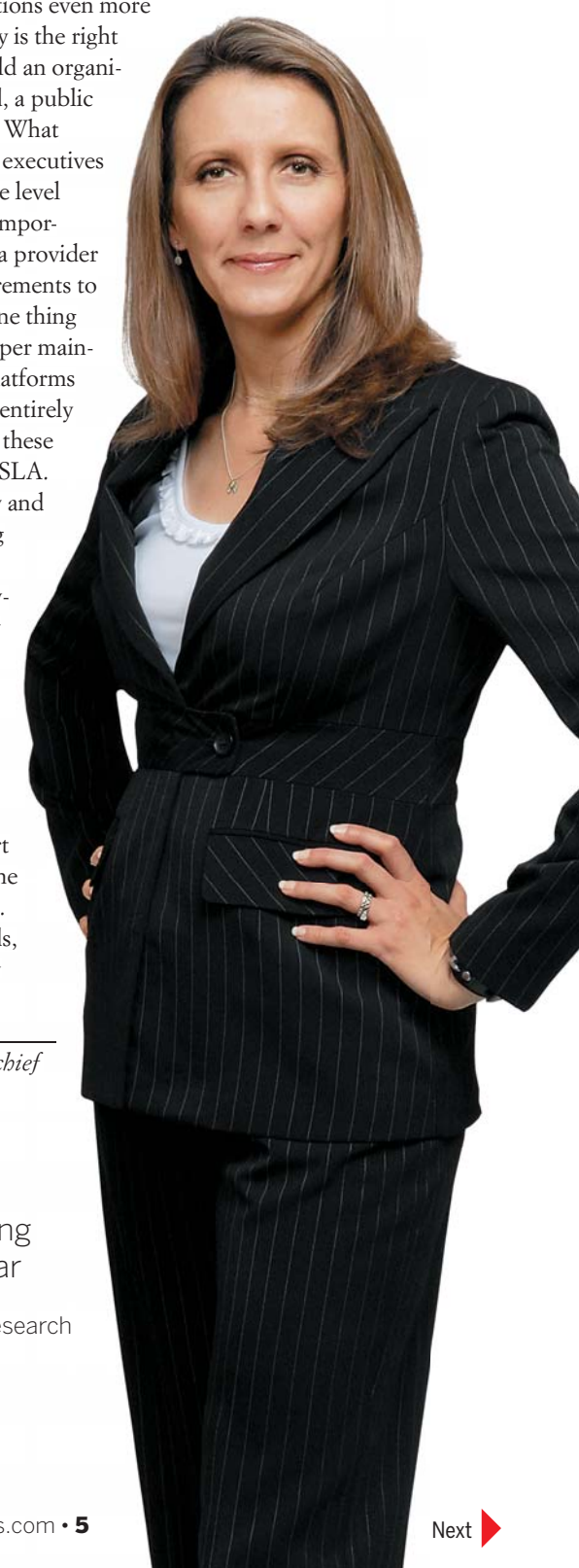
To methodically and diligently safeguard data in the cloud involves a lot of professionals. A corporate security officer who might have her own company's infrastructure locked down tight is forced to rely on and trust that the cloud service provider knows a thing or two about security. And, that's tough given the complexity cloud models can introduce.

For instance, how is access to data in the cloud handled? Is it secure? What about vulnerability updates to storage servers? And, where exactly are the service provider's servers anyway? How can companies stay compliant with any number of regulations when using cloud services (a question which makes the

previous question about locations even more important)? Too, what exactly is the right service delivery model? Should an organization go with a private cloud, a public cloud or a hybrid of the two? What security requirements should executives ensure are noted in the service level agreement (SLA) and, more importantly, how do they convince a provider that's resistant to those requirements to sign on the dotted line? It's one thing for a provider to promise proper maintenance and security of the platforms on which customers rely, but entirely another to actually guarantee these areas are covered in a formal SLA.

Just how to handle security and compliance issues when using cloud services is proving a conundrum for many. However, it's one that many industry pros are trying to overcome. In this *SC Magazine Spotlight* edition, we take an in-depth look at the various problems organizations like yours could face when turning to the cloud, and seek out expert advice and insight on just some of the ways to deal with these. So, if your head's in the clouds, take a moment to let us know what you think.

Illena Armstrong is editor-in-chief of SC Magazine.

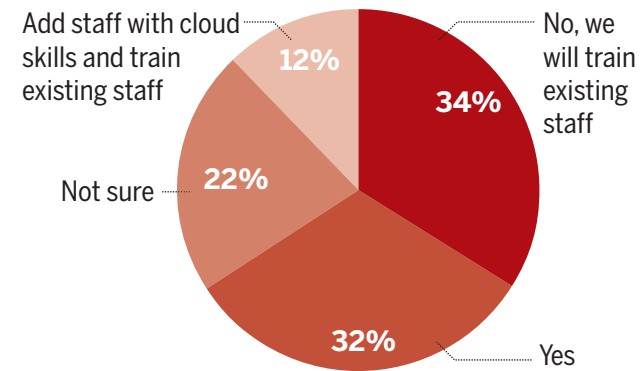


\$40.7B cloud computing market this year
— Forrester Research

CloudGauge

Future personnel needs

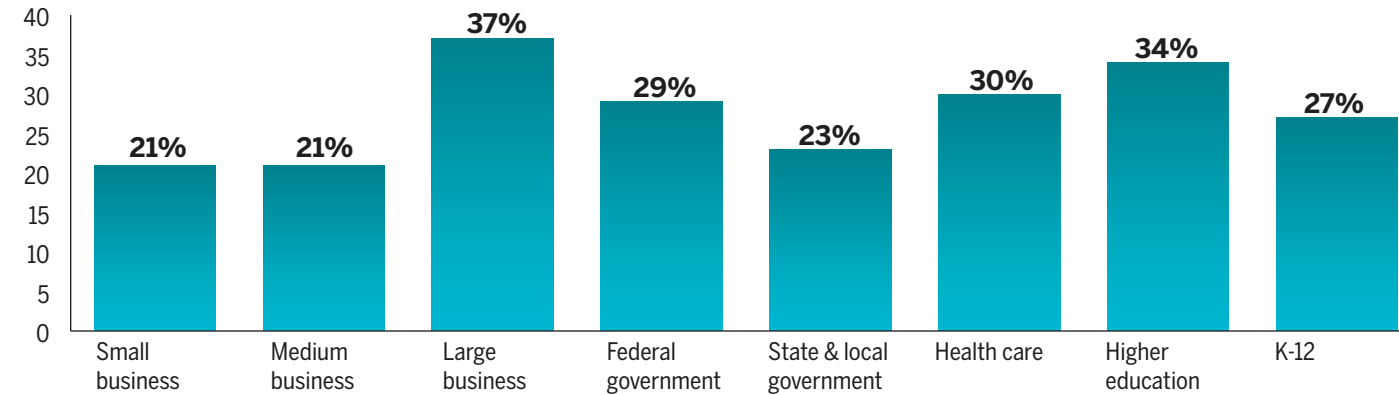
Do you expect you will need to hire additional IT operations staff who possess cloud skills? Source: ScienceLogic government survey, summer 2011



Industry cloud adoption

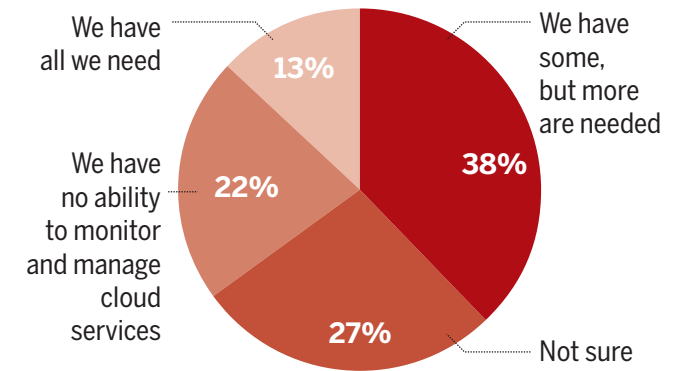
Percentage of organizations implementing or maintaining cloud computing

Source: CDW, From Tactic to Strategy, 2011



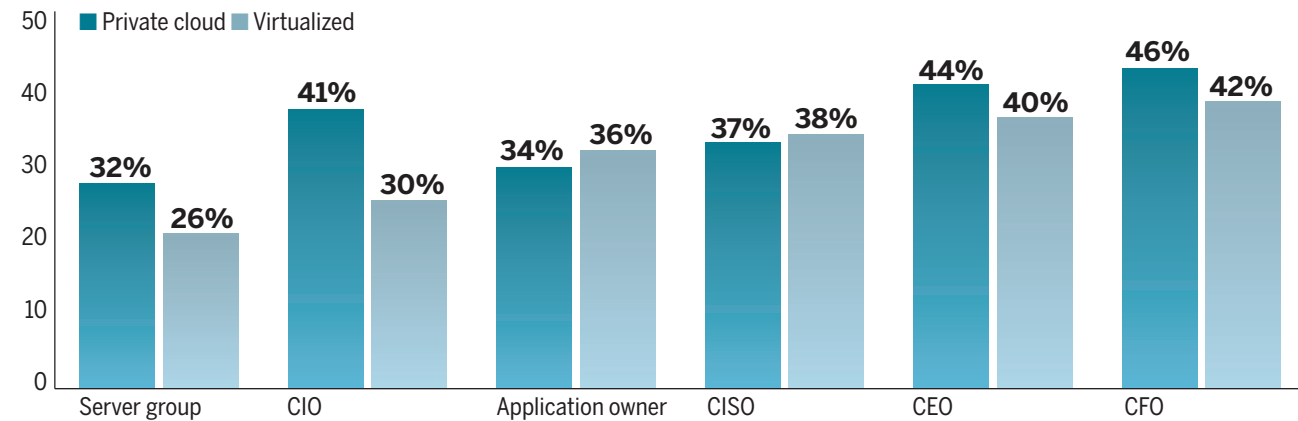
The right tool for the job

Do you have the tools required to monitor and manage the performance of cloud services? Source: ScienceLogic government survey, Summer 2011



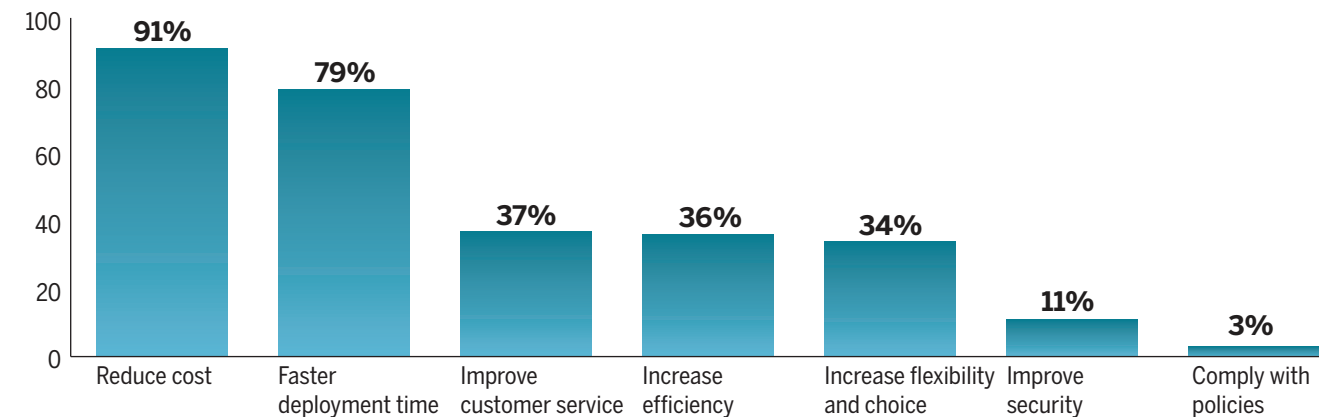
IT and business executives out of sync

Are you open to moving mission-critical apps to cloud environments? Source: Symantec, 2011 Virtualization and Evolution to the Cloud Survey



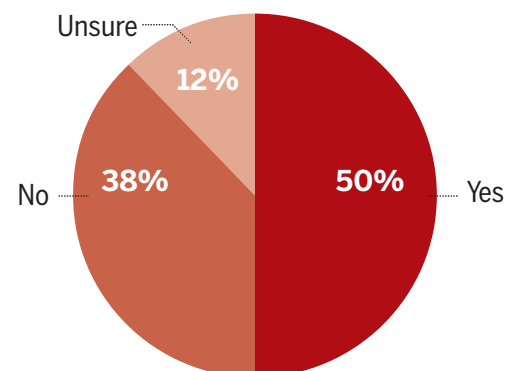
Cost savings primary driver to cloud implementation

Reasons customers migrate to the cloud computing environment (U.S. & Europe) Source: Ponemon, Security of Cloud Computing Providers Study, April 2011



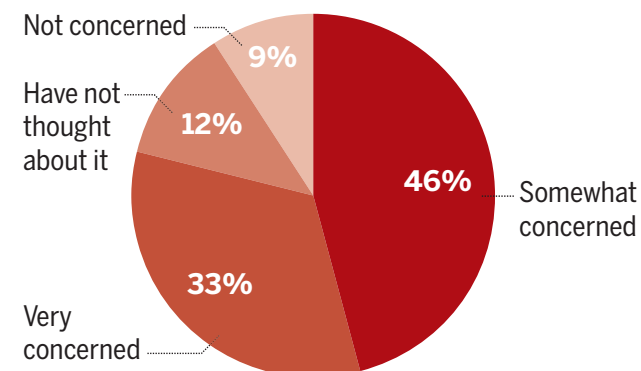
Adoption proceeds

Does your organization have a written plan for the adoption of cloud computing? Source: CDW, From Tactic to Strategy, 2011



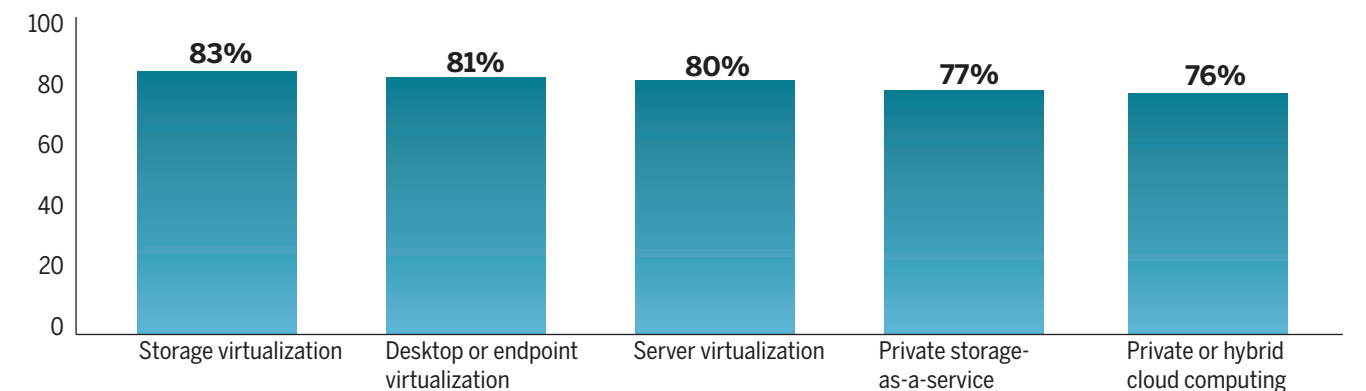
Cloud anxiety

How concerned are you about the performance and availability of services hosted in the cloud? Source: ScienceLogic government survey, Summer 2011



A lot of talk about cloud implementation

At what stage is your organization in each of the following areas? Source: Symantec, 2011 Virtualization and Evolution to the Cloud Survey



News Update

A standard approach

Cloud computing is, no doubt, increasingly making its way into enterprise environments thanks to alluring benefits, such as reduced costs and increased flexibility. But, as cloud deployments grow at a rapid pace, so too does the need for security standards that apply to the new technologies.

Standards are necessary, for one, to be able to show compliance with existing mandates, said Jim Reavis, executive director of the nonprofit Cloud Security Alliance (CSA). Also, from an overall risk management perspective, standards provide an objective security baseline to help organizations manage threats introduced by cloud computing.

There is a flurry of activity underway to develop such guidelines, Reavis said. The CSA is working to bridge the gap between slow-moving standards bodies and the rapidly evolving cloud market economy, he added.

“Almost any standards body that has traditionally done a standard related to information security will have something they are working on,” Reavis said.

The International Organization for Standardization (ISO), which developed the widely accepted ISO 27000-series information security management standards, is working on a new body of guidelines related to cloud computing, Reavis said. The five-part standard, which is a work in progress and tentatively named ISO 27017, is intended to cover information security controls required by both cloud computing providers and customers.

Members of the CSA are also working with the ITU, a United Nations agency responsible for telecommunication standards, to examine how security is delivered through the cloud via security-as-a-service (SaaS) solutions, Reavis said. That effort will also likely lead to standardization.

Cloud computing users are currently operating in an “evolving, pre-standards market,” he said. For this reason, it’s important for users to stay abreast of what type of benchmarks they may need to comply with in the future.

While various groups are hard at work, finalized versions are still a ways off, according to Marlin Pohlman, chief governance officer at EMC and chair of CSA’s standards committee. A final draft of ISO 27017 should be released for review by mid-October, at which point it will be up for public comment for two years before being finalized. Meanwhile, the ITU standards development process will likely take about a year.

Ultimately, standards are necessary to provide cloud customers with a way to choose among various offerings, said Vint

Cerf, Google’s chief internet evangelist, who along with Bob Kahn, is recognized as one of the founders of the internet.

“The purpose is not to inhibit development of new, competitive and potentially incompatible services, but rather to provide at least a basic way in which to evaluate offerings in a commensurate fashion,” Cerf said. “Ideally, users should not be locked into any one cloud provider without an ability to move to a new one.”

Ensuring availability

Every practitioner knows that the three pillars of information security are confidentiality, integrity and availability.

These days, given the popularity of cloud computing, the job of protecting the availability of data requires more than just warding off distributed denial-of-service (DDoS) attacks, said Jake Kouns, president of the nonprofit Open Security Foundation (OSF), which runs Cloutage.org, a project to document cloud service incidents. While attention is paid to major cloud computing outages, such as the multi-day blackout of Amazon Elastic Compute Cloud (EC2) in April, organizations may be overlooking the risk posed by smaller, more frequent service degradations, he warned. “Outages and availability issues are real and they continue to happen,” Kouns said.

Minor failures, such as those lasting just a few minutes and affecting a small subset of a provider’s customers, occur “more often than we expect,” Kouns said. Added together, the impact of downtime can be quite substantial.

Before embracing the cloud, organizations should evaluate the frequency of both large and small-severity outages their potential provider has sustained, Kouns said.

Configuration options and features to create a more “bulletproof” environment offered by the provider also must be taken into consideration, he said. The use of multiple availability zones and load balancing, for example, can provide the redundancy needed to withstand service failures with little to no downtime. There is often an added cost associated with such features, however.

Kouns recommended security practitioners evaluate their company’s tolerance for an interruption, and determine the acceptable amount of downtime. Then, put the controls in place



to provide redundancy as necessary.

Perhaps most importantly, organizations must develop a plan for when, not if, an outage occurs, Kouns said. He advised working with cloud providers to understand service and support standards before such incidents. Also, simulated outages can help prepare employees for an eventual failure.

The good news is that cloud providers seem to be learning from past mistakes, Kouns said. Vendors commonly conduct inquiries to determine the root cause of outages that have occurred, enabling them to improve their services. Still, it is incorrect to believe that the cloud is fool-proof, he warned.

“There’s nothing wrong with going to the cloud,” Kouns said. “Organizations need to understand the risks and appropriately manage them. To blindly jump in is not appropriate.”

Consumer-driven risks

A new class of consumer-oriented cloud services, such as Apple’s recently announced iCloud, could leave organizations more vulnerable to data loss, experts say.

iCloud, to be launched this fall, will allow users to store music, photos, apps, calendars and documents in the cloud, and wirelessly push data to all their devices. In all its hype of the new service, Apple has, as of yet, failed to communicate how it intends to secure data, said Andrew Storms, director of security operations at nCircle.

“Apple hasn’t historically addressed enterprise security concerns and requirements on the first revision of its products,” Storms said.

Besides iCloud, services such as Livedrive, Dropbox and Mozy offer a simple and inexpensive way to back up and share documents online. These services are convenient and useful, but could have a major impact on an organization’s security and compliance, Storms said.

These cloud services are opening a new door through which emails, contracts or other confidential company documents can exit an enterprise, experts say.

Dropbox, for example, recently admitted that for several hours one day in late June, anyone could have logged into user accounts without any password at all. The company blamed the security lapse on a faulty code update. In the case of iCloud, criminals will likely attempt to use social engineering methods to trick users into revealing their logins, experts said.

In addition, these services, which are meant to rapidly make files accessible to multiple devices, could also be abused by individuals to spread malware, said Andrew Jaquith, CTO at Perimeter E-Security. If one device became infected, the malicious file could subsequently be pushed to all of a user’s devices. “It could be a pretty amazing malware distribution mechanism,” Jaquith said.

Despite the potential for data loss, many enterprises are currently ignoring the dangers, Jaquith said. Some have even embraced the services without considering the ramifications.

“With consumer technology in the workplace, you go through stages of adoption a lot like the stages of grief,” he said. “With cloud services, we are in the denial and anger stage.”

Jaquith said he believes cloud-based file synching services are unfit for business use. “This does not have a place in the enterprise, especially if you are working in an industry with any level of regulation,” he said.

For now, organizations may choose to blacklist the services or ramp up user security awareness programs, Storms said. Several security vendors are developing anti-virus and data leakage prevention products that can scan cloud-based services, Jaquith said, but those solutions are likely a few years off.

Meanwhile, there are still a number of question marks surrounding iCloud, such as which security mechanisms it will employ and whether users will be able to control what data is synced to it. One thing is for sure, though – it will be in high demand. “There will be mass adoption,” Storms predicted.

– Angela Moscaritolo



[Consumer-oriented cloud services do] not have a place in the enterprise.”

–Andrew Jaquith, CTO at Perimeter E-Security



Understanding how one's cloud vendor defines security and employs assurance protocols is essential, reports **Stephen Lawton**.

AT YOUR

SERVICE

Despite cloud vendors' assertions of 99.9 percent uptime and worldwide data access, what many of them refer to as security is not necessarily the definition employed by users. Customers, experts say, are more concerned about their own access to the data stored on remote servers than they are about intruders finding their way into the files.

Although users might expect their cloud vendor to employ reasonable security protocols, "reasonable" being the operative term here, providers are only responsible for what is specifically in the contract agreement. Amazon EC2, for example, puts the onus for security entirely on the client. In its terms of use, the company specifically states: "We do not guarantee that Your Files will not be subject to misappropriation, loss or damage and we will not be liable if they are. You're responsible for maintaining appropriate security, protection and backup of Your Files."

Service-level agreements (SLA) with cloud providers today generally are designed to protect the vendor, not the customer, says Anders Westby, senior manager at Seattle-based Logic20/20, an IT consultancy that specializes in cloud strategies and systems.

So, understanding how one's cloud vendor defines security and employs assurance protocols is essential, adds Jared Carstensen, manager of the enterprise risk services group at Deloitte and Touche in Dublin, Ireland. One should not assume that data stored in the cloud is being backed up or that the cloud

vendor is employing any special security capabilities unless one contracts for those services, he warns.

"The cloud is driven by vendors that want to sell as many licenses as possible," Carstensen says. As a result, the basic storage package likely will have the minimum of security add-ons, and data storage will be housed in the most cost-effective locations as possible.

Cloud storage is a commodity, he says, so vendors will want to store data in the least expensive locations unless otherwise required by contractual agreements. He recommends that users negotiate security with their vendors and ensure that data required by law to stay within geographic boundaries are indeed stored on appropriate servers.

Taking responsibility

Just as users will want to make certain that their vendors provide adequate security to ensure that data does not fall into the hands of a hacker, the user must recognize that "security cannot be wholly outsourced. The onus is on the client who [owns] the data," Carstensen says.

Many experts agree that the first line of defense against data being compromised is for assets to be software-encrypted at no less than 256-bit AES (advanced encryption standard) levels. Additional encryption at the cloud level, such as hardware-based disk encryption, adds another layer of security. However, two of the most common tools in a corporate environment – log and access control files – do not neces-

sarily have the same significance in a cloud environment, nor are they always available from vendors.

Unlike a corporate data center, where files are stored on a discrete number of servers in a well-defined environment, data stored in the cloud might be sitting on 50 servers at one moment and then 100 servers a few minutes later, experts say. Whereas IT managers can build walls around corporate systems, using a combination of firewalls and segmented networks, along with such tools as access control and log files, the cloud makes those approaches next to impossible.

The cloud's *raison d'être* is its flexibility and scalability, but at the expense of commonly used security tools, experts say. Since data is moved so quickly from one system to another, log and access control files could be impractical or, in some environments, valueless.

However, a data center housed in a corporate environment does not necessarily make it more secure, says Jim Reavis, co-founder and executive director of the Cloud Security Alliance. The recent rash of corporate breaches – including EMC's security arm RSA, Sony, the U.S. Senate, the Pentagon, and several high-profile defense contractors, like Lockheed Martin – demonstrate that a corporate data center is no guarantee of security.

"All risk models start with understood risk," says Tom McAndrew, executive vice president of professional services at Coalfire Systems, a Louisville, Colo.-based IT audit and compli-

Illustration by Marc Tohin

Types of clouds

Public cloud

Essentially, there are four types of clouds. A public cloud, such as Amazon S3 or Google, is open to all comers. Users generally will have their data hosted in a multi-tenant environment, in many ways similar to the way web hosting is done. One storage server will have multiple clients' data on the same disk drive, separated by virtual machines.

Private cloud

A private cloud can be compared to a hosting environment where all of a company's data is segregated on its own physical server, which then might house multiple virtual servers. A private cloud can be located in a corporate data center or can be in a hosted environment. The difference is that firewalls, log files and access control files can be used to monitor and limit access to that cloud, just as is done in a corporate environment.

Hybrid cloud

A third cloud type is the hybrid cloud. As the name suggests, this is a combination of public and private clouds, depending on the requirements of the data. For example, data that must meet strict regulatory controls might be stored on a private cloud, while other corporate data could be stored in public clouds.

Community cloud

Essentially, there are two types of structures to a community cloud. One could be considered a supply chain cloud. A large corporation could create a cloud accessible only to its approved supply chain partners. In so doing, the manufacturer conceivably would have control over what companies can participate in its cloud.

ance firm. "Moving data to the cloud has similar risks to keeping it locally."

One of the crucial components to ensuring security is to make sure that companies do appropriate due diligence of their cloud provider's policies and procedures, as well as those of the provider's contractors, McAndrew says. "Cloud brokers will tell you what you need and how to store your data," he says. They pick your storage solution, just like an insurance broker finds the appropriate policy to meet its client's needs, he says.

To best understand the value of storing data in the cloud, the CISO needs to first understand the company's priorities. "What is your business? Where is your data? What are your storage needs?" McAndrew asks. Understanding a company's own data requirements goes a long way to helping the CISO and network administrator select a provider that can meet the company's specific needs rather than providing a one-size-fits-all offering.

Part of the decision to move data to the cloud is deciding which data to move, he says. That decision is based on a company's risk profile and on the type of cloud being used.

Users need to remember that if they require specific levels of adherence to industry or legal standards, compliance is binary – one is either compliant or not, says Coalfire's McAndrew. The customer is responsible for ensuring that its cloud provider remains in compliance through such methods as auditing and requiring the vendor to produce attestation from reliable and trusted testing organizations. The key, he says, is to ensure that data is irrelevant wherever it resides in the cloud by using encryption, tokenization or other security technologies.

Regardless of the type of cloud infrastructure a user selects or the security precautions put in place by the cloud vendor, ultimately, the owner of the data is responsible for security, says Justin Lundy, CEO of Phoenix-based Tegatai.

He recommends that, no matter the provider's security precautions, any data sent to a provider should be encrypted by the user first. Additional layers of data protection at the cloud provider's site, such as hard disk encryption or virtual machine controls, adds value, he says, but it is still up to the user to ensure that their property is safe.

An audit can lead to ROI

One method customers can use to ensure their service provider is doing what they promise is to conduct an audit, says Rick Blaisdell, CIO of ConnectEDU, a website that provides services to college students. When Blaisdell took over as CIO of the company two years ago, his first task was to make sense of all of the disparate computer systems the company operated, he says. To that end, he outsourced all of the primary computing services to a managed service provider, changing his IT department from being capital expenditure-based to operations-based.

Eliminating "almost every server" saved the company \$1.6 million on hardware purchases and software licenses, he says, with almost a 40 percent monthly

savings on IT expenses. He credits some of the savings to being in the right place at the right time and finding a provider that met his specific needs, but he also sees significant benefits to no longer having to maintain hardware and software.

The timing was beneficial, he says, because the company was in the process of updating its code base to make managing operations easier. Because those changes were already planned, the transition from a physical environment to a virtual one was easier to accomplish.

One unanticipated challenge, however, had to do with staffing and training. Blaisdell said that prior to the transition, he polled his staff to gauge their interest in moving from a hands-on engineering team to one that essentially managed service providers. He said that after the change was made, many of the staffers who had initially supported the migration to service providers found that their skill set did not match what was needed or they wanted to be managers rather than technicians. As a result, he says, he had unanticipated staffing changes.

The changes allowed Blaisdell to hire technologists who also had auditing skills. The new employees, he says, are

better able to ensure that their service provider is doing what it said it would.

Blaisdell is upbeat about his outsourced infrastructure-as-a-service (IAAS) and software-as-a-service (SaaS) environment. When it comes to security, he says his managed service provider (MSP) probably does a better job (at data security) than the company could do in a physical environment. He admits, however, "you can never have enough security."

Robert Ayoub, global program director for information security research at Frost & Sullivan, the Mountain View, Calif.-based research and consulting firm, concurs that auditing service providers is crucial. Vendors' SLAs generally address total system uptime, not necessarily a specific customer's ability to access their data. This inherent conflict of interest is something that customers and vendors need to define clearly when

the contract is signed in order to ensure that expectations are met.

Ayoub strongly recommends that any customer which plans to use a cloud provider include language in the contract that addresses the possibility of eventually changing cloud vendors. Likening the contract to prenuptial agreement, he suggests that language be included that spells out any additional costs the client will incur if it decides to move its data to another vendor, the anticipated time it will take to make the migration, and the format the data will take when delivered by the vendor. Otherwise, he says, the client could find itself waiting a long time to be presented with data that is in an inaccessible format, essentially making it worthless, even to its owner.

In fact, Ayoub says, not only must companies better understand how cloud providers will process and manage

their data, they also need to learn new negotiating skills so that they can ensure access to their data whenever and wherever they need it. Customers also need to understand the legal ramifications of a data breach to a service provider or one of its storage subcontractors.

Questions will invariably arise, he says, such as: If a service provider hires third parties to store data, who pays what if a breach happens? Do service providers and their contractors have sufficient security protocols and insurance in place if a data-loss incident occurs? What are the reporting requirements if a breach occurs? "It's less about the technology and more about the legal agreement," Ayoub says.

Auditing MSPs requires more than simply ensuring that the vendor's staff is doing what it is supposed to do, says Ashley Podhradsky, an assistant professor of computing at Drexel University. Not only must companies ensure their MSP meets corporate security requirements, but that the MSP's contractors do so as well.

Finding protection

In a utopian world, IT staffs will have a full understanding of the supply chain of their company's vendors, ensuring that every subcontractor provides the same high-quality security protocols and procedures that the MSP employs. However, she says, that rarely is the case.

"Companies are outsourcing, but not all have the ability to follow up [on their suppliers]," she says. "It's challenging, but it needs to be a priority."

As companies begin to move their data to the cloud, the idea that security will be provided as a service is increasing. However, Drexel's Podhradsky says no one seems to know precisely how that security will be managed. "Should there be a requirement for security?" she asks. "Security should never be anything but expected." However, she adds, if data security joins the ranks of other regulations, such as those for the financial industry, it is possible data

79% of IT executive respondents said they are running some production apps in the cloud
– ScienceLogic/Gatepoint Research, July 2011

15 QUESTIONS: For cloud providers

You've made the decision to move at least some of your data to the cloud. OK, what's next? Here are 15 questions from Ashley Podhradsky, an assistant professor at Drexel University, that one needs to ask a potential service provider:

Reliability

- Do you have references available?
- Statistics?
- Where is your core physical location? Satellite locations?
- How many customers do you have? What percentage renews their contracts annually? What is your longest contract?

Availability

- What does the agreement with your provider say about services? Strive for 99.9 percent uptime.
- How transparent are your system issues? Do you post downtime? Do you compensate users for extended downtime?
- What is your disaster recovery policy? How frequently do you evaluate it?

Security

- What is your security policy? What technologies have you adopted?
- How do you authenticate users?
- What standards and policies are you required to abide by?
- What type of encryption do you use?

Privacy

- What is your organization's policy on privacy? Is it audited? Frequency?
- What type of data privacy laws govern the location of my data?
- Do you sell customer metadata?
- What happens when the customer deletes their data? How frequently is it deleted on the servers?
- What happens to customer data when they terminate their contact? Is the data deleted immediately?

security could become politicized. Who should regulate it, she asks. Who sets the standards?

Throughout this country today, Podhradsky says, individual states have the primary responsibility for setting security standards. As a result, data that moves from server to server, state to state, falls under a variety of regulations and jurisdictions.

One way to protect corporate data is to have shorter and more frequent audit cycles, she says. Annual audits likely will be insufficient.

Not only must the client be responsible for understanding the cloud provider's technological capabilities and enhancements, in some cases, it also must understand the provider's data flow through its own supply chain, says Logic20/20's Westby. Clients that reside in locales where local law restricts the movement of data across international boundaries, for example, need to ensure that their contracts with cloud providers specify these limitations, he says. For example, the European Union (EU) has strict privacy laws that limit the movement of certain types of data across international borders, even within the EU.

Although a client can ask a cloud vendor to provide them with information on the vendor's subcontractors – such as the physical locations of the storage companies that the provider uses for data storage – it might not be willing or able to provide that data. In some cases, Westby says, it becomes a matter of trust with the provider.

Major vendors generally have the size, expertise and wherewithal to meet regulatory needs, he says. Clients normally can be confident that they have the necessary technical certificates they need as well. Smaller providers, however, will require an audit by the potential customer to ensure that the provider's policies, procedures and capabilities meet their requirements, including the ability to ensure that data stays within the necessary international boundaries.

"There still is no standard way to evaluate [cloud] providers," Westby says. "There is no gold litmus test. Even among the major providers with SLAs, you will find that SLAs differ widely."

However, the CSA's Reavis points to recent activity to develop guidelines. His organization is working to bridge the gap between slow-moving standards bodies and the rapidly evolving cloud market economy, he says.

Meanwhile, the debate concerning conflicting laws in the EU and the United States about data security has become a "muddy subject," says Tegatai's Lundy. Today's global economy means that data storage facilities could be located anywhere in the world, but as noted, local laws can restrict where that data ultimately resides. However, laws such as the *U.S. Patriot Act* can put even locally stored data in the EU within reach of the American intelligence community.

The *Patriot Act* states that if a U.S.-based company is doing business overseas, it must follow the law. For example, if a company in Ireland is saving its data to Amazon cloud servers also located in Ireland, U.S. intelligence would, under the act, have the ability to access that data because Amazon is a U.S. company. The fact that the com-

“It's a Wild West out there now...”

– Jim Reavis, executive director, Cloud Security Alliance

pany is Irish and storing its data locally would not override the act. That is why, says Drexel's Podhradsky, companies always should encrypt their data before sending it to the cloud.

While encrypting data before sending it to the cloud goes a long way to protecting information, if a government agency wants to decrypt that data, chances are it will, warns Cedric Jeannot, founder of I Think Security, a data protection company based in Waterloo, Ontario, and co-author of two books on security. Though customers might contract with their cloud service provider for security services, Jeannot stresses the company that owns the data has primary responsibility for its security.

A topic that has gained traction in the industry is security as a service, he says. While service providers can layer on additional capabilities, such as hardware encryption on top of the software-encrypted data sent by the client, or file-splitting, a technique that chops encrypted data into smaller pieces

that are spread across multiple servers in the cloud, Jeannot recommends that users hire security experts. In this way, dedicated professionals can assist with the security aspect of moving data to the cloud and let the cloud providers focus on managing the data once it reaches them. He also recommends hiring a third-party firm to audit both the security and cloud providers, ensuring that everyone is doing what they said they would do.

One precaution Jeannot recommends is for companies to make sure that their service provider does *not* have decryption keys for any data. Sharing a key with a service provider effectively compromises all encrypted data and would make any standards-compliant data (such as payment card information) immediately non-compliant. This precaution is echoed by security experts that specialize in standards for the financial services and health care industries.

Further, CSA's Reavis cautions users about selecting a service provider for the cloud without performing sufficient due diligence. Working with an MSP is unlike nearly any other business relationship, he says, because when a company uses hosted applications, it is betting its business on availability guarantees. Customers who buy cloud storage without building in redundancy and resiliency are effectively swapping out a local disk drive for a drive on the cloud, he says.

In the future, he anticipates that cloud computing will be similar to today's public utilities, such as water and power. It eventually will be possible, he says, to depend on the utility to supply the service with a minimum of downtime. However, that is not the case today.

Selecting an MSP is not like hiring a contractor to build a house, he says.

If one has problems with a contractor, he can be fired and another brought in who will use the same basic tools as the first – nails, wood, plasterboard and paint. One need not worry that the drywall selected by one contractor will be incompatible with that selected by another. However, that is not always the case with cloud providers.

Some MSPs build their cloud using proprietary extensions and application programming interfaces (APIs.) While the basic plan might provide easy portability to another cloud provider, more sophisticated features could convert client data into something that is not portable, he says.

"It's a Wild West out there now," Reavis says. Companies that choose to move from one provider to another might be trading one IT benevolent overlord for a new one.

Despite all of the buzz about cloud computing as a new paradigm, Reavis acknowledges that today's cloud environment is not so different from the early 1960s when companies started to buy time on other companies' computers – a service known as time-sharing. While the cloud is distributed and the levels of control are significantly different, he says, companies can learn lessons from legacy technology.

In the mainframe days, users had terminals that connected to remote servers where applications were based and data was stored. While today's laptops and mobile devices are, generally speaking, more powerful than the mainframes of the past, the scenario where remote applications and storage servers are used is not so different, he says.

One of the hallmarks of the halcyon days of mainframes, however, was proprietary hardware and software, which limited a user's ability to move from one time-sharing vendor to another. This too, he says, is similar to today's environment where cloud vendors use proprietary applications that make it difficult to move from one cloud provider to another. ■



Photo by David Paul Morris/Bloomberg via Getty Images

SAFE

With cloud computing becoming popular for e-commerce, what are the security and privacy concerns moving forward, asks [Jim Romeo](#).

That warehouse of personal data and information, the desktop computer, is going the way of the dodo bird. All the essential bits and bytes once available right from the hard drive inside the computer will soon be migrating to servers far, far away in a mysterious realm known as the cloud.

According to research conducted by the Pew Research Center, by 2020 the majority of computer users will access software applications online, and share and access information by way of remote server networks. The survey predicts that cloud computing will trump the desktop and will use connections to servers operated by outside firms. For many of the survey respondents, this raises questions about the security of their data.

Combine this with the fact that the burgeoning payment card industry – with about 180 million credit card users and a fast-growing number of debit card users – has seen a slew of regulatory reform from Congress in the past two years. Additionally, an industry-wide movement of self-imposed standards has given retailers and commercial enterprises governance and best prac-

tice guidelines, such as those from the PCI Security Standards Council, which describes its Payment Card Industry-Data Security Standard (PCI-DSS), as providing “an actionable framework for developing a robust payment card data security process – including prevention, detection and appropriate reaction to security incidents.”

Users buy everything from a new car to a week’s groceries on their purchase card. But is PCI enough, given the coming proliferation of card activity by way of cloud computing?

“PCI-DSS standards are just one of many standards agencies that must be met for certain industry types,” says Wade Yeaman, founder and CEO of Texas-based Fluid Consulting. “A key component is to know the data center where your cloud is being provided. Data centers are classified in tiers for availability and failover, but also in their adherence to standards, such as SAS-70, PCI-DSS, ISO 9001, external audits and other industry specific standards.”

The data center should be willing and happy to provide this information, he says. A cloud provider should then be able to offer additional security prac-

tices. “The most important factor is to know your business and which standards apply to you,” Yeaman says. “With new laws and regulations being released on a regular basis, this becomes an ongoing endeavor.”

No silver bullet

There are no foolproof security mechanisms, and PCI compliance is not a solution, but simply a set of guidelines or best practices/checklists that one should follow, says Clifford Neuman, director of the University of Southern California Center for Computer Systems Security. So, he adds, even if PCI guidelines are followed, they do not guarantee that a system will remain secure.

“If we were dealing with simple machine-generated threats, the answer to this question might be different, but today’s threat environment is much more complex,” says Tim Keanini, chief technical officer for nCircle, a San Francisco-based network security and compliance auditing firm. Information security is a complex problem that is evolving rapidly, he adds. “Compa-



PASSAGE

nies are dealing with intelligent, persistent attackers using a wide variety of attack methods.”

Standards and compliance definitely help, Keanini says, but when one is faced with structured threats – similar to those that have been in the news lately – those guidelines are not enough to ensure the safety and security of sensitive data.

Where is my data?

Data stored in the cloud, such as purchasing card details and transaction history, is a new dimension within a technology management paradigm that ordinarily deals with client servers as conventional networks. Some aspects of cloud security pose different considerations than traditional network environments when trying to keep information safe and staying compliant with industry and regulatory mandates.

“Data stored on a cloud solution will mean that the data is constantly in the hands of a third party,” says Marcus Ranum, CSO of Maryland-based Tenable Network Security. That will add one more network that sensitive data resides on that has to be audited and secured, he says. The more networks data sits on, the better chance it has of falling into the wrong hands. Additionally, user authentication strength will vary between a cloud provider and the

base provider. If the cloud provider does not mandate a certain level of authentication that is higher than the original provider, one should drop them as a provider immediately, he says.

Within IT security ranks, cloud computing poses some trepidation that sensitive consumer and purchase data and information is outside of the control of a CIO or CSO. There has been much talk within the IT security industry around the notion that companies aren’t sure where their data is when using services from a cloud provider. So, what does that mean for compliance?

“The issue of data location and control is getting dramatically better, partially as a result of consistent push-back from customers on the cloud providers,” says Dean Ocampo, director of cloud and compliance solutions for Maryland-based SafeNet. Providers built their clouds around redundancy and pushing multiple copies of data around so they wouldn’t lose anything, he says. It was an afterthought to even think about where it might be going, he says.

However, cloud providers now have built-in geographical definitions in their management GUIs and are getting better about tagging data for geographical control. “It comes up consistently in their conversations with customers, and customers are forcing some of the cloud providers to limit geographical data dispersion in their contracts,” he says.

Many large-scale deployments have a management platform built on top,

capable of spanning multiple providers, according to Ocampo. Such platforms were primarily built to automate provisioning, handle compatibility across systems and integrate virtualization into organizational workflows. They also are increasingly being used as a data governance control mechanism.

“These platforms can define how the system controls data migration, and under what security policy,” he says. “True, these systems are in their infancy for providing security, but since organizations are building them anyway, why not build some controls for the data location issue?”

Brian Thomas, a partner in the advisory services department at Weaver, a Texas-based consultancy, explains that in the basic cloud storage scenario, the customer is purchasing the storage services from a provider and that it is up to this vendor to manage where that data is logically and physically stored. “So, if the [provider] has multiple facilities housing its servers, then the hosted data could be located in any of those facilities,” he says.

The reality is, the customer does have at least some control over this situation and needs to be actively involved with the provider in establishing requirements for cloud-based services, including compliance requirements. “The way that organizations get themselves in trouble with compliance and cloud-based services is by not addressing their compliance requirements up front,”

Thomas says. “Considering compliance requirements up front can alleviate the issue by allowing the organization to find a [provider] that meets all of their requirements, including those that are compliance related.”

Another concern is the malicious insider who lurks about while getting familiar with the intricacies of cloud computing. Eventually, these miscreants learn the landscape well enough to dodge any security measures and this, experts say, could be a growing problem.

“There are always rogue users who have intimate knowledge,” says Weaver’s Thomas. “The cloud computing industry in the United States alone probably consists of thousands of companies at this point employing hundreds of thousands of personnel, at least some of whom are bound to be disgruntled or have criminal backgrounds.”

**IN THE CLOUD:
PCI guidance**

The PCI Security Standards Council, an organization formed on behalf of the leading credit card brands and with a mission to thwart data leakage and stop payment cardholder data fraud, last June released “PCI DSS Virtualization Guidelines.”

The 39-page document provides guidance to those enterprises in the payment chain on the use of virtualization technology in relation to their compliance with the Payment Card Industry Data Security Standard (PCI DSS).

The guidance helps to update PCI DSS in the era of cloud computing, addressing such hot-button items as tokenization, chip-and-PIN and end-to-end encryption.

To respond to critics and advisers, the council developed special interest groups (SIGs) to clarify the use of virtualization technology. Compiled by Virtualization SIG Chair Kurt Roemer, chief security strategist at Citrix Systems, and more than 30 participating organizations of the council, the supplement aims to assist merchants,

“There are always rogue users who have intimate knowledge.”

—Brian Thomas, partner, Weaver

These people pose a significant threat in any computing environment, and cloud is no different, he says. The critical difference is not whether they can identify the flaws in the security model and work their way around them. “It is that if successful, the rogue user could adversely impact the operations of the [provider]’s customers, not just vendor itself,” Thomas says.

There will always be individuals that know how to dodge the security and stay ahead of preventative measures, but this may not be an insurmountable obstacle to the viability of cloud secu-

service providers, processors and vendors to understand how PCI DSS applies to virtual environments including:

Evaluating the risks of a virtualized environment;

Implementing additional physical access controls for host systems and securing access;

Isolating the security processes that could put the card data at risk; and **Identifying** which virtualized elements should be considered “in scope” for the purposes of PCI compliance.

“It is important to recognize that while the use of virtualization technology certainly offers many benefits to organizations, the complexity of virtual configurations can lead to accidental misconfiguration or entirely new vulnerabilities that the system’s designers never anticipated,” Bob Russo, general manager of the PCI Security Standards Council, told *SC Magazine*. “This resource helps merchants in better understanding some of these risks and how to minimize them when considering the use of virtualization in payment card environments.”

rity, says Chris Stephenson, partner and co-founder of ARRYVE, a Redmond, Wash.-based IT consultancy.

“This could be a problem for providers that are not serious about security and monitoring, but I think the major players will all be able to handle this just like credit card and ATM fraud,” says Stephenson.

Another challenge is the difficulty of prosecuting malicious users because of the often incongruous laws that exist from country to country. Many data breaches and compromises initiated by rogue users cross national boundaries, – computer networks in one jurisdiction may be penetrated from a computer from a foreign nation – making cooperation by law enforcement a bane of prosecution.

A manageable risk?

The takeaway, says ARRYVE’s Stephenson, is that cloud computing can be considered a significant technologic advancement in a society that now spends a good share of its time before a computer monitor. But with convenience, comes risk.

“I remember when e-commerce first came out, and many people were unwilling to enter credit card information into a website,” he says. “As the websites proved secure, users started entering credit card info and now many even save the information to the site.”

He sees the cloud evolving in a similar way. “There is a natural distrust of [the cloud], but the providers that survive will be those that prove they are secure enough to use.” ■

Jim Romeo is a freelance writer based in Chesapeake, Va. He focuses on business and technology topics.

CLOUD QUERY

A number of leading cloud experts explain how their companies provide secure and cost-efficient solutions to their customers.

Illena Armstrong and Dan Kaplan report.

In this special Q&A, *SC Magazine* gathers input from some of the leading cloud service providers to learn what they think are the most worrisome threats and how they are working with their customers to combat these as more organizations turn to the cloud.

The assembled experts include Jonathan Coombes, CSO at Rackspace, a specialist in the cloud computing industry; a spokesperson from Google, the corporation offering internet search, cloud computing and advertising technologies, who chose to remain anonymous; Norm Laudermilch, COO at Terremark Federal Group, a Verizon division which works with government agencies to provide managed infrastructure services; Latha Maripuri, director at IBM Security Services, which offers risk management solutions; and Stephen Schmidt, chief information security officer at Amazon Web Services (AWS), which has provided companies of all sizes with an infrastructure web services platform in the cloud since 2006.

What do you consider to be the greatest benefits of cloud computing for enterprises?
Latha Maripuri, director, IBM Security Services: The benefits of

cloud computing can be realized by IT and business users alike. Not only can organizations reduce the cost and complexity of delivering traditional IT services by utilizing the cloud, but organizations can leverage the cloud to create new service capabilities and new revenue streams by taking advantage of self-service capabilities and faster deployment models. While the business and IT users within an organization are drawn to the cloud for different reasons and with different goals, both roles are unified in their view of cloud’s overall value: the ability to deliver IT without boundaries, improve speed and dexterity, and create new business value.

Stephen Schmidt, CISO, Amazon Web Services (AWS): Enterprises are recognizing that cloud computing enables organizations to offload the heavy lifting of managing servers and

data centers. This means not only is the security of the physical infrastructure management passed on to the cloud provider, but also the security and the technology that enables virtualization across multiple operating systems.

What are the drawbacks?

LM: The change in service and IT delivery models associated with cloud computing can affect the basic way organizations perceive risk. Cloud computing represents a new delivery model. Control over operations and data at many layers can be shifted to the cloud provider requiring a delicate trust relationship between the provider and the subscriber.

SS: Most often

“Cloud computing offers a unique opportunity to get the best of many worlds...”

Norm Laudermilch, COO, Terremark Federal Group



the challenges are related to getting started – some businesses are unsure where to start or need help identifying which applications to put in the cloud. Smaller businesses are often all-in from the start because they are not dealing with legacy systems.

Norm Laudermilch, COO, Terremark Federal Group: The strong attraction to the benefits of cloud computing is exactly the root of the main drawback: You have to be very careful who you choose as your cloud provider. Anyone with a fast internet connection and a rack of home-built servers can become a cloud provider. Cloud consumers need to do their homework and select the vendors that use world-class data center facilities, the best connectivity in the business and world-class security teams.

From your perspective, what are the most severe cloud computing security threats?

LM: Cloud computing is subject to the same types of threats that traditional enterprise networks face – threats that impact the confidentiality, integrity and availability of data and information systems. According to the IBM X-Force Research and Development team, the most vulnerable attack vector for compromising both cloud and non-cloud environments is through vulnerable web applications, often the gateway into databases and servers that store sensitive data.

SS: At the core, the biggest security threat is the failure to understand the division of responsibilities between the provider and customer. The infrastructure provider should be an absolute expert at building large data

centers with redundant systems. This requires the provider to secure numerous data centers spread across the country, if not the world. The customer assumes responsibility and management of, but not limited to, the guest operating system (including updates and security patches), other associated application software, as well as the configuration of the AWS-provided security group firewall.

NL: The biggest security threat we face in cloud computing today is choosing a cloud provider that doesn't have their eye on the ball. We should all agree that most organizations do a terrible job with their internal security. The reason is that the economies of scale allow very few companies – even those in the Fortune 50 – to build, train and run a 24/7 security operations and analysis team that is world-class. A cloud provider that takes a world class security staff and focuses them on the cloud infrastructure 24 hours a day is going to do a better job of securing your information and workloads every time.

How is your company working to combat these threats?

LM: We advocate security by design. Each deployment option for cloud, whether public, private or hybrid, has a core set of foundational security controls in areas like identity and access management, governance, data protection, incident management and logical and physical infrastructure security that are consistent for that deployment model regardless of the purpose of that particular cloud. At the operational level we take advantage of skilled architects and security standards that have been tested through a long history of strategic outsourcing. At the infrastruc-

ture and platform level, our solutions leverage our portfolio of security products and services.

SS: AWS has developed a number of white papers, as well as a security and compliance center, to help customers understand the various elements, considerations and responsibilities related to security in the cloud. In addition, our support center provides customers free access to a resource center, service health dashboard, technical FAQs and developer forums.

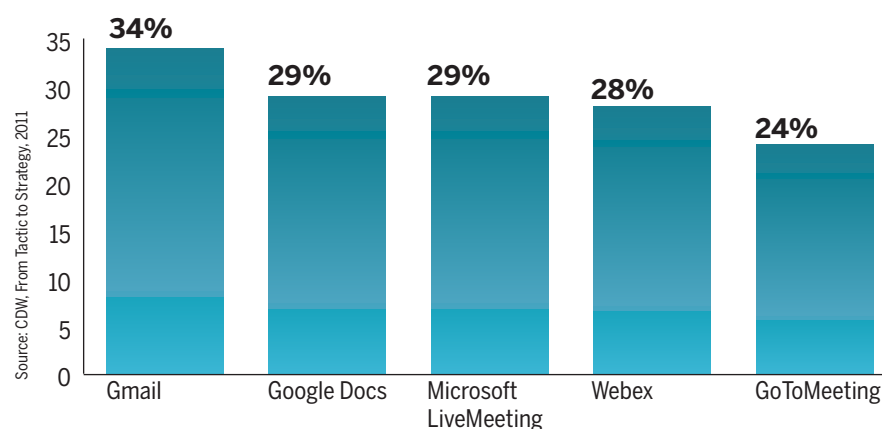
NL: Terremark combats these issues with a security team, tools such as memory forensics, full-packet capture, and correlation that yield better visualization of the environment, and the best quarantine, analysis, and response engineers in the business. We use all of this to do one thing: Watch our cloud computing infrastructure worldwide on a 24/7 basis and keep our customers safe.

How can customers ensure their security priorities are being met when using your services?

LM: This can be achieved through taking a risk-based approach. By understanding the risk profile associated with the workload you wish to migrate to the cloud, you can implement the appropriate security controls to address your priorities. This might be through contractual, procedures or technical controls in your environment or that of your provider.

SS: Examining the AWS cloud, you'll see that the same security isolations are employed as would be found in a traditional data center. These include physical data center security, separation of the network, isolation of the server hardware, and isolation of storage.

Which of the following tools does your organization currently employ?



NL: Because it's part of the core set of operational values we've based our service on. It's part of the way our service is defined, and it's the way our operations employees think while doing their jobs. Security has to be part of a culture to be effective, and at Terremark we've ensured that it's a key component of ours. We also monitor and report on our performance on a regular basis, allowing full transparency to the customer and eliminating doubts that arise due to lack of information.

JC: First, fanatical support is one of our core values. Customers can reach our support teams, by phone or email or chat, 24/7, 365 days a year, and those teams will ensure that their needs are met. Second, we maintain a dedicated customer security advocacy team focused exclusively on representing our customers' security priorities throughout the product-development process. Finally, we recognize that the cloud is not a one-size-fits-all solution, and through our hybrid model, we enable customers to move some workloads to the cloud while keeping others in a dedicated hosting environment.

Google: We protect the data of Apps users in three ways: people, process and technology. We employ some of the top security experts in the world. Access to

data is limited only to those who need access, and people receive the minimal access they need to do their jobs. This includes the physical protection of our data centers, safeguards we put in place to prevent network attacks, and the application environment in which we build software. Note that Google Apps is SSAE 16 audited and FISMA certified.

Whose responsibility is it to secure resources stored in the cloud – yours or your customers?

LM: The responsibility for security in relation to cloud computing is shared amongst the provider and the subscriber, although the weight of responsibility varies depending on the type of cloud deployment model. For instance, in the case of software-as-a-service solutions, security controls are largely the responsibility of the provider because of how the solution is packaged and consumed. Conversely, in an infrastructure as a service deployment model, the user is exposed to a greater responsibility for security regarding the protection of their virtual images, networking and storage. Ultimately, customers should have contractual, procedural, and technical controls and assurances that their data is secure – be it with the provider, or as part of their own augmented security program.

JC: This is very much a shared responsibility, and the actual split depends on the cloud service model and, by extension, how much of the cloud infrastructure is under the customer's control. In our infrastructure-as-a-service product, we are responsible for security up through the virtualization layer. Customers have full control of individual virtual machines, and with this control comes the responsibility for securing whatever runs within them. As you move up the cloud service stack to platform- and software-as-a-service models, customers have less control over individual system components and cloud providers necessarily assume a greater share of the responsibility for security.

What sorts of security requirements must you fulfill in SLAs signed with customers?

LM: IBM provides an approach based on its security framework and supported by foundational controls. We work with customers to explain our approach and ensure their requirements are understood. The benefit of working with IBM is we have many different delivery options so we can find the right solutions to fit the customer needs.

SS: We believe, and our customers have told us, that validating the security of cloud services happens through certifications and accreditations, as well as third-party evaluations of security and operational controls. AWS has achieved ISO 27001 certification and has successfully completed multiple SAS 70 Type II audits. We will continue to obtain the appropriate security certifications and conduct audits to demonstrate the security of our infrastructure and services.

Google: We have an SLA for our Google Apps for Business customers that guarantees that our Google Apps service will be operational and available at least 99.9 percent of the time during a calendar month. ■

A more extensive version of this Q&A will be posted on our website.



“Smaller businesses are often all-in from the start...”

Stephen Schmidt, CISO, Amazon Web Services

AHEAD IN THE CLOUD

IlliniCloud provides the technology backbone that helps several school districts in Illinois manage critical IT functions, reports

Greg Masters.

The economic downturn is having a tremendous impact on schools around the nation, as administrators desperately try to maintain their current programs, retain teaching positions and meet aggressive state and national performance benchmarks – all with shrinking budgets.

In addition, the cost of maintaining aging onsite IT infrastructure is a tremendous expense for school districts. IT professionals are challenged to find ways to delay or reduce spending, while

still meeting the needs and growing technology expectations of students, parents and teachers.

One apparent success story is taking place at Bloomington Public Schools District 87 in Bloomington, Ill., where IlliniCloud, a nonprofit consortium of school districts, banded together to streamline functions with the idea of sharing hardware and software resources among Prairie State school systems, all while saving on IT costs. The implementation began in 2009 and now serves more than 150 districts with three primary data centers throughout the state in Bloomington, Belleville and DeKalb.

IlliniCloud was created to provide K-12 school districts with affordable access to virtual servers, online storage and high-speed network connectivity across the state. When the plan began more than 10 years ago, the technology was limited. But, thanks to developments in virtualization software and cloud computing, resources that were

once only available to large organizations are now available to everyone, from rural school districts to Fortune 500 companies.

“We are able to do this through cloud computing, because as long as you have an internet connection, you have anywhere/anytime access to your data,” says Jason Radford, systems administrator for IlliniCloud and Bloomington public schools. “Without the consortium, many school districts would not have access to these technologies.”

Flexibility

IlliniCloud offers three IT services to school districts – disaster recovery (DR), infrastructure-as-a-service (IaaS) and software-as-a-service (SaaS). Most importantly, IlliniCloud is a community cloud and so is able to be flexible to its members depending on their needs, says Radford.

“By sharing data center resources, districts can spend fewer hours in the



Photo courtesy of IlliniCloud

IlliniCloud, a nonprofit consortium of school districts in Illinois, currently provides cloud services to 150 school districts in the Prairie State, with hopes to expand to several hundred more.

data center and focus more on advancing their core mission: to refocus technology resources into the classroom for the direct benefit of the students,” he says.

IlliniCloud hopes to expand to include 400 member school districts – and offer more advanced enterprise applications – within the next three years.

As a consortium of school districts, IlliniCloud’s leadership and IT support comes from its members, including a board of 17 appointed and elected representatives. The consortium also receives consultation from its technology solutions provider CDW.

As a co-op, IlliniCloud’s services and solutions are driven by the members’ needs, says Radford. CDW’s sales and solution architects worked closely with IlliniCloud, providing onsite consultation and services to help the consortium validate and expand its plans to establish a community cloud, as well as implement the solutions necessary to meet the needs of the state’s school

districts, says John Pellettiere, director K-12 education at CDW.

“Whether it’s a small school district, or a large corporation, we all need IT to accomplish the same core tasks,” says IlliniCloud’s Radford. “What is different is that IlliniCloud was created for K-12, by K-12, and as a result, we cater to the specific needs of education, which is why we are focused on disaster recovery, IaaS and SaaS. The community cloud model lets us provide the services our members demand, while also allowing us to expand our offering as needed.”

For its disaster recovery needs, for example, IlliniCloud delivers security measures that are often better than districts’ current capabilities, he says. IlliniCloud members are able to secure their assets, including curriculum, student information, financial data and library systems.

To keep information secure, IlliniCloud uses data leakage prevention

software, which can identify personal or financial information, such as Social Security numbers or birth dates, and strip the data out before it has the chance to leave the network.

Added value

Additionally, network virtualization tools keep members’ data separated in a multitenant data center, while several data encryption options provide another layer of protection – defense abilities that most districts have yet to implement, says Radford.

The implementation of the CDW solution for IlliniCloud went smoothly, says Radford. “We planned and implemented the infrastructure and quickly resolved issues when they arose.”

Cloud computing, especially the pay-as-you-go model that IlliniCloud uses, helps districts better manage their IT budgets, he says. IlliniCloud offers districts the flexibility to increase or decrease computing resources as their IT requirements change.

“Schools have always worried about maintaining control and ownership of their data,” says Radford. “As a co-op, rather than a third party or a company, members are comfortable knowing where their data is stored and knowing that they have control of it.”

An internal security group, called IllinoisSAINT (Security Advisory and Incident Network Team), conducts monthly audits as well as a vulnerability assessment of cloud servers to continuously assess new threats. Additionally, CDW performs an annual external audit as part of IlliniCloud membership benefits, Radford says. Meanwhile, updates are managed by the IlliniCloud IT staff.

“IlliniCloud is a proven case study for the ‘community cloud,’ which can be modeled by any organization in which users have the same technology requirements,” says CDW’s Pellettiere. “This means that the IlliniCloud can be replicated in any state and across most common user settings.” ■

REMOTE OPTIONS

Can cloud providers be trusted with your most sensitive data?

Deb Radcliff finds out.

Aspate of recent high-profile outages and intrusions into cloud networks demonstrates the real risk of using these services for critical operations.

In April, a problem in Amazon's data center caused outages for its Web Services customers. Also that month, Epsilon, the world's largest "permission-based" email marketing provider, announced that the address lists belonging to its customers had been exposed through a successful hack of its systems. And the highly advanced breach into security company RSA announced in March led to the compromise of information about its SecurID products, which include hardware token authenticators, software authenticators, authentication agents and appliances supported over the web.

All these cases impacted the customers who used web services to run their business or support network operations. The RSA breach potentially blew the security out of millions of multifactor authentication applications. The Epsilon case ultimately eroded customer trust in email they received from Citi, Chase and numerous other affected retail and financial outlets. And the Amazon outage highlighted how a physical data center problem can impact multiple web

services customers hosted there (including, in this case, HootSuite, Reddit, Foursquare and others).

Before these events, technology research firm IDC predicted that public and private clouds would drive 15 percent of IT spending in 2011, while Gartner forecasted that cloud computing would grow to become nearly a \$150 billion market in 2014. However, these recent cases have experts questioning more than ever the ability of cloud providers to protect their data.

"If you put your critical data in public clouds and anything happens in the cloud—whether an attack from outside or system failure or any type of disaster—you no longer have control of that data," says Joe Wulffenstein, department chair at Northwood University in Midland, Mich. "That's what I think is the biggest threat to cloud computing."

Creating a standard model

Despite the latest setbacks for some highly public cloud providers,

Jim Cavaliere, chief trust officer of Salesforce.com, contends that cloud providers are maturing into what he believes will be bellwethers of security and compliance.

For example, he points to the guidelines for public clouds put out by the National Institute of Standards (NIST). They tout several security benefits that public clouds can provide, including having specialized staff that agencies can't usually afford on their own, and providing and maintaining stronger

platforms, better availability of resources, more robust backup and recovery, and more.

The Force.com platform from Salesforce.com encourages organizations to build auditable processes, which enable faster spin-up of more reliable, trustworthy clouds for organizations putting together their applications. Cavaliere explains how using standardized applications properly managed by the cloud provider can give better overall security for all customers of that vendor.

"When running a single copy of the application for multiple tenants, any single security update is immediately in place for all customers in the multi-tenancy," he says. "Security is democratized – all security features and fixes are available to all customers and users when they are implemented."

Instead of enterprises trying to get this right on their own by building their own clouds and porting them to a provider, Cavaliere predicts that new applications will be easier to create in this well-run cloud, where all these services are offered.

Others concur. "This is where the cloud model presents its strengths," says Chris Stark, founding CEO of Vienna, Va.-based Cetrom, a cloud provider. "Partner with a provider and let them worry about the configuration, compliance and security problems. Access and security requirements should be plug and play."

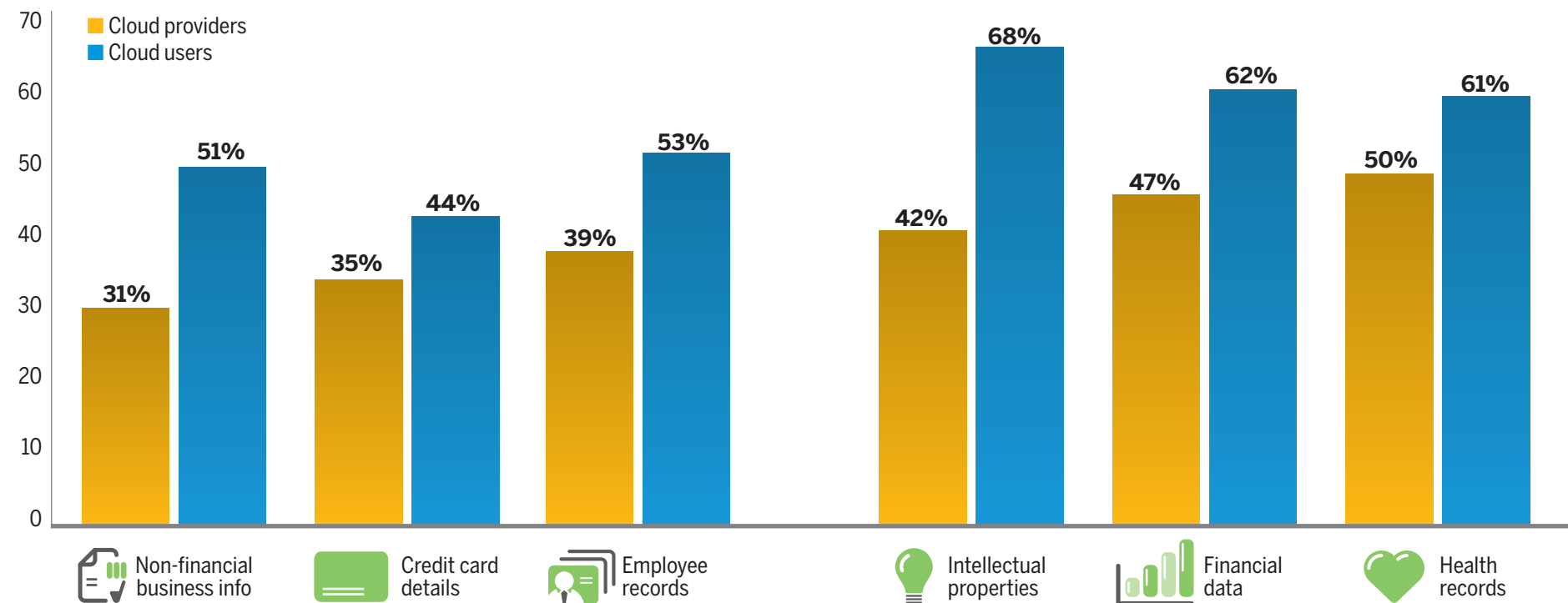
Cetrom has standardized about 150 commonly used customer relationship management (CRM), accounting, office, database and other applications commonly used in today's enterprises.

New security layers required

Cloud.com is another example of a web-based software and IT company that offers cloud builds with security policies and control options that buyers can choose as part of their configurations.

"As customers build their applications, we build in security policies around user access, application controls and data isolation," says Peder Ulander, chief product officer at the Cupertino,

Types of information too risky for the cloud



Source: Ponemon Institute research report, April 2011

Cloud providers

Calif.-based company. “What we can’t do is help with multicloud access. So far, however, not many of our customers are using multiple clouds at this time.”

When moving to public clouds, most organizations will need to layer on additional cross-platform access control management capability that preferably integrates with existing dashboards and user directories, such as Active Directory or LDAP (lightweight directory access protocol). The setup will also need to support federated identity models. Like other leading cloud vendors, Salesforce.com provides these access management options for its applications.

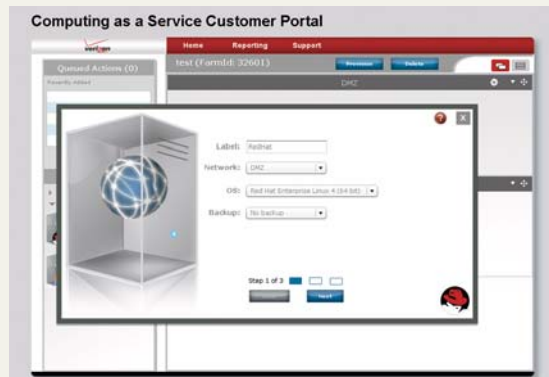
Contracting out

To support multicloud and internal authentication management that goes beyond its boundaries, Cloud.com refers customers to management platforms RightScale or enStratus, the latter of which supports 17 separate public and private clouds through management and scaling.

TO CLOUD: Or not to cloud

When developing cloud strategies, decide first what data will be interacting in the cloud and whether it should even be out there, experts say. Also, consider the connection. For example, rather than take the chance going over the web to their applications and infrastructures, Verizon’s most risk-adverse users are asking for access into their cloud applications over dedicated connections, says Michael Clark, the company’s cloud computing security strategist.

Verizon provides several types of services, its most popular being Verizon Computing as a Service (CaaS) Enterprise (above), an infrastructure-as-a-service offering launched in June 2009.



“You...have no idea what’s going on...[with your provider]...”

—Peter Schlampp, VP for Solera Networks

Fortunately, there is no shortage of federated-type unified access vendors that also can integrate with consumers’ existing identity infrastructures to manage them together with access to cloud applications. Along with the vendors mentioned here, companies like Symplified, Ping Identity, ActivIdentity, SecureAuth and Accenture showed up en masse at the RSA Conference in San Francisco in February.

The other cloud issue, the one of visibility, is a little harder to manage, many say. Mature providers offer customers dashboards to see into their own systems. These dashboards also can be made to hook into portals management dashboards if desired. What they can’t do is show the organization that the cloud vendor itself is compliant, reliable

The bottom line, say experts, is not to stampede to the cloud just because it is the new trend in technology. “I tell people at this stage of cloud computing, ‘If it ain’t broke, don’t cloud it,’” says Michael Cote, founding senior analyst with RedMonk, a cloud analyst firm based in Austin, Texas. “Cloud your new applications or some part of IT that’s problematic. Then build those from the ground up, securely.” — DR

and secure enough to prevent breaches and outages, such as what occurred at Amazon, Epsilon and RSA.

“The number one issue IT security professionals have with the public cloud is they can’t see into it,” says Peter Schlampp, VP of product management for South Jordan, Utah-based Solera Networks, a vendor of network forensic tools and services. “You literally have no idea what’s going on between the hosts running within the cloud or with the provider at large, so threats are beginning to take advantage of that.”

Inspect the provider

So, experts say, use diligence vetting the provider. Look for vendors with evidence of strong information security practices — such as ISO 27001 and Sys-Trust certification, regular SAS 70 Type II reports, and others — which leading providers, including Verizon (see sidebar, left), offer annually to customers.

An example of controls to audit would be those presented by Salesforce.com’s Cavalieri during a cloud summit at the RSA Conference. He discussed the main risk management pillars embedded in the company’s internal culture, including physical, network, application, access and mobile security policies.

Another consideration is that security responsibilities vary across different cloud computing models, says Carson Sweet, CEO of CloudPassage, a San Francisco-based software-as-a-service (SaaS) provider.

“Customers move to the cloud for flexibility and control,” he says. “Just remember that with more flexibility comes more responsibility for security.” ■

This article originally appeared in the June issue of SC Magazine.

SSLL
WPAW
BFFF

Let’s face the facts. You’ve been so dedicated all year. Now it’s time to get the recognition you deserve.

Make sure you check out our two NEW categories:
Best Cloud Computing Security & Best Fraud Prevention Solution

SC AWARDS
MAGAZINE 2012
Honored in the U.S.

Final deadline: Sept. 2, 2011

Nominate your products, team members and company today and come Feb. 2012 you could be taking home the most coveted trophy in information security.

Save the date: Tuesday, Feb. 28, 2012

2012 SC Awards U.S. Dinner and Presentation

Visit scmagazineus.com/awards to download your entry kit today.

Sponsors

websense[®]

ESSENTIAL INFORMATION PROTECTION™

Websense, a global leader in unified web, data and email content security solutions, delivers the best security for modern threats at the lowest total cost of ownership to tens of thousands of enterprises, mid-market and small organizations around the world. Distributed through a global network of channel partners and delivered as software, appliance and software-as-a service (SaaS), Websense content security solutions help organizations leverage new communication, collaboration and Web 2.0 business tools while protecting from advanced persistent threats, preventing the loss of confidential information and enforcing internet use and security policies. Websense is headquartered in San Diego, Calif., with offices around the world.

For more information, visit www.websense.com.