

Cloud Control

A perfect storm is coming, one that pits security groups against business leaders desperate to contain costs. Can we find a middle ground?

By Mike Fratto

The amorphous nature of cloud computing can make IT pros charged with protecting their organizations' data feel like they're trying to rope the wind. While privacy and security top the list of governance woes cited by the business technology professionals we spoke with, availability,

performance management, accessibility, auditing, and monitoring are far from nonissues, especially for those subject to restrictive regulations such as Payment Card Industry standards or the Health Insurance Portability and Accountability Act.

"Cloud computing, in my opinion, would cause too great a reliance on

having Internet connections, plus expose company information to compromise or theft," says one respondent to our September *InformationWeek Analytics* cloud computing survey. "From a PCI compliance point of view, it would be a nightmare."

Still, the pluses—scaling applications quickly and seamlessly while shedding capital and operating expenses associated with maintaining servers—are attractive enough that this model will continue to gain popularity with business leaders. And cloud computing proponents, including the big vendors vying for shares of this lucrative market, are masters of accentuating the positives while downplaying potential negatives, like outages and governance challenges.

So how can infosec pros reconcile their need for governance with business leaders' directives to bring capital

internet evolution

Part of an ongoing series assessing the future of the Internet. For more, check out internetevolution.com. Contributors to its ThinkerNet blog include David Silversmith, a Web analytics consultant and former CTO of Carfax, and Mattathias Schwartz, who's contributed to *The New York Times Magazine*, among other publications. Internet Evolution also features industry-specific content in its IT Clan and Security Clan sections.

and ongoing costs under control? Our advice: CIOs must sit security groups down at a table with legal counsel and data owners to hash out issues. Having these hard discussions up front is the only way to counter skepticism, like that expressed in our poll, where just 18% of the 456 business technology professionals surveyed said they were using cloud services, compared with 34% who have no interest. More than half said they are very concerned about security, with performance, control, and concerns over vendor lock-in and support rounding out the top five worries.

We've heard this refrain before for software as a service. If you don't control your data—or, in some cases, even know where in the world it's residing—you can't govern it, and you surely can't promise an auditor that it's protected from unauthorized access. But even more than SaaS, cloud computing, by its distributed nature, raises issues regarding privacy rights and regulatory compliance. This is true whether you subscribe to the infrastructure model of cloud computing, where you lease resources on a metered basis, as with Amazon.com's Elastic Cloud Compute (EC2) and Microsoft's Azure, or an application platform model, where application services in the cloud are populated with your data, as with Salesforce.com or PeopleSoft. Governance issues, such as data management and regulatory compliance, are still very much in limbo. The courts and industry groups will eventually help develop guidelines, but for now, we're on our own.

Control Freaks

In a co-location scenario, where a company leases rack space, power, and network connectivity, IT is free to insert whatever equipment it wants. The co-location vendor should have auditable controls governing physical access to your hardware, mitigating the risk of someone stealing data locally.

5 Fast Fixes [SECURE DATA IN THE CLOUD

1. Define Your Governance Needs

Are they internal, external, legal? List the requirements and how they're satisfied.

2. Classify Your Data Before you can determine what data you can safely put in the cloud, you first have to classify and label it according to sensitivity and type.

3. Choose Wisely Identify cloud vendors that can satisfy your processing and governance needs. Direct business leaders to walk away from the rest, no matter how attractive pricing is.

4. Set Limits Define what the service provider can do with your data. Prohibiting the outsourcing of processing to a third party without your consent is basic.

5. Put Rules In Writing Publish policies and procedures stating which cloud vendors can receive which types of data.

In an infrastructure cloud environment, the situation is radically different. Your data and processing power can get moved at will from location to location, possibly with varying levels of physical access controls. The underlying virtualization systems of some infrastructure cloud providers may not yet be capable of providing strong assurances that virtual machines sharing a hypervisor are in fact separated and immune from attack. Cloud providers—in particular, the infrastructure variety—tend to be opaque computing services offering little visibility into their underlying architectures and technologies. You can't audit what you can't see, and this is a deal killer in many regulated industries.

On the flip side, Christopher Hoff, chief security architect with Unisys, points out that startup SaaS vendors that would once have had to build their own data centers now use infrastructure cloud services, such as Amazon Web Services, to provide not only the underlying core computing resources, but also value-add security

features like denial-of-service defenses, port scan monitoring, basic firewalling, and multitenant separation, which is more than what a typical startup SaaS vendor would provide on its own.

When Outsourcers Outsource

To make matters more complicated, all types of service providers may now off-load processing to the cloud, sometimes unbeknownst to the data owners.

“Governance is about where data lives and how it's classified,” says John Pironti, president of IT consulting firm IP Architects. “Outsourcing companies are themselves outsourcing their processing. Now you have to worry about where your data ends up.”

Pironti cites a company he consulted with that outsources data processing to a vendor in India. The company went through a due-diligence process to ensure that the outsourcer met security standards. However, the Indian outsourcing vendor in turn outsourced processing to a partner in China. Pironti's client didn't discover that its data had migrated to China until a routine audit detected network connections to the Chinese company. The Indian company stated it was doing what the original customer was doing—outsourcing processing to save costs.

Does this mean laws regarding data ownership and responsibility that bind the original host service no longer apply? Depending on whom you ask, you'll get very different answers. Pironti points out that any company that's outsourced data processing has encountered similar governance issues, and the same rules apply: Whether you're outsourcing to an ISP, a SaaS provider, or a cloud provider, ensure that clear definitions and responsibilities are defined in the contract governing privacy and security requirements. For this, you



GET A COPY For a link to this article, send a text message to 88411 that reads: jan2604YourE-mail@YourDomain.com. SMS rates apply.

need help from legal counsel because privacy laws are wildly inconsistent from country to country, and even state to state in the United States.

The type of data in a cloud service may have significant regulatory and legal ramifications, says Carolyn Lawson, CIO for the California Public Utilities Commission. She points to a 9th Circuit Court of Appeals ruling stating that, under the Stored Communications Privacy Act, providers of hosted e-mail/SMS services may not turn over messages to the company that's paying for the service without a warrant. In other words, if you contract with a cloud provider to manage your employees' e-mail, that provider may not supply you with copies of messages on demand, even though you're footing the bill. This could throw a serious wrench into e-discovery or internal investigations.

Stuart Charlton, chief software architect with cloud startup Elastra, further points out that companies doing business within the European Union need to ensure that EU citizens' private data doesn't reside in countries that have less stringent laws—like, say, most of the United States. And because of its

MORE AT INTERNETEVOLUTION.COM

Internet2: Can this overhaul help ensure cloud performance?

informationweek.com/1212/ie_internet.htm

Patent reform should be on IT's radar as computing models evolve. Watch out for trolls.

informationweek.com/1208/ie_patent.htm

strict privacy laws, Lawson says, before California governmental organizations consider cloud computing, they must make sure that private data remains within state borders or, after conferring with lawyers, that hosting data in other states or countries is acceptable.

Clouds Without Borders

Think outsourcing data—much less using a service like Amazon's EC2 or Microsoft's Azure—is out of the question for security reasons? Like the company that saw its data head to China, you may end up an inadvertent customer anyway.

Elastra, for example, is a management vendor for cloud computing. One of its reference customers is Christian James, which offers retail point-of-sale apps on a SaaS basis. The offering, called PayGo SaaS, may be hosted on your servers or in Amazon's EC2 cloud and uses a

credit card processor, Authorize.Net, to process credit purchases. That's three separate entities that may or may not have an impact on your overall Payment Card Industry compliance. Representatives from Christian James say the company takes measures to ensure that its software is PCI compliant, but they're unsure about the processes when the application is hosted with Amazon EC2.

MedCommons, which makes software for storing and managing patient health data, has a similar issue. MedCommons sells its software directly and as an Amazon EC2-based SaaS offering. Adrian Gropper, chief science officer for the company, points out that, as part of its SaaS licensing, customers must sign on to Amazon's user agreement as well as MedCommons'.

Call in the lawyers now, because whether you're subject to PCI or HIPAA or both, you need to ask de-

IMPACT ASSESSMENT		CLOUD GOVERNANCE	
	● BENEFIT		● RISK
IT organization	●●●●● Extending governance to all aspects of IT ensures business alignment and tighter control of assets. The cloud is no exception.	●●●●○ Fail to implement good cloud governance policies and risk running afoul of government, legal, and contractual obligations. "I didn't know the data was in China" is no excuse.	
Business organization	●●●●○ There's no doubt cloud computing provides business benefits. But it takes a well-governed move to the cloud to mitigate the associated risks.	●●●○○ Laws, regulations, and industry best practices around who is responsible for securing data in the cloud are in their infancy. There's no passing the buck here, so business leaders must stay vigilant.	
Business competitiveness	●●●●○ A sound governance program lets you gain the competitive edge that comes with cloud services while still complying with regulations.	●●●○○ Noncompliance will put your company at risk for fines and lawsuits. Both will consume time and money to fend off and erode customer confidence.	
Bottom line	●●●●○	●●●○○	Cloud computing is coming to your organization, like it or not. A governance plan gives IT the proactive control needed to proceed safely. In addition, auditors will be better able to conduct reviews and assert your practices are sound when policies are in writing and enforced.

tailed questions about where and how data is stored and who's responsible for it. And the answers have to be addressed in your contract.

Don't bother looking to state or federal government entities or industry groups for help just yet. They're simply not moving fast enough to keep up with the pace of technology.

Troy Leach, technical director of the PCI Security Standards Council, explains the council's position: "The council tries to maintain a technology-neutral approach and address specifically the risk associated with the cardholder data environment. [We] are currently evaluating whether the current requirements of version 1.2 of the PCI Data Security Standard mitigate emerging threats and vulnerabilities related to virtual components. The council hopes to provide clarity on the topic in the upcoming year."

Thanks a lot.

Caveat Emptor

Governance encompasses more than location awareness. Availability, accessibility, auditing, and monitoring are also key. Millions of Salesforce customers suffered a 38-minute outage in early January, and users of Amazon's Web services also saw downtime in 2008. The lesson: Pay careful attention

If you don't *control* your data, you can't *govern* it, and you surely can't promise an auditor that it's *protected*.

to the service provider's service-level agreement. Anything less than 99.9%, translating to about 8.75 hours of downtime per year, is unacceptable in most cases. Be sure you understand exclusions as well. For example, SLA claims usually are limited to the equipment and services under the provider's control and exclude problems like Internet disruptions.

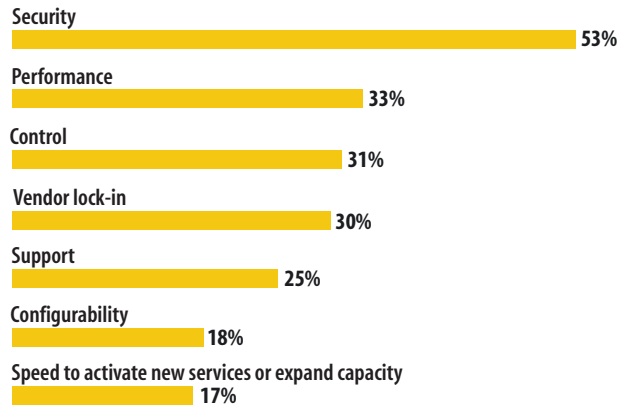
IT often must assert that regulated

or sensitive data is properly protected and that access is audited. This is where compliance gets murky; someone has to be responsible for data protection, yet agreements for services like Amazon EC2 and Microsoft Azure are clear—these companies aren't going to be held liable for data loss or fines or other legal penalties suffered while using their services. Now, both vendors offer guidance on using their cloud platforms in a secure manner, and, in fact, depending on your situation, data may be better

protected in their cloud than in your own facility.

But the fact is, these companies offer shared computing services, while regulations—including PCI—generally mandate that IT prove its systems are securely managed, and in some cases, require an independent audit demonstrating that fact. Unless yours is a big contract, good luck getting your auditor into either Amazon's or Microsoft's

CLOUD-RELATED ISSUES THAT HAVE IT PROS CONCERNED



% indicating they're very concerned about these issues

Data: InformationWeek Analytics Cloud Computing Survey of 172 business technology professionals considering or using cloud services

data centers to perform an inspection.

You'll often have better luck with smaller providers. For example, Zoho, which offers productivity and other applications in the cloud, has undergone external audits at customers' requests, and at the customers' expense.

Note that a service provider's SAS-70 audit is not a sufficient replacement for an independent review. For starters, you generally won't have the opportunity to review the auditor's full report, which details very sensitive information, like the architecture and service provider's controls. You'll see only the statement of opinion, which is a summation of the auditor's judgment as to whether the provider's controls satisfy its goals. Further, SAS-70 audits are typically applied only to a subset of the service provider's IT systems, so the statement of opinion may not even cover all relevant portions of the operation.

Until a legal framework on adequate controls in cloud environments is worked out through legislation, regulation, or court cases, IT is left trying to get its arms around a cloud.

Write to Mike Fratto at mfratto@techweb.com.