Think your data will be safe in the cloud? Here are six tough questions to ask your provider.

**Also inside:** Securing the Cloud Daisy Chain | Cloud SWAT Teams
The Cloud Security Checklist

6  Do you think your data will be safe in the cloud? Here are six tough questions to ask your cloud service provider.

Securing the Daisy Chain

12  Contracts aren’t fail-safe. Make sure your data is secure as it travels among cloud providers and their subcontractors.

Cloud SWAT Teams

16  A new breed of specialized incident-response teams aim to make the cloud more trustworthy.

HEADS UP | 4  A startup tackles cloud security. | Editor’s note:
This digital issue of Computerworld features exclusive content that examines what many consider to be cloud computing’s biggest pitfall: security.

OPINION | 20  Thomas J. Trappler advises you to vet cloud providers to make sure they have adequate physical security safeguards.
“THE WISE MAN SOLVES 1,000 PROBLEMS WITH A SINGLE SOLUTION.”

Switch to single-platform Simpana® software for truly modern data and information management.

Year after year, some companies stick with legacy data protection software not designed to handle today’s IT realities. The result? Business at risk, frustrated users, out-of-control costs, and compromised business agility. In a word, insanity.

With its revolutionary single-platform architecture, Simpana software enables you to solve these problems right now and far into the future. It will lower operational, labor, and infrastructure costs, streamline integration of new technologies like virtualization and cloud computing, and smooth adaptation to challenges like data center consolidation and eDiscovery requirements.

The result? Up to 50% reduction in storage-related costs, and a far simpler, saner way to manage, access, and recover business information. In a word, oneness.

To learn how you can do far more with less and add real value to your end users and your business with Simpana software, visit AchieveOneness.com or call 888-311-0365.
Is Security The Cloud’s Achilles’ Heel?

Computerworld’s fourth Digital Spotlight examines what many consider to be cloud computing’s biggest pitfall: security. Security regularly tops IT managers’ lists of concerns about the cloud. Yet some experts say data is more secure in the cloud than it is in typical corporate data centers.

The report, produced by Computerworld’s editorial staff, cuts through the concerns about cloud security and offers useful strategies. “The Cloud Security Checklist” (page 6) identifies six security and compliance capabilities your cloud provider must have, and it spells out tough questions you should be asking.

And remember: Some cloud service providers outsource some of their services to subcontractors, making it difficult to know where your data is and how secure it is. “Securing the Daisy Chain” (page 12) explains how to ensure that those players are protecting your information.

In “Cloud SWAT Teams” (page 16), you’ll learn how cloud-specific security incident-response teams could help governments and enterprises deal with malicious activity.

Watch for the fifth Digital Spotlight, planned for November, as well as several more next year.

Scot Finnie is Computerworld’s editor in chief. You can contact him at sfinnie@computerworld.com and follow him on Twitter (@scotfinnie).

Bromium Takes Aim at Cloud Security

SIMON CROSBY, the former CTO of Citrix Systems’ data center and cloud business, has formed a startup called Bromium that will aim to solve security problems in a cloud environment.

Bromium’s plan is to use a hypervisor to provide servers and clients continuous protection from malware.

Enterprises are worried about the security of cloud computing, but the threat doesn’t lie in the cloud, said Crosby. Most attacks on enterprises’ private clouds “happen through unprotected clients,” he said. “It’s you putting your private stuff and your work stuff on a relatively insecure client device.”

The fact that cloud-based resources can be accessed from any location, through a variety of devices, means users need a new approach to security, said Crosby.

Locking down PCs hurts the user experience, and using virtual desktops provides greater security but still leaves enterprises vulnerable to harmful elements such as e-mail attachments, Crosby said.

Bromium’s technology will secure application clouds and virtual desktops as well as rich client devices. It will run on multiple processor platforms, including x86 and ARM, and be optimized for mobile devices.

Other cloud security vendors include CloudPassage, SecureAuth, StillSecure and Symplified, among others.

Bromium, based in Cupertino, Calif., and Cambridge, England, plans to introduce a product in the second half of this year.

– Stephen Lawson, IDG News Service

TECH STARTUP

Bromium Takes Aim at Cloud Security

S

imo Crosby, the former CTO of Citrix Systems’ data center and cloud business, has formed a startup called Bromium that will aim to solve security problems in a cloud environment.

Bromium’s plan is to use a hypervisor to provide servers and clients continuous protection from malware.

Enterprises are worried about the security of cloud computing, but the threat doesn’t lie in the cloud, said Crosby. Most attacks on enterprises’ private clouds “happen through unprotected clients,” he said. “It’s you putting your private stuff and your work stuff on a relatively insecure client device.”

The fact that cloud-based resources can be accessed from any location, through a variety of devices, means users need a new approach to security, said Crosby.

Locking down PCs hurts the user experience, and using virtual desktops provides greater security but still leaves enterprises vulnerable to harmful elements such as e-mail attachments, Crosby said.

Bromium’s technology will secure application clouds and virtual desktops as well as rich client devices. It will run on multiple processor platforms, including x86 and ARM, and be optimized for mobile devices.

Other cloud security vendors include CloudPassage, SecureAuth, StillSecure and Symplified, among others.

Bromium, based in Cupertino, Calif., and Cambridge, England, plans to introduce a product in the second half of this year.

– Stephen Lawson, IDG News Service

– Stephen Lawson, IDG News Service
Every day, malware attacks, evolves and attacks again. It has to—because we keep stopping it. Blue Coat Web Security Solutions are powered by WebPulse™, a community of over 75 million users. That’s 75 million strong taking a stand to shut down over 3.3 million threats a day. Proof, there’s safety in numbers.

Learn how Blue Coat Web Security Solutions with WebPulse can keep your gateway secure @ bluecoat.com/WebPulse
Whether you’re a small business relying on Google Docs for document sharing or an enterprise moving your global ERP system to the cloud, you should demand that some common security and compliance requirements are met by vendors providing applications and services over the Web. These requirements involve who can access your applications and data, as well as the systems hosting them; where the data is stored; and whether the data is hosted on dedicated, rather than on shared, hardware. They also ensure that you get detailed logs of who has accessed your data and applications so that you meet corporate and regulatory standards, and they verify that data is properly encrypted — a factor that’s more critical outside the corporate firewall.

Think your data will be safe in the cloud? Here are six tough questions for your cloud service provider. **BY ROBERT L. SCHEIER**
What you demand of the cloud depends on your corporate standards and your compliance needs, the amount and type of workloads you’re moving to it, and how you are dividing administrative and security responsibility between your staff and your provider. Security requirements also vary depending on whether you’re using software as a service (SaaS), infrastructure as a service (IaaS) or platform as a service (PaaS) offerings. But you should at least consider each of the following questions in your cloud security plans.

### 1. WHO HAS AUTHENTICATION/ACCESS CONTROL?

The ability to prove that users are who they say they are and control the data they can see and the functions they can perform, based on their identities and roles, is the top priority of almost every cloud user interviewed for this story. Authentication can be the most challenging when you maintain user information and controls within the firewall using a repository such as Active Directory but host your servers and applications in the cloud.

The ideal is a “federated” identity management access system that pools authentication information from all of your organization’s systems — internal and external. This allows instant authentication of any user who presents the proper credentials, such as a password or a password and a token. It also provides for single sign-on, allowing users to access all of their applications and data, in-house and in the cloud, with a single username and password. While top SaaS providers have the infrastructure to provide single sign-on to large customers that are themselves equipped to serve as “identity providers,” many smaller service providers and their customers lack those capabilities, says Eve Maler, an analyst at Forrester Research.

However, because federated identity management can be expensive and cumbersome to implement, many organizations settle for a “synchronized” approach in which different copies of a user’s authentication information are maintained by different applications, says Maler. This can compromise security by spreading user credential data among multiple locations and companies. It can also create delays between the time that an employee’s access is withdrawn from internal systems and from a cloud-based application, creating a potential security gap.

Another authentication option is for the cloud provider to connect directly to the company’s store of user information, which Maler says “is probably safer than synchronizing” but practical only if you have a relatively simple collection of systems. That’s the route taken by healthcare provider HCR ManorCare. Thomas Vines, director of information security at HCR, says he has used a cloud-based application to host the company’s electronic medical record system.

### 2. IS THE LOCATION SECURE?

The cloud allows data to be moved to the most cost-effective location without users’ knowledge. But to safeguard security, customers should know the location of their data. Gary Landau, vice president of IT infrastructure and information security at financial services provider Wilshire Associates, wants cloud vendors to provide replication to redundant sites, “but I also want to know where that [data] is going to be, because I don’t want my data being migrated” to a country that lacks strong legal protection for it.

Cloud customers whose concern is document security can use SaaS tools like WatchDox, which lets them control who can view cloud-based documents and track who accessed them. According to Kevin Gholston, vice president of business development at defense manufacturing consultancy CVG Strategy, WatchDox is easier to use and less cumbersome than digital rights management software.

AMAG Pharmaceuticals relies on cloud providers to host all 24 of its sensitive applications and just under 8TB of data, including information related to manufacturing processes and quality control, says Nathan McBride, AMAG’s executive director for IT. He uses CloudLock for Google Apps from CloudLock (formerly Aprigo) to restrict document access to authorized users and to transfer ownership of documents to another employee when a user leaves the company. This eliminates the manual process of finding each document and changing who can access it.

### 3. WHEN ARE AUDITS CONDUCTED?

Proving your applications and data meet corporate, industry and government standards requires audits and reports. Vines does a quarterly audit of each of HCR’s critical application providers, covering everything from software updates to the validity of users’ accounts and the controls required for HIPAA and Sarbanes-Oxley compliance. He says years of experience and “hand-in-hand” cooperation between the audit and security groups means audits require only a quarter of one staffer’s time. “Once we get into the flow, it’s well documented and not so ad hoc,” he says, noting that scripts and processes his team developed proactively highlight problems.

Each cloud vendor that AMAG’s McBride uses must meet strict

Continued on page 10
Building Trust Around The Globe

When you want to establish trusted relationships with anyone, anywhere on the internet, turn to Thawte.

Securing Web sites around the globe with:

- strong SSL encryption
- expansive browser support
- multi-lingual customer support
- recognized trust seal in 18 languages

Offering outstanding value, Thawte is for those who know technology. Secure your site today with a Thawte SSL Certificate.

www.thawte.com
FDA data security requirements, one of which calls for a multiday on-site audit by AMAG of the vendor’s facility and processes.

While SAS 70 compliance is frequently cited as an assurance of security, it only lists the controls the provider has in place, not how it enforces those controls, says Karthik Chakkarapani, IT director of technology solutions and operations at the American Hospital Association, which hosts everything from CRM systems to payroll to data for mobile applications in the cloud. Jason Lau, director of IT security at Service Now, an SaaS IT management vendor, suggests ISO 27001 as a more rigorous alternative.

Marlin Pohlman, chief governance officer of storage vendor EMC and chairman of the strategy board for the Cloud Security Alliance (CSA), suggests using SOC 2 and the Statement on Standards for Attestation Engagements (SSAE) No. 16 instead of SAS 70. The CSA also has put forth a set of security principles in its Cloud Controls Matrix and, in the fourth quarter, expects to give users access to security questionnaires completed by cloud vendors for its Security, Trust and Assurance Registry (STAR). This will give users a format for comparing the security practices that providers claim to follow, says Jay Chaudhry, CEO of Zscaler and a co-founder of the CSA.

In any case, Chakkarapani advises, ask detailed questions about which systems store which data, how the data is stored and encrypted, and the exact paths by which it is read and written. Also, he says, find out which administrators can access your systems and how their access is controlled.

While the single sign-on capability eliminates the confusion of multiple usernames and passwords, it can also provide more complete audits by capturing all of a user’s actions regardless of which systems they logged in to and the credentials they used, according to NetIQ’s Cecere.

Vendors such as Core Security Technologies and nCircle allow users to conduct vulnerability scans. Many companies want to do the same scans they do internally and see the same reports on cloud providers that they see for their own organizations, says Tim Keanini, chief technology officer at nCircle. But some argue that by mimicking attacks, the tests themselves can interrupt a provider’s service. Others say the scans are incomplete and inaccurate or, as McBride says, “one sure way to put a dent into the relationship” with a provider. Pohlman recommends the Security Content Automation Protocol, developed by the National Institute of Standards and Technology, as a less intrusive way to assess a provider.

Encryption is central to Herrin’s plan for “getting out of the data center and hardware business” by hosting applications on servers owned by a cloud provider but managed by his staff. He uses hardened appliances from Voltage Security to encrypt portions of customers’ credit card numbers from the time they are swiped at the merchant through to their processing. The approach allows him to reap the cost savings of the cloud without worrying about whether every step is compliant with Payment Card Industry standards for protecting customers’ credit card numbers.

Because the full credit card numbers are unreadable, he says, the processes aren’t subject to PCI requirements.

Larry Whiteside Jr., director of information security and chief information security officer at the Visiting Nurse Service of New York, insists on 1,024-bit encryption for data moving between users and cloud applications, as well as for the associated encryption certificates. Encryption for data at rest is desirable but not mandatory for his organization, assuming other security controls are in place, such as data obfuscation and the use of separate SQL instances or even physical machines.

One way to avoid unpleasant surprises is to make sure your IaaS provider quotes prices for servers and storage fast enough to handle the required level of encryption without slowing applications. Pohlman suggests consulting the FIPS (Federal Information Processing Standards) 140-3 guidelines to determine the level of encryption required for each organization and jurisdiction. You should also make sure that a provider’s disaster recovery plan protects not only the encrypted data, but the decryption keys necessary to use the data, Vines advises.

Once all precautions have been taken, the key to security is people. Some users feel cloud vendors can do a better job of keeping data secure than they could themselves, since vendors have more money — and more at stake.

Rather than trust someone on his own staff “who might be doing 15 different things” in addition to security, McBride says he’s more confident relying on a cloud vendor “whose very job depends on” keeping clients’ data secure.

“You know they’re going to get it done,” he says. •

Schier is a veteran technology writer. He can be reached at bob@scheierassociates.com.
IS YOUR SECURITY FORECAST CLOUDY?

HP Enterprise Security provides hybrid controls to provide comprehensive, integrated protection for your infrastructure, applications and networks, whether local, virtual or in a cloud.

For more information go to www.hpenterprisecurity.com.
Contracts aren’t fail-safe. Here’s how to guard your data as it travels among cloud providers and their subcontractors. By Stacy Collett
IT’S 2 P.M.
Do you know where your cloud data is? Really?
Executives at one large Fortune 500 company thought they knew, but a routine audit of the cloud provider uncovered a serious problem.
“The cloud provider that we thought we had became merely a shell, and it outsourced the provision of the service to an offshore company that no one had even heard of and that the company would never have provided data to,” recalls Brad Peterson, counsel for the company and a partner in the Chicago office of Mayer Brown LLC.

Fortunately, the problem was discovered and there was no harm done, but there might have been serious consequences if it hadn’t been addressed.
“We deal with companies with hundreds of thousands of customers. If a data breach can cost $400 to $500 per customer record and you lose 100,000 records, you’ve got a huge exposure,” says Peterson.
With some cloud computing providers outsourcing underlying parts of their services to subcontractors, who may in turn outsource to others, do you really know who has your company’s data or how secure it is? Industry insiders offer advice on how to ensure that every company in that daisy chain is protecting your information.
OUTSOURCING

Security Haves and Have Nots

Major cloud computing providers, such as Google, Salesforce.com, Amazon and Microsoft, know the data security requirements of large enterprises and are happy to oblige.

“Most of the larger cloud service providers have gotten SAS 70 audits and ISO 27001 [security] audits in response to large businesses” that require it, says John Pescatore, an analyst at Gartner.

Google and others have even established dedicated U.S.-based data centers for government customers in order to comply with federal mandates that require government data to be stored domestically. The move helped Google win a contract to provide hosted email service to the U.S. General Services Administration in December; it was the first agency-wide federal cloud email deployment.

Still, security and compliance concerns are the top two inhibitors to the use of cloud-based services, according to a 2010 Gartner study. Some 42% of the survey respondents cited security, privacy and compliance as major concerns, though that’s down from 49% in 2009, Pescatore says.

Sophisticated providers of software as a service (SaaS) have clauses dealing with data security in their contracts, Peterson says. “They understand customers’ needs and provide hybrid offerings to address security concerns better than you might be able to address them internally,” he says.

Contracts will usually give clients the opportunity to do the due diligence and spell out where data can be transferred and stored. Providers will give customers the right to approve subcontractors that will have access to their data and describe how they will respond to security incidents. They will also agree to give the customer the right to sign off on any changes before they are implemented, whereas a utility service provider may make changes and inform the customer afterward.

Cloud service providers will also have procedures for properly destroying data at the end of a contract. They will accept meaningful liability for their own breaches, and they may have published information security standards that they are required to follow. Finally, the provider will give the customer audit rights “so they can verify that the provider is keeping its promises about your data,” Peterson adds.

That’s the best-case scenario. But what happens when a department within your company seeks cloud services on its own?

“There’s a tremendous amount of cloud outsourcing going on in major corporations where departments buy a cloud service over the Internet using a procurement card,” perhaps to test new applications, Peterson says. “That sort of sourcing may be the majority. In those cases, it may be an unsecure service [provider], but one hopes that central IT has categorized its data well enough that critical pieces are not going outside.”

In such cases, and in situations where a company is dealing with smaller or newer SaaS companies, “you still have [some vendors] who won’t tell you where your data is or who you’re subcontracting to,” Peterson says.

The Exit Strategy

STANDARD CLOUD SERVICE CONTRACTS often don’t require the vendor to return your data to you at the termination of the agreement, says attorney Brad Peterson, a partner in the Chicago office of Mayer Brown.

“If you rely on that data, it’s a real problem. If you think about some of these small companies [that run their entire IT systems in the cloud], they could go out of business tomorrow,” he says. And if a service provider goes bankrupt, “the courts could take months to decide whether to give back your data.”

Companies need to keep data secure — and accessible — until its exit from the service provider, whether planned or unplanned, say industry watchers.

“Some of the big cloud providers feel like once they ‘onboard’ you and they have your data, they kind of have you by the back of the neck,” says Lou Guercia, CEO of Scribe Software, a Manchester, N.H.-based provider of hosted and on-premises data integration systems. “When it’s time to renew, that’s a piece of leverage that a service provider has — because they have your data.”

With data integration services such as Scribe’s, customers get local, real-time updated records of everything that’s happening in a cloud application.

To make it possible for users to see those records, cloud software vendors can write a “connector” — a task that should take one developer about a month. With a connector, “whatever data is running in their cloud can run on top of [the data integration service] — and get that local copy of their data regardless of the application,” Guercia says.

Today, vendors are more concerned about their reputations than they are about “squeezing a little revenue out of somebody” by holding data hostage, Peterson says. But that could change.

The cloud is a new phenomenon, and most contracts haven’t been up for renewal yet. “But as the industry matures and begins to consolidate,” says Peterson, “people might start to think they’ve got to grab every bit of revenue they can. It could get ugly.”

– STACY COLLETT

In the case of the Fortune 500 company, the fact that the vendor was outsourcing some services didn’t amount to a breach of contract because the cloud provider had cleverly stated that the services would be provided by it and its providers, without a restriction on subcontracting, says Peterson.

There are ways to use less-expensive, consumer-grade cloud services and keep data safe, Pescatore says. For starters, companies are beginning to deploy cloud-based security-as-a-service offerings to add features such as encryption, Web access and authentication.

The Best Defense

Industry watchers agree that encryption is the best way to secure data no matter where it goes. Even the most sophisticated service providers can’t prevent attacks by determined hackers, but encryption could help.

Pescatore points to several recent incidents where hackers infiltrated servers and stole passwords and then tried those same passwords on Google accounts. “By hacking your password in one place, and [discovering that] people were using that same password in Google mail, they were able to publish tens of thousands of corporate emails on the Web,” he says.

Several vendors, including Trend Micro, Unisys and Intel, now offer cloud-based encryption services.
“If I want to use Amazon’s cheap S3 storage service, but I don’t trust them to protect my data, I can feed my data through [a cloud security provider]. It’s encrypted in the cloud, and then it’s stored at Amazon in the cloud,” Pescatore says. “Amazon never sees the keys, and there’s no risk of the data ever being exposed at Amazon. So I get the benefits of the cloud at a reduced cost, but I don’t get the commodity-level storage.”

**Access Denied**

When an employee leaves the company or a contractor’s engagement comes to an end, you need a way to completely discontinue their access to your data. New cloud-based identity and access management tools are designed to do just that.

Cloud-based services from vendors such as Okta and Simplified federate identities across all of an enterprise’s hosted services. If an access change is required, the service makes the change across all of the cloud providers. For example, these tools can be used to terminate Contractor A’s access and grant access to Contractor B.

In the near future, more and more cloud providers will offer this as part of their service, says Jonathan Penn, an analyst at Forrester Research. “Salesforce.com already allows you to encrypt certain columns of data, but they still aren’t managing that,” he says. “If you want to manage the keys, that will be another level [of service].”

In a 2011 Forrester survey, more than 2,300 U.S. and European companies were asked how they would prefer to handle data security for the cloud or SaaS. Some 29% of the respondents said they would prefer to have security embedded by the service provider, and 11% said they would prefer to seek an add-on service from a security-as-a-service vendor. And 24% of respondents said they would like security tools that they could implement themselves.

**Web Security**

Many companies use multiple cloud service providers, and their employees and even customers may be able to access all of their data via browsers on their home PCs or smartphones — creating a potential security risk.

Smaller vendors offer Web security in the cloud to control data access. These services sit in front of the cloud services a company uses. If an employee tries to access a SaaS site, the information flows through the Web security service, which authenticates it and can audit the data the user is sending out or retrieving.

This type of service is becoming more common, says Pescatore. Small companies like Zscaler, Websense and Blue Coat Systems offer Web security in the cloud, and Cisco recently acquired Web security provider ScanSafe.

**Cost Considerations**

Procurement costs may look lower when buying a commodity cloud service and then adding one or more security layers, but don’t forget to account for manpower and management time.

Gartner reminds its clients that procuring IT systems in the cloud involves many of the same challenges as any other method of acquiring IT tools. “The more vendors you have to manage, the more management time and mature management process you will need,” Pescatore says. “Many smaller organizations without mature vendor management processes are better off looking at a specialty provider than commodity storage. Your people time and management time are going to be lower with a specialized service provider.”

**Easy Tips**

Finding a cloud vendor that can keep data secure doesn’t have to be a complex or expensive process. For instance, just look for a SaaS provider that has substantial assets or stands to lose a lot if its reputation is compromised, Peterson says. “At least they have a big name, and they care about their reputation,” he says.

You should also look for service providers that have security certifications such as SAS 70 or ISO 2701. Pescatore advises. Then ask questions to learn, for example, where they store data and where they keep backups of data.

And read the contract. “If it specifically disclaims things like ‘data security’ or makes specific statements such as ‘user shall not place highly confidential or private data on this system’ . . . that means they’re not intending to protect it,” Peterson says.

Once the decision is made to use a hosted service, “be highly conscious of what data will be part of what you’re sending to the cloud provider,” he says. Don’t send test data to an unsecure provider and then add production data to the site without considering security.

Even with smaller vendors, it doesn’t hurt to ask for extra security guarantees. “If you have a sufficiently large deal, these contracts are negotiable and providers are willing, because they know it’s a key to greater revenue with large clients. Most are willing to offer valuable protection — but not all of them,” Peterson says. “Use [utility] service providers when it’s appropriate” for less sensitive data, “and pay a little extra for a service when a utility service is not appropriate.”

**Down the Road**

As the cloud continues to mature, so too will security standards. New standards for cloud security are emerging with help from organizations like the nonprofit Cloud Security Alliance, ISO and other groups, Pescatore says. Gartner believes that by 2015, companies will start to see many more cloud services that are “business strength” and secure enough for the most regulated users, including government agencies and banks.

However, between now and 2013, Pescatore cautions, “any enterprise that’s putting customer, financial or other sensitive data out in the cloud is going to have to add some additional security capabilities to the mix or use some very specialized cloud service providers that offer that specialized cloud security.”

Forrester’s Penn offers some encouragement. “[SaaS providers] may not be perfect, but your own environment isn’t perfect. Let’s not try to compare it to the ideal but to reality,” he says. “We’re not outsourcing it specifically for security, although eventually I think that security will be a driver because those big providers are going to have better security than you have. We’re looking at a lot of other business drivers here — agility, flexibility in terms of TCO and pricing models. It’s a matter of understanding all the risks but also putting them in context to the business value.”

Collett is a Computerworld contributing writer. You can contact her at stcollett@aol.com.
LOUD COMPUTING poses unique security challenges for organizations, and multiple industry surveys have shown that security and privacy are among the key concerns of executives considering the cloud.

To address the challenges of securing the cloud, the Cloud Security Alliance (CSA), a not-for-profit organization made up of cloud vendors, user organizations and other key stakeholders, is developing the concept of cloud-specific security incident-response teams (CloudSIRT). Security executives and industry analysts say the initiative is a good move and should help bolster security in the cloud.

For many, the threat of security breaches is the biggest reason why they’re reluctant to embrace cloud computing. IT and security executives still aren’t convinced that service providers can adequately safeguard their data, particularly when it comes to using public cloud services for business transactions.

Some of this apprehension might be justified. In one of the latest industry surveys on cloud computing, conducted by security services provider Trend Micro in June, 43% of the respondents said their enterprises had experienced a security “lapse” or other problem with their cloud vendors within the past 12 months. The company queried 1,200 IT decision-makers in the U.S., the U.K., Germany, India, Canada and Japan.

According to the survey, respondents said the top barriers to adopting cloud computing are concerns about the security of data or the cloud infrastructure (50%), and concerns about performance and the availability of cloud services (48%).

Another report, released in June by research firm 451 Group, venture capital firm North Bridge Venture Partners and research firm GigaOM Pro, shows that many organizations are still in the early stages of cloud adoption or are taking a wait-and-see approach.

In that survey, 40% of the 413 respondents, including both IT professionals and vendor personnel, said they are only beginning to experiment with a move to the cloud. Another 26% said they are awaiting market maturity before adopting a formal cloud strategy.

Taking a Team Approach

CSA is aiming to quell many of the concerns about cloud security and privacy by promoting the use of best practices for cloud security and providing education on using the cloud to help secure other forms of computing.

In January, the organization began pushing the idea of CloudSIRT, an initiative in which major cloud providers are working to address the future of collaborative incident response and information sharing in the cloud.

The CSA’s premise is that SIRTs form the cornerstone of coordinated incident response and security information sharing for government agencies and enterprises, and that the model has worked well for handling malicious activity on the Internet.
**BEST PRACTICES**

But the organization says the advent of cloud computing has created a new set of challenges. The characteristics of cloud computing, such as multitenancy, resource sharing and on-demand provisioning, have the potential to complicate traditional response team operations. As a result, new types of teams are needed, it says.

“Most incident-response teams are focused [on] more traditional, on-premises computing infrastructure belonging to enterprises, governments and education institutions, and the threats to them from malware, spam, DDoS attacks and hackers,” says John Howie, who heads the CSA working group for the CloudSIRT initiative. He is also senior director of technical security services for the online services security and compliance team at Microsoft Global Foundation Services.

“With public and off-premises private cloud computing, organizations of all types no longer have computing infrastructure, or have a much reduced attack surface,” Howie says. “Cloud providers are managing the computing infrastructure. Incident response now has to cross not just boundaries within an organization, but across organizations.”

What’s more, the concentration of information assets from multiple user organizations creates the real possibility that the consequences of security breaches in the cloud will be much more severe than those of traditional incidents.

“An attack against a cloud provider, successful or not, can impact many organizations,” Howie says. “Complicating the situation, organizations might contract service with many cloud providers. As hackers develop new attacks, cloud providers and consumers need a new breed of team to coordinate incident response effectively.”

Cloud providers present a rich target for hackers, Howie adds. “Instead of compromising a single organization, a hacker can attack a cloud provider and can potentially gain access to the data belonging to several organizations,” he says. Because of this, they’re willing to devote much time and resources to attacking a cloud provider.

A cloud incident-response team that includes cloud vendors can share operational threat information to coordinate defenses against potential attackers as they’re identified, Howie says, helping to ensure the security and privacy of customer data.

The goal of the CSA working group is to bring together cloud service providers, telecommunications and Internet service providers, established computer emergency response teams (CERT) and other qualified parties to establish an industrywide CloudSIRT.

“Since the initial working group was brought together at the beginning of the year, we have developed a charter, membership criteria, information exchange protocols and other collateral that will be necessary to bootstrap CloudSIRT,” says Howie.

CloudSIRT has been formally incorporated, and the group is working toward establishing a memorandum of understanding with the CSA and registering as a nonprofit with the Internal Revenue Service. CloudSIRT will officially launch at the CSA Congress in November.

The group will initially consist mainly of cloud vendors and related service providers and established CERTs. Members will be expected to share information in a trusted fashion, and they must feel comfortable sharing information, Howie says.

To accomplish these goals, the working group has drawn up strict membership criteria and will publish details of who is eligible to join CloudSIRT and how they can join in the coming weeks. Howie wouldn’t say whether users would be included, but he did indicate that the working group is exploring “many more opportunities.”

Security experts say the CSA effort is a good step toward addressing cloud security. “I’m positive on CSA and the CloudSIRT initiative, because appropriate forms of information sharing are very important in incident response and threat assessment,” says Dan Blum, a security analyst at Gartner.

“The CSA has been an excellent focal point for the industry to collaborate on cloud computing security issues and has developed useful guidance,” he says. “The CSA has also done well on coordinating with other organizations, such as standards bodies.”

As hackers develop new attacks, cloud providers and consumers need a new breed of team to coordinate incident response effectively.

**JOHN HOWIE, HEAD OF THE CSA’S CLOUDSIRT WORKING GROUP**

Blum agrees with the premise that cloud computing requires a different type of response team. “A serious incident in the cloud may affect multiple [cloud service providers] and enterprise customers,” he says. “Each enterprise must have its own [incident-response] team to deal with a variety of issues, including legal and PR. But the enterprise IR team may be completely dependent on [cloud provider response] teams for information about the incident and some aspects of operational response.”

Today, Blum says, cloud customers likely aren’t being notified of all incidents their cloud service providers detect, and what information they do receive might be inconsistent, untimely or insufficient.

“Cloud-specific IR teams may help customer confidence to the extent they’re actually able to do [something] to resolve incidents or facilitate information exchange,” he says. “But cloud service providers and legal or regulatory bodies may first need to develop uniform codes of conduct that allow greater transparency and reduction of liability.”

As hybrid clouds evolve and organizations are linked more closely to cloud service providers and the providers are linked to one another at an operational level, Blum says, “IT’s world will become increasingly interdependent, and the effectiveness of incident-response processes and risk management in general will be even more critical. This will require CERT-level IR teams, much like incidents affecting multiple ISPs.
SECURITY EXECUTIVES are pleased with the CSA CloudSIRT plan. "I think the CSA’s effort is a very good initiative and in the right direction because of the cloud operational risk models," says Bart Falzarano, chief information security officer at Walz Group.

"For example, operating systems within companies have traditionally been the targets of attack over the past two decades," Falzarano says. "However, cloud introduces new potential targets, such as hypervisors and open APIs, and an attack against these new targets has potential to compromise groups of concentrated assets."

Pointing out that providers of public cloud services might not immediately adopt the latest security tools, Falzarano says, "I believe the CSA’s effort can certainly help organizations bolster security and defenses in the cloud."

Walz Group operates a private cloud in its data center. It enables the company to quickly move applications that support business processes among different pools of computing, memory, fabric, network and storage resources. Walz delivers software-as-a-service offerings that are hosted on its private cloud.

Falzarano says the company would like to get involved in the CSA CloudSIRT to collaborate on security and share best practices.

"I believe that a CloudSIRT is something that can help make the cloud more trustworthy by understanding incident lessons learned and establishing a set of best practices and standards," he says.

Improving incident-response capabilities must be an IT priority, given the precarious nature of today’s security landscape, including new threats to hosted data and applications in cloud environments with shared infrastructures, says Kathleen Moriarty, who is responsible for governance, risk and compliance strategy in the office of the CTO at EMC.

"Although some providers may adequately segregate information and applications, cloud tenants may require [their providers to offer] incident response and monitoring capabilities," Moriarty says.

The CSA CloudSIRT group “has taken positive steps to form an alliance between SIRTs and organizations that manage cloud infrastructures to raise the security posture of the cloud through effective incident coordination and awareness capabilities,” Moriarty says. "Incident handling involves the detection, reporting, identification and mitigation of an incident, whether it be a benign configuration issue, an IT incident, an infraction of a service-level agreement, a system compromise, a socially engineered phishing attack or a denial-of-service attack.”

Moriarty says global standards are needed to facilitate the exchange of incident information across national boundaries, languages and vendor offerings. She has been heavily involved in the development of such standards, including the IETF’s Incident Object Description Exchange Format and Real-time Inter-network Defense. Moriarty says she has become involved in the CSA’s CloudSIRT effort to ensure that the standards meet the needs of cloud providers.

BEST PRACTICES

It will also require teams that can work across [cloud service providers] on issues affecting a single customer or multiple customers.

Internal Cloud Teams

Some organizations have created their own cloud incident-response teams or are planning to do so, and they will be looking to the CSA for guidance.

"It’s exciting to see a [cloud] response team being formed," says Rosie Rivel, director of IT global risk and compliance at Kelly Services, a Troy, Mich., provider of workforce services.

“Our IT security group is always dealing with security-related issues, but in more of a traditional fashion," Rivel says. "As we’re moving into the cloud, what we’re trying to do is build a knowledge base internally, but we can’t do that in a short period of time.”

Being involved in the CSA effort would help Kelly Services gain valuable knowledge about cloud security, she says. The company began using cloud computing in 2004, when it adopted Salesforce.com as its customer relationship management platform. The cloud is now a major part of its IT strategy.

Bart Falzarano, chief information security officer at Walz Group, a Temecula, Calif., provider of communications and compliance technology services, has set up an internal cloud incident-response team that monitors its private cloud and SaaS services. Team members include senior managers, infrastructure engineers and technical operations support personnel.

For those looking to form their own teams, Blum says it’s best to include people from various parts of the organization.

“In general, IR teams must be cross-functional to cover multiple types of incidents,” Blum says. For example, human resources would get involved in incidents involving insiders, external security service providers might be needed for incidents involving hackers from the outside, operations would cover low-consequence incidents or those concerning availability, and legal might be drawn into incidents with regulatory compliance or public relations implications.

“Cloud technical specialists will be needed on the team for organizations using public cloud services for real business,” Blum says.

Howie, who is responsible for the incident-response function at Microsoft in addition to leading the CloudSIRT working group, wouldn’t discuss Microsoft’s efforts regarding cloud incident response. But he says for organizations that are adopting cloud computing and want to establish a cloud security team, the best place to start is with an existing CERT.

“There are plenty of excellent resources that an organization can leverage,” such as information and tips about security incident-response teams provided by the Software Engineering Institute, Howie says.

An organization looking to create a cloud response team has to "take into account the unique characteristics of cloud computing, establish lines of communication with its cloud providers, and draw up standard operating procedures for a range of potential incidents, [from] service outages all the way up to breach notifications," Howie says. ◆

Violino is a freelance writer in Massapequa Park, N.Y. You can reach him at bviolino@optonline.net.
physical security issues require a lot of attention when you’re considering a cloud service provider.

Just as a bank is a central repository for money and thus an attractive target for a robber, so is the data center of a cloud provider a central repository for valuable data resources and thus an attractive target for malicious hackers. So it’s important to vet the physical security of a cloud provider’s data centers. Here are some of the key issues to investigate:

**Security policy.** A policy typically details the mechanisms that the vendor has in place to prevent security breaches. An incident response plan typically details steps the provider will take should a breach occur. If the vendor has such documents, carefully review them. If it doesn’t, that’s a big red warning flag.

**Access Controls.** Does the cloud provider have physical access controls in place to ensure that only authorized personnel are able to access the IT infrastructure on which your data is stored and processed? Ask the following questions:
- Are the data centers in nondescript facilities?
- Do those facilities have security guards, gates and checkpoints?
- Do they have video surveillance systems?
- Does the vendor use intrusion-detection technology?
- Does it use multifactor authentication?
- Does it have a need-based access policy, with access rescinded if a user’s need changes?

**Background checks.** Does the cloud provider conduct background checks on everyone who has access to its infrastructure and your data? This can prevent malicious insiders from getting inside in the first place.

Additionally, you should determine if the cloud provider requires all staffers to receive training that covers the issues pertinent to data security and the provider’s own security policies.

**Segregation of duties.** Does the cloud provider distribute key tasks among multiple employees? This can help ensure that no single person is able to execute an unauthorized or inaccurate end-to-end transaction and go undetected. And if there are malicious insiders, the practice of distributing tasks among various people will make it harder for them to get away with anything.

**Third-party adherence.** If the cloud provider works with third parties, does it contractually require that those third parties understand and abide by the same security policies that apply to the provider’s employees? Also, does the provider have processes in place to monitor the activities of third parties to ensure compliance? This can help prevent a malicious third party from becoming a malicious insider.

As always, you need to address these issues in the contract. If the cloud provider’s security policy and incident response plan pass muster, then simply attach those documents to the contract and designate them as the cloud provider’s minimum security requirements. If the policy and plan are lacking, you can address any shortcomings with additional corrective language in the contract.

Following this process and codifying requirements in the cloud service contract is the best way to effectively minimize risks in the cloud.

---

**THOMAS J. TRAPPLER**

is director of software licensing at UCLA and a nationally recognized expert in cloud computing risk mitigation, as well as a regular contributor to Computerworld.com on the topic of cloud computing contract issues. For more information, visit ThomasTrappler.com.