Cloud Computing: Both Sides Now

A CFOworld Focus on What Finance Should Wonder At — and Worry About

INSIDE

The Cloud and the CFO  2
A Peek Inside the Cloud  3
Agility Rules  8
The Scary Side of Virtualization  15
What’s Behind the Cloud: A Glossary  19

CFOworld looks at the wonders and worries of cloud computing for financial executives.
The Cloud and the CFO

A real-world look at how the computing phenomenon plays in the finance department.

IT ALL SOUNDS SO SIMPLE ON THE MICROSOFT WINDOWS television commercials: “To the cloud...” says the mother, and soon she’s pasting smiling faces on the chaotic family portrait glaring at her from the desktop. But, of course, the mom isn’t worried about compliance issues; or data being mishandled or lost by a third-party provider; or passwords being stolen; or CEO, board and shareholder wrath when problems arise.

Making decisions in the finance department about to what extent to use cloud technology, if it is used at all, is a far more complicated, and risky matter.

This special report from CFOworld, a new online publication from a publisher well versed in technology matters, seeks to take finance expertise and the experience of early adopters, and to blend it with the best that CIOs have to offer. Our goal has been to use a finance filter – rather than a tech filter – to help CFOs penetrate the mysteries of the cloud.

The effort is typical of what CFOworld aims to do with its launch: add value for corporate finance with critical information, in part by giving CFOs and IT people a common ground of understanding.

— ROY HARRIS
Editorial Director
CFOworld, a CXO Media Inc. Publication
A Peek Inside the Cloud

THE 2007 SUCCESS STORY IS PART OF cloud computing lore. The New York Times, in attempting to prepare a full online archive dating back to 1851, had faced a daunting and what seemed enormously expensive task: converting 11 million articles, already scanned into digital images of newspaper pages, into a format more conducive to web presentation.

The hero was Times software developer Derik Gottfrid, who famously wrote a program that would glean the bits and pieces of each article from the 150-plus years of image data and assemble them into individual PDF files.

What CFOs Need to Know about the Phenomenon

BY ROB GARRETSON
He used Amazon Web Services (AWS) and its Elastic Compute Cloud (EC2) utility, renting 100 so-called virtual computers to manipulate the stored images in parallel and save the newly created PDF files back on Amazon servers. The reported cost: $240.

Using the “cloud” — the term now so easily tossed around, often by people who understand it poorly — he accomplished in about 24 hours a job that would have taken weeks of planning, provisioning and processing, and thousands of dollars of dedicated hardware and software had the newspaper used internally owned and operated resources. Had it not been for the ease and low cost of the Amazon cloud, Gottfrid has said, the Times might have abandoned the project.

The resourcefulness detailed in Gottfrid’s blog post remains among the clearest examples to date of the twin attractions of cloud computing. One was the flexible pay-as-you-go delivery model for information technology that in recent years has constituted the next big thing in IT. Companies such as Amazon, IBM, Microsoft and Google are investing billions of dollars in it. The other: the elimination of upfront costs — in this case for acquiring hardware and software licenses, while reducing operational complexity and maintenance burdens. At its best, the usage-based utility model can boost business agility, allowing companies to quickly respond to changing business conditions or new opportunities.

“There are two drivers” in adopting cloud computing, notes Chris Eimas, vice president, financial planning and analysis at Herndon, Va.-based software maker Deltek, and a former CFO at several private companies. “The case for cost reduction and agility are both very compelling.”

An Edge to the Little Guy
The cloud approach has been vital to start-ups and smaller companies that can now afford to deploy complex business applications like customer relationship management and enterprise resource planning — thanks to companies like Salesforce.com and NetSuite — that were once the exclusive domain of the Fortune 1000. Yet despite the purported cost advantages that are particularly attractive to CFOs, larger companies are moving business processes and data into the cloud at a more measured pace.

Larger public companies have more burdensome disclosure requirements, often making them more deliberate about changing their business processes, notes Eimas. And “with Sarbanes-Oxley, companies are reticent to make anything but incremental changes.”

Only 8% of U.S. corporations
had implemented a cloud service at the end of 2010, according to research firm Gartner Group, which projects that percentage to soar to more than 50% by the end of next year. Yet, according to its annual Emerging Technologies Hype Cycle report, cloud computing has just crested the “peak of inflated expectations” and is still two to five years way from mainstream adoption.

That may be due to a lack of clarity, not just among finance executives, but among IT professionals as well, about what constitutes cloud computing. [See “What’s Behind the Cloud: A Glossary.”] The most frequently cited definition, from the National Institute of Standards and Technology (NIST) IT laboratory, is now on its 15th version, offering five essential characteristics, three different service models, and four distinct deployment models. It is nearly 700 words long and carries a disclaimer that the “definitions, attributes, and characteristics will evolve and change over time.”

What’s Public and What’s Private

The key component of the “spirited debate by the public and private sectors” that defines cloud computing, according to NIST, is distinction between so-called public clouds – infrastructure owned and operated by a third-party such as an Amazon, Google or Microsoft – and private clouds. Private clouds have infrastructure deployed either internally or hosted by a third-party that is owned and operated by the organization itself, but pooled and made available as on-demand service to individual business units, departments or end users.

“Technically, clouds existed anytime anybody had a data center,” contends William Miller, an associate vice president and controller at Nationwide Insurance responsible for IT finance. “I have a data center. I restrict access, but technically all my applications and all my data lives in my data center, and is accessed remotely through some kind of connection. So I’ve had a private cloud since

I’ve had a data center; that’s 25 years now.”

The technology that turns corporate data centers into private clouds – an approach that has only become ubiquitous in recent years – is known as “virtualization” for its ability to abstract computer applications and operating software from the underlying hardware. It allows the near-instantaneous spawning of what techies call “virtual machines” or “instances” that can be deployed and turned off on demand. It enables the type of resource pooling and rapid elasticity of services that has become known as cloud computing. And though large organizations still take a cautious approach to migrating their processes and data to the cloud, the momentum is building rapidly.

“There is absolutely no doubt cloud computing is here,” says Nationwide’s Miller. “We know for a fact that in an environment with 100,000 servers, the [per-unit] hardware cost is less than half of
Small firms moved to the cloud first, but large ones now are jumping on the bandwagon.

Measuring the Momentum
Management consultancy McKinsey & Co. found evidence of the momentum behind the cloud in its most recent global business technology survey published in November. More than 80% of IT respondents said their companies are using or experimenting with cloud technology, while 63% said their companies are using cloud-based applications in some aspect of day-to-day operations. Over the next 12 to 18 months deployment and piloting is expected to increase across all application types explored in the survey.

And though the lion’s share of cloud deployment to date has been by smaller companies, taking advantage of the economies of scale to access enterprise-class software, large organizations of all kinds are jumping on the bandwagon.

That includes the federal government, in a big way. Recently the Obama Administration announced a 25-Point Implementation Plan to Reform Federal IT Management, a key component of which is the shift to a “Cloud First” policy, giving each government agency three months to identify three IT services that it will move to the cloud; the first within 12 months and the remaining two within the next 18 months.

One notable five-year goal of the new federal plan is to eliminate 800 federal data centers, which swelled to 2,094 in 2010, up from only 432 in 1998.

“For too long, many government IT projects cost hundreds of millions of dollars more than they should, took years longer than necessary to deploy, and delivered technologies that were obsolete by the time they were completed,” the federal CIO Vivek Kundra noted in a recent post on the White House blog.

Last week the Treasury Department said it is moving four existing web sites into the Amazon Web Services cloud, as well as a newly created site, reportedly becoming the first cabinet-level agency to move to AWS. The federal government diving headlong into cloud computing may go a long way toward easing the concerns that keep financial executives up at night: business continuity, data security and compliance.

Under the Federal Risk and Authorization Management Program (FedRAMP) launched last year, the govern-
Both Sides Now  
CFOworld looks at the wonders and worries of cloud computing for financial executives.

A WikiLeaks Worry

Though he concurs with the government’s cloud computing initiative, Nationwide’s Miller remains cautious about data security in what is still a relatively immature IT delivery model. “WikiLeaks makes everybody take a step back and say, ‘Wait a minute, let me think about this a little differently,’” he suggests.

Privacy, data control and data containment remain critical considerations for financial executives working with IT leaders in migrating operations to the cloud, Miller says, as is performance of critical business applications to ensure that there’s no unnecessary latency accessing resources remotely.

“My experience is that once people get their hands around it, there’s a much higher level of comfort,” Deltek’s Eimas notes. “Everybody knows what can happen if data is compromised; it’s a public relations nightmare” – and often much more. “But these problems are largely preventable with a little bit of forethought.”

As far back as 2009 the Deloitte consultancy concluded that the scale of major cloud computing providers had grown sufficiently to ensure that their security measures would likely be stronger than what most companies could implement internally. “Generally, the level of computer security, data privacy practices and the expertise of major cloud service providers are likely to be greater than those provided by an in-house IT staff and systems,” according Deloitte’s report, Moving to the Cloud.

“The reality is, if you’re a large enterprise, you likely already have a data center; you already have a private cloud,” Miller adds. “So the question becomes, what portion of my portfolio makes sense in a third-party (public) cloud, and what portion of my portfolio makes sense in a private cloud?”

The applications that enjoy the most beneficial economics in the cloud are those with predictable usage spikes. That includes, for example, the order entry system at a florist, which sees business balloon on Mother’s Day and Valentine’s Day each year.

“In that case, not maintaining capacity that goes underutilized for 12 months out of the year so that I can have that one big day, there are tremendous and compelling rational reasons [for] a cloud environment, so that I’m only renting what I need, when I need it and not paying for it the rest of the year,” Miller says. “Absolutely, that’s compelling.”


Rob Garretson is a business and finance writer based outside Washington, D.C.
Agility Rules

CFOs expecting mainly lower costs in the data center sometimes get a nice surprise.

BY ROBERT L. MITCHELL AND ROB GARRETSON

THE OFFLOADING OF IT infrastructure to third-party cloud providers has become a popular way for finance to contain technology costs. But boosting the flexibility of business systems may be the most compelling benefit of the growing cloud computing movement.

In its most recent global business technology survey, management consultancy McKinsey & Co. found cloud computing’s promise of that increased agility to be by far the greatest potential advantage recog-
Both Sides Now | CFOworld looks at the wonders and worries of cloud computing for financial executives.

nized by corporate leaders. Asked to identify the most significant ways they expected their companies to realize value from cloud computing, 70% of the non-IT respondents cited “increased business flexibility,” while 55% named “increased ability for IT to scale up (or shrink) to meet business needs,” and only 29% cited the “lower unit cost of IT.”

And many larger companies — even if they aren’t yet ready to outsource significant portions of their IT infrastructure to third-party service providers — are achieving much of the scalable, on-demand flexibility offered by third party cloud services from their own “private” clouds. These typically don’t deliver the economies of scale of public clouds — infrastructure owned and operated by a third-party such as an Amazon, Google or Microsoft. But private clouds provide many of the same benefits. These internally owned and operated IT systems — whether hosted in-house or by a third-party — are similarly pooled and made available as on-demand service to individual business units, departments or end users, making them nearly as elastic as third-party cloud services.

“The agility that’s purported as existing in the cloud can exist in any environment, if IT thinks through the process, and the business thinks through the process appropriately,” insists William Miller, an associate vice president and controller at Nationwide Insurance who handles IT finance.

Long-Term Payback
In the time it takes to get a cup of coffee, any one of the hundreds of engineers and developers at mobile computing chip-maker Qualcomm Inc. can provision himself a new server — one that’s fully configured with compute, storage, networking, middleware and other resources. “You can get something provisioned within 15 minutes,” says Matthew Clark, senior director of IT.

Though Clark insists that the San Diego-based company’s self-service infrastructure, dubbed “AutoZone,” falls short of true cloud computing, it includes the primary hallmarks of a private cloud: a self-service portal with a menu of standardized services for

Key Elements in a Private Cloud
Virtualization
Highly standardized infrastructure
Automated provisioning
User self-service
Catalog of services
Usage-based cost accounting and chargeback
Dynamic resource scaling as application loads change

SOURCE: COMPUTERWORLD INTERVIEWS WITH IT EXECUTIVES.
users to choose from; a “virtualized” infrastructure built using standardized suites of hardware and software; fully automated provisioning and de-provisioning, as the IT people call those processes; and the ability for IT to meter and allocate costs from the division level down to the individual department, application or user.

James Staten, an analyst at Forrester Research Inc., says Qualcomm is on the leading edge. No matter how Clark defines cloud computing, he says, “Qualcomm is a lot further along than most companies are.”

And Clark’s peers are certainly watching with great interest. Heading into the new year, private clouds are rapidly becoming a priority for corporate IT. The core elements – on-premises virtualization, standardized infrastructure and service offerings, and automated provisioning – can deliver cost efficiencies and reduce administrative overhead. But the biggest driver by far is time to market, executives say. “We look at the benefit as quicker time to onboard applications, not cost savings. It’s all about speed of deployment,” says Norm Fjeldheim, Qualcomm’s CIO.

With all of the hype about the cloud, it’s important to keep in mind that, unlike some public cloud services promising instant gratification, private cloud is an “infrastructure play” designed to deliver a long-term payback. “The economies only work when it’s shared,” says Staten. And that means business users must be willing to accept a limited set of standardized service offerings – and fewer customizations.

Private clouds aren’t necessarily hosted on-premises, although they often are. Sometimes, hosted private cloud services from third-party providers manage dedicated cloud infrastructures for their customers at off-site locations, in

Economies Based on Sharing
In addition to the core attributes of virtualization, standardization and automation, there’s another important element in a private cloud architecture: “multi-tenancy.” Cloud-based services must be shared across all of the organization’s departments and business units in order to pay off. “The economies only work when it’s shared,” says Staten. And that means business users must be willing to accept a limited set of standardized service offerings – and fewer customizations.

“Private clouds aren’t necessarily hosted on-premises, although they often are. Sometimes, hosted private cloud services from third-party providers manage dedicated cloud infrastructures for their customers at off-site locations, in

“It’s all about speed of deployment,” says Qualcomm CIO Norm Fjeldheim.
a formulation often called hybrid clouds.

An advantage of such arrangements is that the service providers can offer “cloud bursting” – the rapid addition of computing capacity from the public, multi-tenant cloud to handle temporary periods of heavy loads. But IT executives remain cautious about such setups because they have concerns about security and control; they’re also leery of service-level agreements that seem better suited to small businesses.

“Security is a big, big deal for us. And not just security, but [also] the perception of it,” says Fjeldheim.

Wake Technical Community College in Raleigh, N.C., built a different kind of hybrid. The school is part of a consortium that developed a hosted private cloud that serves as a virtual computer lab (VCL) for students. The VMware-based system, built on IBM Blade-Servers by the Microelectronics Center at North Carolina State University, automatically provisions a virtual machine when a student logs in. Each image lasts for up to eight hours before it’s automatically de-provisioned.

The VCL system eliminated the need to open a new 50-seat lab, saving $50,000. But CIO Darryl McGraw says the school did run into one issue with a private cloud hosted by a third party. The fall semester starts earlier at Wake Technical College than at North Carolina State, and just as classes started at the former, administrators for the VCL took down the servers for maintenance. “The concept of multiple tenants on the same hardware can be problematic,” McGraw says.

He has also limited the cloud to student labs, as opposed to, say, the school’s ERP system. “The worst that can happen is that someone gets their homework hacked into,” he says. Overall, however, he considers the VCL to be a success, and he plans to push 137 physical computer labs into the VCL cloud over the next five years.

Using commercially hosted private clouds also presents contractual challenges. The CIO at one Fortune 500 company, who is currently negotiating with a major cloud service provider, says it’s not always clear who’s responsible when things don’t work – or how the problem will be resolved.

Providers expect to be able to change terms and conditions in contracts at a moment’s notice, he complains. And he says that the
service-level agreements he’s seen are totally inadequate. “They want to limit their liability so greatly that – why bother?” he asks, adding, “If I offered those types of SLAs to the business, I’d be out of a job.”

The CIO, who asked not to be named because he’s still in discussions with the vendor, says that in many cases, such contracts simply aren’t designed for enterprise-class, mission-critical applications. The negotiations with vendors so far, he says, have been “burdensome.”

The Caveats
But the need for rigid standardization of processes, services and infrastructure that underlie the cloud may be the biggest nut to crack in the year ahead. Problems come when IT – or its customers – begin customizing the standardized catalog of services because they don’t like the predefined choices.

“For a private cloud to work, the IT shop has to deliver highly repeatable, consistent services with minimal or no customization,” says Nick Van der Zweep, director of business strategy for industry standard servers and software at Hewlett-Packard. For example, HP offers just three configuration templates for hosting an Oracle RAC database in the cloud: small, midsize and large. To host an Exchange email system in the cloud, the administrator can choose only the number of users.

Straying from the path can lead down a slippery slope, since without a finite, standardized services catalog, the benefits of the system are greatly reduced. “All these things I change turn off the ‘cloudi-ness’ of it,” Staten says.

The only way to succeed, he argues, is to make it more costly for users to go outside of the standard offerings. Users who follow the rules get a system in 15 minutes and a neatly packaged services-based chargeback model. Those who need a custom configuration must wait longer – and pay more.

But he doesn’t think the chargeback model will fly in many organizations, and he contends that this is what will hold up broader adoption of internal clouds. “We’re confident that 95% of IT shops aren’t ready for that,” says Staten.

Fjeldheim sees “IT process standardization” as a key to success. “We have a very standardized way of doing things, good automation and process control,” he says, adding that the company recently earned the ISO 20000 IT service management and ISO 27000 IT security management systems certifications. But that doesn’t necessarily mean you have to create different processes or tool sets for managing cloud and managing traditional infrastructures.
John Fiore, CIO at Bank of New York Mellon, worries about vendor lock-in with the so-called cloud-in-a-box offerings of some large vendors as he ponders choices for a pilot project. “There really aren’t any standards at this stage of the game. If you go down a certain path, that’s yet another new architecture you’re accepting – and what might be the life span of it?” He says he likes the idea of cloud-in-a-box offerings that bundle all the necessary hardware and software into one neat, tidy package but adds, “We’d prefer not to have a tight coupling between the two. Until they evolve to a point where a loose coupling is achievable, there are definitely some business risks here.”

**Starting Slowly**

Most private cloud pilots focus on relatively safe, internal IT functions, such as testing and development. Bank of New York Mellon, for example, plans to focus early cloud-automation efforts in the development and quality assurance areas. Wake Technical focused on student labs, where student homework is the only thing at risk.

At Roswell Park Cancer Institute in Buffalo, N.Y., the initial test will be to allow the IT staff to automatically provision virtual machines for testing purposes, before moving on to the server team and application developers, according to Tom Vaughan, director of IT infrastructure. “Instead of going through the paperwork of requesting that a server be built, they will be able to do it themselves,” he says. And as the center rolls out virtual desktop technology to its Citrix clients next year, Vaughan says the back-end servers will move into the cloud. “I’d like to push out as many services to people as we can,” he adds.

That’s the plan at Bank of New York Mellon as well. Fiore says the bank plans to aggressively invest the investment they’ll have to make upfront to take full advantage of a private cloud architecture. “You’ve got to do your homework on the application side.”

To Daniels at integrator ManTech, the key is to identify services that can be reused across the organization – and stick with them. The problem, he says, is that each user organization wants things done slightly differently.

“You get into this ugly business-process re-engineering that has to go on. You say you have to do it this way, and then you have a rift with the user community,” he explains. Those who have gone down this route with service-oriented architectures will have a leg up with internal clouds, he contends. Others, he says, may not appreciate the technology most important to your organization in the next 12 months:

1. Virtualization
2. Cloud computing

SOURCE: COMPUTERWORLD’S EXCLUSIVE FORECAST SURVEY OF 209 IT PROFESSIONALS, JUNE/JULY 2010
Private clouds could take over large tracts of data centers, especially for applications with variable workload demands.

Robert L. Mitchell is a national correspondent for Computerworld. Rob Garretson is a business and finance writer based outside Washington, D.C.

Editor’s Note: This story is based on an article originally written for Computerworld by Mitchell. The finance perspective was enhanced by Garretson.
A key underpinning of cloud computing is the technology known as virtualization, done through a layer of software that isolates computer applications and operating software from the underlying hardware. The virtualization process allows various computing resources – storage, processing, memory, network bandwidth and the like, across a network of computers – to be dynamically reallocated to individual, software-defined machines, applications, or even end-user desktops.

The technology has been in use since the 1960s, in the basic operating software of multi-million-dollar mainframe
“One of my biggest fears is the ability to steal” virtual servers: Rent-a-Center Inc.’s Jai Chanani.

computers. But in recent years it has been widely deployed, thanks to popular software such as VMware – letting IT departments allocate resources flexibly across the networks of inexpensive PC servers that have proliferated in corporate data centers. Its use accelerated during the recent economic downturn, as companies sought to trim IT budgets by consolidating those often massive server farms. And this ability to rapidly provision and deploy what techies call “virtual machines,” or “instances” of a particular software application, make public cloud computing services possible, along with the private clouds that larger companies have started to create.

Yet the movement to virtual environments – where specific computers are no longer physical devices that can be secured by lock and key – has executives, and particularly IT professionals, nervous. When TheInfoPro surveyed 214 IT security professionals in November, it found that one-third were “very or extremely” concerned about security in a virtualized environment.

At the Computerworld Premier 100 IT Leaders conference in last March, one CIO stood up to express his unease about the security of a virtual infrastructure that has subsumed more than half of his company’s production servers. Two other IT executives chimed in with their own nagging worries.

None of the executives in that room wanted to admit on the public cloud computing services

Getting Worried

How concerned is your organization with the issue of security in a virtualized environment?

- Very or extremely: 32.7%
- Somewhat: 36%
- Minimally: 23.7%
- Not at all: 7.6%

SOURCE: THEINFOPRO SURVEY OF 214 IT SECURITY PROFESSIONALS, NOVEMBER 2010

“One of my biggest fears is the ability to steal” virtual servers: Rent-a-Center Inc.’s Jai Chanani.

computers. But in recent years it has been widely deployed, thanks to popular software such as VMware – letting IT departments allocate resources flexibly across the networks of inexpensive PC servers that have proliferated in corporate data centers. Its use accelerated during the recent economic downturn, as companies sought to trim IT budgets by consolidating those often massive server farms. And this ability to rapidly provision and deploy what techies call “virtual machines,” or “instances” of a particular software application, make public cloud computing services possible, along with the private clouds that larger companies have started to create.

Yet the movement to virtual environments – where specific computers are no longer physical devices that can be secured by lock and key – has executives, and particularly IT professionals, nervous. When TheInfoPro surveyed 214 IT security professionals in November, it found that one-third were “very or extremely” concerned about security in a virtualized environment.

At the Computerworld Premier 100 IT Leaders conference in last March, one CIO stood up to express his unease about the security of a virtual infrastructure that has subsumed more than half of his company’s production servers. Two other IT executives chimed in with their own nagging worries.

None of the executives in that room wanted to admit on the public cloud computing services possible, along with the private clouds that larger companies have started to create.

Yet the movement to virtual environments – where specific computers are no longer physical devices that can be secured by lock and key – has executives, and particularly IT professionals, nervous. When TheInfoPro surveyed 214 IT security professionals in November, it found that one-third were “very or extremely” concerned about security in a virtualized environment.

At the Computerworld Premier 100 IT Leaders conference in last March, one CIO stood up to express his unease about the security of a virtual infrastructure that has subsumed more than half of his company’s production servers. Two other IT executives chimed in with their own nagging worries.

None of the executives in that room wanted to admit on the
Firms see half their critical apps on virtual infrastructure and say, ‘Gee, is that secure?’

record that they feel vulnerable, but Jai Chanani, senior director of technical services and architecture at Rent-A-Center Inc., feels their pain. “One of my biggest fears is the ability to steal [virtual servers],” he says.

Chanani’s team has about 200 virtual servers operating as file, print and, in some cases, application servers. But, for security reasons, his shop doesn’t use virtualization for the company’s ERP system, databases or e-mail.

Michael Israel, CIO at amusement park operator Six Flags Inc., voices a different concern. For him, the most unnerving scenario is a rogue administrator moving virtual servers from a secure network segment onto physical hosts in an unsecured segment, or creating new, undocumented, unlicensed and unpatched virtual servers. “The last thing I want is 25 servers out there that I don’t know exist,” he says.

Potentially Devastating

John Kindervag, an analyst at Forrester Research Inc., says he’s heard stories from clients who have had VMware’s vCenter management console compromised, enabling the attacker to copy a virtual machine that can then be run to access data. “When you steal a VM, it’s like you broke into the data center and stole a piece of hardware. It’s potentially devastating,” he says.

“We worked for many years with customers on best practices that make this a complete nonissue,” says Venu Aravamudan, senior director of product marketing at VMware Inc. He says most users address such risks by following best practices such as creating an isolated network segment for managing the resources, and creating role-based access controls.

The migration onto virtual servers has saved businesses huge sums of money as a result of consolidation and improved efficiency, but as virtualization gobbles up more and more production servers, some IT executives are getting indigestion. Has anything been overlooked? Could a catastrophic breach bring down critical applications — or perhaps an entire data center?

“Customers wake up one day, realize that 50% of their business-critical apps reside on virtual infrastructure and say, ‘Gee, is that secure?’ That’s very common,” says Kris Lovejoy, vice president of strategy at IBM Security Solutions, a security consultancy.

“We worked for many years with customers on best practices that make this a complete nonissue,” says Venu Aravamudan, senior director of product marketing at VMware Inc. He says most users address such risks by following best practices such as creating an isolated network segment for managing the resources, and creating role-based access controls.

Firms see half their critical apps on virtual infrastructure and say, ‘Gee, is that secure?’
the truth,” says Andrew Mulé, a senior security consultant in EMC Corp.’s RSA unit.

The problem isn’t that a virtual infrastructure is difficult to secure per se, but that many companies still haven’t adapted their best practices (if they have them) to the new environment. In fact, concerns persist despite the fact that there have been no known attacks against virtual infrastructures, says Eric Baize, RSA’s senior director for secure infrastructure.

“People are wringing their hands over theoretical scenarios rather than ones that have been documented to be a problem,” agrees Bill Trussell, managing director of security research at TheInfoPro, an IT market research firm in New York.

**5 Things the CFO Should Ask**

Among the key questions CFOs should ask their CIOs about the security of their virtual environments are:

- Are we using industry best practices to secure our virtual environment (for example, no use of default passwords in creating virtual machines)?

- Have we realigned responsibilities and the approval process within IT to address potential security gaps in our virtual environment?

- Are we using adequate network storage access controls and file integrity monitoring to secure our virtualized data?

- Are our core network architectures setup to accommodate virtualization, and do all our firewalls, intrusion-detection and -prevention systems, and other monitoring tools have visibility into the virtualized systems?

- Have all our reporting and compliance policies been strictly implemented in the virtual environment?

The best way to create a secure virtual infrastructure is to get security experts involved early. Gartner estimates that as many as 40% of IT shops don’t seek IT security’s input on a virtual deployment until after the system is already built and online.

It all comes down to policy, contends KC Condit, senior director of information security at Rent-a-Center. “If you don’t have a strong security policy in place, a virtual infrastructure is going to show up those weaknesses much more quickly because things happen more rapidly,” he says, referring to how quickly virtual servers can be created and then moved around between physical host servers.

“A certain healthy level of paranoia is always a good thing,” he adds.

Robert L. Mitchell is a national correspondent for Computerworld. Additional reporting on the finance perspective was provided by Rob Garretson.

Editor’s Note: This article was adapted by CFOworld from a Computerworld cover story.
What’s Behind the Cloud: A Glossary

As CFOs seek to understand cloud computing, IT jargon complicates the effort. This brief 10-item glossary is designed to interpret and clarify some of the most common and useful cloud-related terms with the finance executive in mind.

Cloud Computing

A method of delivering computing resources – including storage, servers, processing, memory, network bandwidth, applications and services – typically over the public Internet, using a shared infrastructure. In one of its greatest contributions to cost-efficiency, a “utility pricing” model lets customers pay only for what they use.

Virtualization

The creation of a software layer between existing computer hardware and Windows or other host operating systems. By fooling the operating system into thinking it’s talking to the hardware, this buffer layer of software allows multiple “virtual machines,” each hosting their own operating system and application, to run side-by-side on the same physical hardware. Effi-
ciency also results from the software acting as a traffic cop, intercepting requests from each virtual machine and redirecting them to the appropriate resources, such as storage, network bandwidth or compute cycles.

**Private Clouds**
Describes a model in which the cloud infrastructure is operated solely for one organization. It may be managed by the organization, or by a third party, and may exist on or off the premises. The infrastructure supporting those services is completely dedicated to one customer.

**Public Clouds**
The model in which the cloud infrastructure delivers a set of shared “multi-tenant” services, often to a variety of businesses, individuals, or industry groups.

**Community Clouds**
Here, the infrastructure is shared by several organizations, and supports a specific community that has common concerns, such as mission, security requirements, or policy or compliance considerations. The organization may manage it, or it may be managed by a third party.

**Hybrid Clouds**
Their infrastructure is composed of two or more clouds – whether private, public or community – that remain unique entities, but are bound together by standardized or proprietary technology that lets the data be portable, allowing such things as “cloud bursting,” for example, to help balance loads between clouds.

**The IaaS Model (Infrastructure as a Service)**
Provides processing, storage, networks, and other fundamental computing resources, with the customer deploying and running the software. The customer does not manage or control the cloud infrastructure, but controls the operating systems, storage and
MSPs (Managed Service Providers)
One of the oldest forms of cloud computing, service through MSPs basically involves applications – such as virus scanning services for e-mail – that are exposed to IT rather than to end-users. Desktop management services are often MSPs, as are security services from SecureWorks, IBM and Verizon, and anti-spam services such as Google’s Postini.

The SaaS Cloud Model (Software as a Service)
The capability provided to the customer lets it use the provider’s applications, but running on a cloud infrastructure, and accessible from various customer devices, usually through a web browser or web-based email. The customer does not manage or control the underlying cloud infrastructure – including network, servers, operating systems and storage – except possibly for some limited applications. For customers it means no upfront investment in servers or software licensing, while provider costs are lower, compared to conventional hosting, because there is just one application to maintain. Salesforce.com, NetSuite and Google Apps are examples.

The PaaS Model (Platform as a Service)
Allows the customer to deploy customer-created or acquired applications within the cloud infrastructure, using programming languages and tools supported by the provider. Customers do not manage or control the underlying infrastructure, however. Microsoft’s Windows Azure is an example.

applications, and may control such networking components as firewalls. Amazon Web Services EC2 is an example.