

Security and the Cloud: Security is Key as Enterprises Contemplate the Inevitable Move to Cloud Computing

Transcript of a BriefingsDirect Podcast on the state of security in cloud computing and what companies need to do to overcome fear, while reducing risk.

Listen to the podcast. Download the podcast. Find it on [iTunes/iPod](#) and [Podcast.com](#). Download the transcript. Learn more. Sponsor: [Hewlett Packard](#).

Offer: Get a free copy of Cloud for Dummies courtesy of Hewlett Packard by going to: www.hp.com/go/cloudpodcastoffer

Dana Gardner: Hi, this is [Dana Gardner](#), principal analyst at [Interarbor Solutions](#), and you're listening to BriefingsDirect.



Today, we present a sponsored podcast discussion on caution, overcoming fear, and the need for risk reduction on the road to successful [cloud computing](#).

In order to ramp up cloud-computing use and practices, a number of potential security pitfalls need to be identified and mastered. Security, in general, takes on a different emphasis, as services are mixed and matched and come from a variety of internal and external sources.

So, will applying conventional security approaches and best practices be enough for low risk, high-reward cloud computing adoption? Is there such a significant cost and productivity benefit to cloud computing that being late or being unable to manage the risk means being overtaken by competitors that can do cloud successfully? More importantly, how do companies know whether they are prepared to begin adopting cloud practices without undo risks?

To help us better understand the perils and promises of adopting cloud approaches securely, we're joined by three security experts from [Hewlett-Packard \(HP\)](#). Please join me in welcoming [Archie Reed](#), he's an HP Distinguished Technologist and Chief Technologist for Cloud Security. Welcome, Archie.

Archie Reed: Hello, Dana. Thanks.

Gardner: We're also joined by [Tim Van Ash](#), director of [software-as-a-service \(SaaS\)](#) products at HP Software and Solutions. Welcome, Tim.

Tim Van Ash: Good morning, Dana.

Gardner: Also, David Spinks, security support expert at HP IT Outsourcing. Welcome, David.

David Spinks: Good morning.

Gardner: Let's start with you, Tim, if you don't mind. Of course, any discussion nowadays that involve cloud computing really deserves a definition. It's a very amorphous subject these days. We're talking about cloud computing in terms of security and HP. How do you put a box around this? What are the boundaries?

Van Ash: It's a great question, Dana, because anything associated with the Internet today tends to be described as cloud in an interchangeable way. There's huge confusion in the marketplace, in general, as to what cloud computing is, what benefits it represents, and how to unlock those benefits.



Over the last two years, we've really seen three key categories of services emerge that we would define as cloud services. The first one is [infrastructure as a service \(IaaS\)](#). [Amazon's EC2](#) or [S3](#) services are probably some of the best known. They're there to provide an infrastructure utility that you can access across the Internet, and run your applications or store your data in the cloud, and do it on a utility-based model. So, it's a pay-per-use type model.

If we look at [platform as a service \(PaaS\)](#), this is an area that is still emerging. It's all about building applications in the cloud and providing those application-development platforms in the cloud that are [multi-tenant](#) and designed to support multiple customers on the same platform, delivering cost efficiencies around development, but also reducing the amount of development required. Many of the traditional tiers from data persistency and other things are already taken care of by the platform.

The last area, which is actually the most mature area, which started to emerge about 10 years ago, is SaaS. Great examples of this are [Salesforce.com](#), HP's partner [NetSuite](#), and, obviously, HP's own Software-as-a-Service Group, which delivers IT management as a service.

Gardner: When we're talking about applying security to these definitions, are we talking about something very specific in terms of crossing the wire? Are we talking about best practices? Are we talking about taking a different approach in terms of a holistic and methodological understanding of security vis-à-vis a variety of different sources? Help us better understand what we mean when we apply security to cloud.

Different characteristics

Van Ash: Once again, it's a great question, because you see very different characteristics, depending on the category of the service. If it's IaaS, where it's really a compute fabric being provided to you, you're responsible for the security from the operating system, all the way out.

You're responsible for your network security, the basic operating system security, application security, and the data security. All of those aspects are within your domain and your control, and there really is a large difference between the responsibility of the consumer and the responsibility of the provider. The provider is really committing to providing a compute fabric, but they're not committing, for the most part, to provide security, although there are IaaS offerings emerging today that do wrap aspects of security in there.



For PaaS, the data persistency and all those elements, for the most part, are black box. You don't see that, but you're still responsible for the application-level security, and ensuring that you're not building vulnerabilities in your code that would allow things like [SQL injection](#) attacks to actually [mine the data](#) from the back-end. You see more responsibility put on the provider in that environment, but all the classic application security vulnerabilities, very much lie in the hands of the consumer or the customer who is building applications on the cloud platform.

With SaaS, more of the responsibility lies with the provider, because SaaS is really delivering capabilities or business processes from the cloud. But, there are a number of areas that you're still responsible for, i.e., user management in ensuring that there are perfect security models in place, and that you're managing entry and exit of users, as they may enter a business or leave a business.

You're responsible for all the integration points that could introduce security vulnerabilities, and you're also responsible for the actual testing of those business processes to ensure that the configurations that you're using don't introduce potential vulnerabilities as well.

Gardner: Archie Reed, it sounds as if there is a bigger task here. We had to evaluate whether the provider has instituted sufficient security on their end. We have to be concerned about what we do internally. It sounds like there is a larger security wall to deal with here. Is that the case when we look at cloud?

Reed: Absolutely. One of the key things here is, if you take the traditional IT department perspective of whether it's appropriate and valuable to use the cloud, and then you take the cloud security's perspective -- which is, "Are we trusting our provider as much as we need to? Are they able to provide within the scope of whatever service they're providing enough security?" -- then we start to see the comparisons between what a traditional IT department puts in play and what the provider offers.



For a small company, you generally find that the service providers who offer cloud services can generally offer -- not always, but generally -- a much more secure platform for small companies, because they staff up on IT security and they staff up on being able to respond to the customer requirements. They also stay ahead, because they see the trends on a much broader scale than a single company. So there are huge benefits for a small company.

But, if you're a large company, where you've got a very large IT department and a very large security practice inside, then you start to think about whether you can enforce firewalls and get down into very specific security implementations that perhaps the provider, the cloud provider, isn't able to do or won't be able to do, because of the model that they've chosen.

That's part of the decision process as to whether it's appropriate to put things into the cloud. Can the provider meet enough or the level of security that you're expecting from them?

Suitable for cloud?

The flip side of that is from the business side. Are you able to define whether the service value that's being provided is appropriate, and is the data going into the cloud suitable for that cloud service?

By that, I mean, have we classified our data that is going to be used in this cloud service regardless of whether it's sitting in a PaaS or SaaS? Is it adequately protected when it goes into the cloud, such that we can meet our compliance objectives, our governance, and the risk objectives? That ultimately is the crux of the decision about whether the cloud is secure enough.

Gardner: Let's go to David Spinks. It sounds as if we almost fundamentally need to rethink security, because we have these different abstractions now of sourcing. We have to look at access and management control, what should be permeable and perhaps governed at a policy level across the boundaries.

I suppose there are also going to be issues around dynamic shifting, when processes and suppliers change or you want to move from a certain cloud provider to another over time. Do you think it's fair that we have to take on something as dramatic as rethinking security?

Spinks: That's absolutely right. We've just been reviewing a large energy client's policies and procedures. While those policies, procedures, and controls that they apply on their own systems are relevant to their own systems, as you move out into an outsourcing model, where we're managing their technology for them, there are some changes required in the policies and procedures. When you get to a cloud services model, some of those policies, procedures, and controls need to change quite radically.



Areas such as audit compliance, security assurance, forensic investigations, the whole concept of [service-level agreements \(SLAs\)](#) in terms of specifying how long things take have to change. Companies have to understand that they're buying a very standard service with standard terms and conditions.

Before they were saying, "Our systems have to comply with this policy, and you have to roll out patches." In a cloud services environment, those requirements no longer apply. They have very standard terms and conditions imposed on them by the cloud providers.

Gardner: So, while we need to think out how we approach cloud, particularly when we want a high level of security and a low level of risk, the rewards for doing this correctly can be rather substantial.

Tim Van Ash, what are the balances here? Who is in the role of doing the cost-benefit analysis that can justify moving to the cloud, and therefore recognize the proper degree of security required?

Pressure to adopt

Van Ash: It's a very interesting question, because it talks to where the pressures to the adoption of cloud are really coming from. Obviously, the current economic environment is putting a lot of pressure on budgets, and people are looking at ways in which they can continue to move their projects forward on investments that are substantially reduced from what they were previously doing.

But, the other reason that people are looking at it is just agility, and both these aspects – cost and agility -- are being driven by the business. Going back to the earlier point, these two factors coming from the business are forcing IT to rethink how they look at security and how they approach security when it comes to cloud, because you're now in a position where many of your intellectual property and your physical data and information assets are no longer within your direct control.

So what are the capabilities that you need to mature in terms of governance, visibility, and audit controls that we were talking about, how do you ramp those up? How do you assess partners in those situations to be able to sit down and say that you can actually put trust into the cloud, so that you've got confidence that the assets you're putting in the cloud are safeguarded, and that you're not potentially threatening the overall organization to achieve quick wins?

The challenge is that the quick wins that the business is driving for could put the business at much longer-term risk, until we work out how to evolve our security practices across the board.

Gardner: We've been dealing with security issues for many years. Most people have been doing [wide area networking](#) and using the Internet for decades. Archie Reed, are the current technologies sufficient? Is the conventional approach to security all right? Or, do we need to recognize that we, one, either need new types of technologies, or two, primarily need to look at this from a process, people, and methodology perspective?

Reed: That's a long question. Tying into that question, and what Tim was just alluding to, most customers identify cost and speed to market as being the primary drivers for going or looking at cloud solutions.

Just to clarify one other point, in this discussion so far, we've been primarily talking about cloud providers as being external to the company. We haven't specifically looked at whether IT inside a large organization may be a cloud provider themselves to the organization and partners.

So, sticking with that model, alongside the cost and speed to market, when customers are asked what their biggest concerns are, security is far and away the number one concern when they think about cloud services.

The challenge is that security, as a term, is arguably a very broad, all-encompassing thing that we need to consider. When we start to look at what the cloud providers offer in terms of security, and whether our traditional security approaches are going to meet the need, we find a lot of flaws.

What we need to do is take some of that traditional security-analysis approach, which ultimately we describe as just a basic risk analysis. We need to identify the value of this data -- what are the implications if it gets out and what's the value of the service -- and come back with a very simple risk equation that says, "Okay, this makes sense to go outside."

If it goes outside, are the processes in place to say who can have access to this system, who can perform actions on the service that's providing access to that data, and so on.

Traditional approaches

Our traditional approaches lead us to the point where we can then decide what the appropriate actions are that we need to put in play, whether they be training for people, which is very important and often forgotten when you're using cloud services. Then decide the right processes that need to be used, whether they be implemented by people or automated in any way. Then ultimately, down to the actual infrastructure that needs to be updated, modified, or added, in order to get to the level of security that we're looking for. Does that make sense?

Gardner: Yeah. It sounds as if it's not so much a technological issue, as something for the architects and the operational management folks to consider, a fairly higher-level perspective is needed.

Reed: Arguably yes. Again, it depends what you're putting into the cloud. There are certain things where you may say, "This data, in and of itself, is not important, should a breach occur. Therefore, I'm quite happy for it to go out into the cloud."

An example may be if you have a huge image database, for example, a real estate company. The images of the properties, in and of themselves, hold little value, but the amount of storage and

bandwidth that you as a company have got to put into play to deliver that to your customers is actually quite costly and may not be something that your IT department has expertise in.

A cloud provider may be able to not only host those images and deliver those images on a worldwide basis, but also provide extra image editing tools, and so on, such that you can incorporate that into an application that you actually house internally, and you end up with this hybrid model. In that way, you get the best of both worlds.

Generally, when we talk to people, we come back to the risk equation, which includes, how much is that data worth, what are the implications of a breach, and what is the value of the services being provided. That helps you understand what the security risk will be.

Gardner: So, if you start to componentize your workloads and understand more about what can be put on a scale of risk, you can probably reduce your costs dramatically, if you do it thoughtfully, and therefore gain quite a competitive advantage.

Reed: Absolutely. We have a vision at HP. It's generally recognized out there as "[Everything-as-a-Service](#)." An IT department can look at that and take things down to those componentized levels, be it based on a bit of data that needs to be accessed, or we need to provide this very broad service. In that way, they can also help define what is appropriate to go into the cloud and what security mechanisms are necessary around that. Does the provider offer those security mechanisms?

Gardner: Is it important to get started now, even for companies that may not be using cloud approaches very much yet to fully engage on this? Is it important and beneficial for them to start thinking about the processes, the security, and the risk issues? Let me pass that to David Spinks.

Next big areas

Spinks: The big areas that I believe will be developed over the next few years, in terms of ensuring we take advantage of these cloud services, are twofold. First, more sophisticated means in data classification. That's not just the conventional, restricted, confidential-type markings, but really understanding, as Archie said, the value of assets.

But, we need to be more dynamic about that, because, if we take a simple piece of data associated with the company's annual accounts and annual performance, prior to release of those figures, that data is some of the most sensitive data in an organization. However, once that report is published, that data is moved into the public domain and then should be unclassified.

What we're finding is that many organizations, once they classify a piece of data as confidential or secret, it stays at that marking, and therefore is prohibited from moving into a more open environment.

We need not just management processes and data-classification processes, but these need to be much more responsive and proactive, rather than simply reacting to the latest security breach. As we move this forward, there will be an increased tension to more sophisticated risk management tools and risk-management methodologies and processes, in order to make sure that we take maximum advantage of cloud services.

Gardner: Tim Van Ash, as companies start to think about this and want that holistic perspective, does adopting SaaS and consuming those applications as services provide a stepping-stone? Is this a good validation point?

Van Ash: Going back to the point that David was just making, it comes down to which processes you're putting into the cloud and the value tied to those processes.

For example, Salesforce.com has been very successful in the SaaS market. Clearly, they're the leader in [customer relationship management \(CRM\)](#) in the cloud today. The interesting thing about that is, the information they store on behalf of customers are customer data and prospect data, things that organizations guard very carefully, because it represents revenue and bookings to the organization.

If you look at how the adoption has occurred, it started out with small to medium companies for whom speed was often more important than the financial security, but it has now very much moved into the enterprise. The level of data being held within an organization like Salesforce is extremely sensitive. Salesforce has had to invest tremendous amounts of time and energy in protecting their systems over the years.

Likewise, if we look at our own SaaS business within HP, not only do we go through external audit on a regular basis, but we're applying a level of security discipline. It could be [SAS 70 Type II](#) around the data centers and practices, or being certified to an ISO standard, whether it be [27001](#) or one of the earlier variations of that. Cloud providers are now having to adhere to a very rigorous set of guidelines that, arguably, customers don't apply to the same level around their information internally.

The big reason for that is that when you run element as a service, you have to build supporting elements around that service. It's not a generic capability that exists across the entire business. So, there's a lot more focus placed on security from the SaaS model than maybe would have been applied to some of those elements within smaller to medium organizations, and, certainly, in some of the non-core functions in the enterprise.

Gardner: I assume that the ways in which an organization starts to consume SaaS and the experiences they have there does set them up to become a bit more confident in how to move forward toward the larger type of cloud activity.

Fear, uncertainty, doubt

Van Ash: That's a great point, Dana. Typically, what we see is that organizations often have concerns. They go through the fear, uncertainty, and doubt. They'll often put data out there in the cloud in a small department or team. The comfort level grows, and they start to put more information out there.

At the same time, going back to the point that both Dave and Archie were making, you need to evolve your processes, and those processes need to include the evaluation of the risk and the value of the information and the intellectual property that you're placing out there.

Spinks: One of the observations I've had talking with a lot of customers about so far, some big customers and small, is they're experiencing this situation where the business units are pushing internally to get to use some cloud service that they've seen out there. A lot of companies are finding that their IT organizations are not responding fast enough such that business units are just going out there directly to a cloud services provider.

They're in a situation where the advice is either ride the wave or get dumped, if you want an analogy. The business wants to utilize these environments, the fast development testing and launch of new services, new software-related solutions, whatever they may be, and cloud offers them an opportunity to do that quickly, at low cost, unlike the traditional IT processes.

But, all of these security concerns often get lost, because these things that they want to work on are very arguably entrepreneurial in nature and move very quickly to try to capture business opportunities. They also may require partners to engage quickly and easily, and getting holes through firewalls and getting approvals can take months, if not quarters, in the traditional model. So, there is a gap in the existing IT architectural processes to implement and support these solutions.

That's what IT has got to deal with, if we focus on their needs for a minute. If they don't have a policy, if they don't have a process and advertise that within an organization, they will find that the business units will get up on that wave and just ride away without them.

Van Ash: We do see enterprises are being somewhat cautious, when they're applying it. As Archie was saying right upfront, you see a different level of adoption, a different level of concern, depending on the nature of the business and the size of the business. Many enterprises today looking for quick wins are leveraging elements like IaaS to reduce their costs around testing and development. These are areas that allow them to get benefit, but doing it in a way that is managing their risk.

Gardner: It sounds as if we need to get this just right. If we drag our feet as an organization, some of the business units and developers will perhaps take this upon themselves and open up the larger organization to some risk. On the other hand, if we don't adopt at a significant pace, we

risk a competitive downfall or downside. If we adopt too quickly and we don't put in the holistic processes and think it through, then we're faced with an unnecessary risk.

I wonder, is there a third party, some sort of a neutral certification, someone or some place an organization can go to in order to try to get this just right and understand from lessons that have been learned elsewhere?

Efforts underway

Reed: We would hope so. There are efforts underway. There are things, such as the Jericho Forum, which is now part of [The Open Group](#). A group of CIOs and the like got together and said, "We need to deal with this and we need to have a way of understanding, communicating, and describing this to our constituents."

They created their definition of what cloud is and what some of the best practices are, but they didn't provide full guidelines on how, why, and when to use the cloud, that I would really call a standard.

There are other efforts that are put out by or are being worked on today by [The National Institute of Standards and Technology](#), primarily focused on the U.S. public sector, but are generally available once they publish. But, again, that's something that's in progress.

The closest thing we've got, if we want to think about the security aspects of the cloud, are coming from the [Cloud Security Alliance](#), a group that was formed by interested parties. HP supported founding this, and actually contributed to their initial guidelines.

Essentially, it lays out 15 focus areas that need to be concentrated on in terms of ensuring a level of security, when you start to look at cloud solutions. They include things like information lifecycle management, governance, enterprise risk management, and so on. But, the guidelines today, knowing of course that these will evolve, primarily focus on, "Here is the best practice, but make sure you look at it under your own lens."

If we're looking for standards, they're still in the early days, they're still being worked on, and there are no, what I would call, formal standards that specifically address the cloud. So, my suggestion for companies is to take a look at the things that are underway and start to draw out what works for them, but also get involved in these sorts of things.

Gardner: I just want to make sure I understood the name. Was it Jericho, the project that's being done by The Open Group?

Reed: [Jericho Forum](#) was the group of CIOs who essentially put together their thoughts, and then they've moved it under The Open Group auspices.

The Jericho Forum and the Cloud Security Alliance, earlier this year, signed an agreement to work together. While the Jericho Forum focused more on the business and the policy side of things, the Cloud Security Alliance focused on the security aspects thereof.

Gardner: What is HP specifically doing to advance the safe and practical use of cloud services, working I would imagine in concert with some of these standards, but also looking to provide good commercial services?

HP's efforts

Reed: There are many things going on to try and help with this. As I said, we were involved in the formation of the CSA, and we were involved, and are still involved, in helping write the guidance for critical areas, a focus in cloud computing, and the next generation. We are, through our EDS folks, directly involved with the Jericho Forum, and bringing those together.

We also have a number of tools and processes based on standards initiatives, such as [Information Security Service Management \(ISSM\)](#) modeling tools, which incorporate inputs from standards such as the ISO 27001 and SAS 70 audit requirements -- things like the [payment card industry \(PCI\)](#), [Sarbanes-Oxley \(SOX\)](#), European Data Privacy, or any national or international data privacy requirements.

We put that into a model, which also takes inputs from the infrastructure that's being used, as well as input based on interviews with stakeholders to produce a current state and a desired or required state model. That will help our customers decide, from a security perspective at least, what do I need to move in what order, or what do I need to have in place?

That is all based on models, standards, and things that are out there, regardless of the fact that cloud security itself and the standards around it are still evolving as we speak.

Gardner: Tim Van Ash, did you have anything further to offer in terms of where HP fits into this at this early stage in the secure cloud approach?

Van Ash: Yeah. In addition to the standards and participation that Archie has talked about, we do provide a comprehensive set of consulting services to help organizations assess and model where they are, and build out roadmaps and plans to get them to where they want to be.

One of the offerings that we've launched recently is [Cloud Assure](#). Cloud Assure is really designed to deal with the top three concerns the enterprise has in moving into the cloud.

Security, obviously, is the number one concern, but the number two and three concerns are performance and availability of the services that you're either consuming or putting into the cloud.

Cloud Assure is designed and delivered through the HP Software-as-a-Service Group, so that its a way that organizations can assess potential cloud services that they want to consume for those security issues, so that they know about it before they go in. This can help them to choose who is the right provider for them. Then, it's designed to provide ongoing assessment of the provider over the life of the contract, to ensure that they continue to be as secure as required for the type of information and the risk level associated with it.

The reason we do it through SaaS is to enable that agility and flexibility of those organizations, because speed is critical here. Often, the organizations aren't in a position to put up those sorts of capabilities in the timeframe the business is looking to adopt them. So, we're leveraging cloud to enable businesses to leverage cloud.

Gardner: David Spinks, are there areas where success is being meaningfully engaged now? Are there early adopters? Where are they? And, are they really getting quite a bit of productivity from moving certain aspects or maybe entire sets of IT functions or business functions to the cloud?

Moving toward cloud

Spinks: We're seeing some of the largest companies in the world move towards cloud services. You've got the likes of [Glaxo](#) and Coca-Cola, who are already adopting cloud services and, in effect, learning by actual practical experience. I think we'll see other large corporations in the world move towards the adoption of cloud, because obviously they spend the most on IT and, therefore, have got the most to gain from incremental savings.

The other key technology that we'll see emerge from one of the issues in cloud computing in the whole area of personal authentication, authorization, and federated access is this concept called [Role-Based Access Control \(RBAC\)](#).

There are a number of clients who are talking to us about how we might use our experiences with some of the largest corporations and government agencies in the world in terms of putting more robust authentication processes in place, allowing our largest clients to collaborate with their customers and their partners.

One of the key technologies there, and obviously one of the key technologies that Jericho have been pushing for years, is much more robust identity management and authentication, including technologies such as two-factor authentication and managed public key infrastructure (MPKI). I would prophesize that we're going to see an explosion in the use of those technologies, as we move further and further into the cloud.

Gardner: Well, very good, I'm afraid we're about out of time. We've been having a discussion about overcoming fear -- caution and the need for risk reduction on the road to successful cloud computing. Our panelists have been Archie Reed, HP Distinguished Technologist and Chief Technologist for cloud security. I certainly appreciate your input Archie.

Reed: Thank you very much, Dana.

Gardner: Tim Van Ash, director of SaaS products at HP Software and Solutions. Thank you, Tim.

Van Ash: Thanks very much, Dana.

Gardner: And David Spinks, security support expert at HP IT Outsourcing. Thank you, David.

Spinks: You're very welcome.

Gardner: This is Dana Gardner, principal analyst at Interarbor Solutions. You've been listening to a sponsored BriefingsDirect podcast. Thanks, and come back next time.

[Listen](#) to the podcast. [Download](#) the podcast. Find it on iTunes/iPod and Podcast.com. Download the transcript. Learn more. Sponsor: [Hewlett Packard](#).

Offer: Get a free copy of Cloud for Dummies courtesy of Hewlett Packard by going to: www.hp.com/go/cloudpodcastoffer

Transcript of a BriefingsDirect Podcast on the state of security in cloud computing and what companies need to do to overcome fear, while reducing risk. Copyright Interarbor Solutions, LLC, 2005-2009. All rights reserved.