# The Upside and Downside of Security in the Cloud
# Transcript

## Part 1: Cloud Services; Security Risks

**Julia Allen:** Welcome to CERT's Podcast Series: Security for Business Leaders. The CERT program is part of the Software Engineering Institute, a federally-funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org.

Show notes for today's conversation are available at the podcast website.

My name is Julia Allen. I'm a senior researcher at CERT, working on security governance and software assurance. Today I'm pleased to welcome Tim Mather, Vice President and Chief Security Strategist for RSA Security Conference. Today Tim and I will be discussing kind of a hot topic these days, cloud computing and some of the upside and downside if you will — the risks and opportunities it creates when it comes to security. So welcome Tim, really glad to have you with us today.

**Tim Mather:** Oh, it's great to be with you Julia. Thank you.

**Julia Allen:** So there is a good deal of hype around this topic, around the performance and cost benefits of cloud computing. It seems to have created quite a bandwagon effect. So just to set the stage, could you say a little bit about what it is, from your point of view, and why you feel it's gaining so much traction these days?

**Tim Mather:** Sure. Let's actually start with the second part first because that's the easier aspect. And why is cloud computing gaining so much traction? And likewise, why is there so much hype about it? And the interest is really around the economics of it. Companies are being lured in by promises of cost savings and with the economy in its current rather poor state, cost savings is definitely of interest to business. So that's what has caught people's attention and it's really around a new economic model to help drive costs down. And that's what's fueling this.

Now for the first part of your question then, what is this — this being cloud computing, really comprised of really three services that are out there? One of them is referred to as Infrastructure as a Service. A very prominent example of this would be Amazon Web Services. And Infrastructure as a Service is where you essentially are renting an entire infrastructure — network, servers — and you provide your own applications then, and you get all of this as a package. And again the idea is the cost savings to do this so that you are basically turning what previously had been CapEx, or capital expenditures, into OpEx, or operational expenditures. And you have a way to, if you will, burst without having a lot of capital outlay. So it's very flexible on that.

So that's Infrastructure as a Service. You have, again, Amazon Web Services being a prominent example. And storage in the cloud is a very prominent, I'll say, application, so to speak, of Infrastructure as a Service.

The second component, sort of moving up a stack, if you will — think of the OSI model and the stack there. So moving up from Infrastructure as a Service, you have what's known as Platform as a Service or PaaS. And with PaaS, what you are essentially renting is a third-party application that is developed on an open platform by one of the cloud providers. The two most prominent examples of this are salesforce.com, with their force.com platform and Google's App Engine.

So here it's a platform that again the providers are providing but essentially their target really is application developers who develop on that platform. And then you, as a prospective customer, can go get this third-party application.

And then, if you will, at the top of the stack is Software as a Service, or SaaS, as it's known. And the best known example here is salesforce.com. And this is where you're renting, if you will, purely an application on that, and the underlying platform, the underlying infrastructure, all of that is taken care of for you. And so again, it's purely a software service that you're doing and the other aspects of it are taken care of for you.

Again, with Infrastructure as a Service, sort of at the lower level, you're renting the network but you have to take care of some of the aspects of networking. You have to take care of the systems or the servers, so to speak, and of course you provide your own applications.

So Infrastructure as a Service, Platform as a Service, and Software as a Service, are the three major components around cloud computing. Now none of that exists in a vacuum and there are various management services that are used to facilitate cloud computing. But think of it at the moment as Infrastructure as a Service, PaaS and SaaS.

Julia Allen: So but would it be too simple conceptually to say that for me, as a user of those kinds of services, that I could access these services, from a using point of view, as though they were within my own shop or within my own infrastructure? Is it that seamless?

Tim Mather: Well it can be that seamless, yes absolutely, especially for Software as a Service, it may be. So for Infrastructure as a Service you may have a little bit more that you need to do. But if you're an enterprise customer, using as an example salesforce.com, yes, it is that simple for you absolutely.

And I guess Julia we're talking primarily about enterprise customers here, as opposed to consumer versions of cloud computing, such as Gmail, Picasa, even Hotmail, etc., etc.

Julia Allen: Right. So you're talking about business organizations, as opposed to, for example, home users.

Tim Mather: That's correct.

Julia Allen: Right. So given that we're on a security podcast series, we would be remiss if we didn't turn our attention to those particular aspects. So given — obviously there's all kinds of operational issues and interface issues to deal with — but for security in particular, what do you see in terms of how the security risks differ when using services and applications in the cloud compared to more traditional? And maybe you could say a little bit about if there are different threats to take into account.

Tim Mather: So good question. It's interesting to note that in spite of all of the hype — and there is quite a bit of hype about cloud computing out there – the number one source of concern from IT professionals and business unit executives about using cloud computing is with regard to security. Now there hasn't been a great deal articulated so far about what does that security concern actually entail but consistently in various polls that are out there — IDC has put them out and several other organizations have as well — it seems to be that security is the major concern.

So when you ask that question, it's important to note that there is a difference between public clouds and private clouds. So a private cloud being an organization's own, effectively internal to that organization, their own cloud infrastructure. Now that private infrastructure may be hosted actually within the facilities of that organization or it may be outsourced to a third-party provider but that cloud infrastructure, that private cloud infrastructure, is dedicated to that particular organizational entity, whatever that may be.

Julia Allen: So that means, if you're talking about private cloud, that means your operational services or applications are not mixed with someone else, right?

Tim Mather: Absolutely. And so when we're talking about cloud computing, generally the reference is not to private clouds but to public clouds. And again the lure of cloud computing is around the economics of it. And the only way you get to those economics is through a shared environment. So it's important to note with cloud computing that everything is shared. If you're doing Infrastructure as a Service, you're sharing those network services, those network resources, with other customers. If you're doing PaaS, you are sharing that platform with not only other applications but with other customers. If you're doing SaaS, Software as a Service, you are sharing that application with other customers.

So it is not only shared — which is again how you get to the economics of it — but your data is often, when we're talking about either PaaS or SaaS, your data is co-mingled with other customers. Some of those customers may, in fact, be your competitors. So that's how you really get there.

And the primary security concern that that draws out is just that. It's co-mingled data, it's co-mingled resources, which from a security perspective brings up a rather fundamental problem of where is your trust boundary or trust boundaries? What is under your control versus what is under the control of a third party; what is that third party actually doing; and whatever their stating, do you actually trust them to do what it is they're saying? And after the fact, from an audit perspective, what

assurance do you have and do your auditors have that those security measures were in fact carried out?

Julia Allen: Well it seems to me Tim that you would actually have to redefine what you mean by control or am I missing the point?

Tim Mather: No, you're not missing the point at all. That's exactly right. So we would like to think that the controls themselves are going to be the same whether it's in cloud computing or a more traditional topology. That is somewhat up in the air right now as people try and get their hands around cloud computing and figure out are those controls the same? The bigger question is if the controls are the same — and many of them are but it's not clear that all of them are — but for those that where there is, I'll say, consensus that the controls are the same, it's who actually has responsibility for those controls? And again how do you have assurance that those controls are being carried out properly or as stated by the provider?

Julia Allen: So have you seen any cases yet where there's been a major security incident against a cloud service provider that affects multiple clients?

Tim Mather: Yes. There are two of them that are public knowledge now. One of them is with regards to Amazon Web Services — and again Infrastructure as a Service — where customers of Amazon's Web Services have effectively been attacked by other customers who are malicious, not only from spam but other types of attacks.

Amazon Web Services hasn't really publicly acknowledged that but the Washington Post has made that available in a story that they did where they interviewed multiple customers and came out with that.

And the second one was with Google and their Google Apps in which information or documents that were shared inappropriately with other customers. So the co-mingling of data was not only for storage. It was co-mingling of information actually being shared in an unauthorized manner. So not clear that that was a deliberate attack. It certainly was a security compromise.

## Part 2: To Cloud or Not to Cloud

Julia Allen: Well this is going to provide us some real interesting fodder for teasing out and sorting through what kind of new issues and risks arise in this environment. You had started talking a little bit about the audit implications. So let's, if you wish, if you will, follow that thread for a while. So legal/audit implications, security, privacy, protecting data, things like PCI — how does that fit into this mix?

Tim Mather: Well quite a bit. In fact, you have cloud providers out there claiming to be — pick a regulatory framework — compliant, one of them being HIPAA. And I don't mean to pick on Amazon. I will use them as an example though. Amazon has a statement on their Amazon Web Services page, one of their major pages there, in which they imply that they are, "AWS is," HIPAA-compliant. Well that's not really true. The owners of the data who happen to be using Amazon Web Services have to

take specific actions themselves — that is the data owners — to maintain compliance with HIPAA. Now that particular problem is not unique to Amazon Web Services by any means. So any provider of Infrastructure as a Service has that problem.

There is another provider, a much smaller provider, which has come up with a statement that says to the effect that they ensure that their customers are PCI-compliant. Well again that's just not true at all. In fact, the owners of the data have to take specific action again to ensure that while maintaining that cloud provider's services that they do not lose their PCI compliance. So you're already seeing issues here around compliance, with the data.

With regards to privacy, there's several issues here. Jim Dempsey from the Center of Democracy and Technology has been rather forthright in some of the statements that he's made. As he put it, there's actually a loss of fourth amendment protection for United States entities who are using cloud services.

And the reason behind that statement is that if there is a legal order, whether it be from a court or otherwise, but a legal order to provide data that legal order does not have to be served on you, the owner of the data. It can in fact be served on the cloud provider and you, as the owner of the data, may not even know that the cloud provider was served with that legal order and has in fact turned over your data to whatever government agency or court is requesting that data.

So there are certainly issues around privacy from a data ownership perspective. There are also, of course, privacy concerns as we just noted with the Google mishap around the co-mingling of data and data being disclosed to other parties in an unauthorized manner.

So certainly concerns around compliance, concerns around privacy as well. There are no audit frameworks that are specific to cloud computing. For the moment, essentially what providers are doing is — I'll call it stretching — but they're using a SAS 70 (hopefully a SAS 70 Type 2 audit) to say that that is covering their service operations that are provided on behalf of customers. Now that's getting some pretty close scrutiny because again there are no audit criteria defined specifically for cloud computing. So what does a SAS 70 Type II really mean? Is it applicable? Are the audit controls that are hopefully being tested actually appropriate to a cloud computing environment? A lot of questions around that.

Julia Allen: So as you work, are out in the community working with your clients, what advice do you give them to be able to be able to perform an informed risk assessment or an informed decision process as they're considering potentially going down this path?

Tim Mather: Well a very good question. Let's come back to two other aspects here before we answer that because I think that they're really appropriate to your question. One of them is is the data that you are thinking of putting into the cloud sensitive or regulated data? And if the answer is no, then probably go ahead and

explore what services may be provided through whichever provider you're looking at — and again whether that's Infrastructure as a Service, PaaS or SaaS.

However, at this point in time, I haven't run across anyone who feels comfortable putting sensitive or regulated data into the cloud. That just doesn't seem to be there as far as a comfort level that the security and the audit aspects of that will stand up to scrutiny. So again if it's non-sensitive, non-regulated, go ahead and think about that.

The other thing is, to keep in mind is, I don't want to sound entirely negative here about cloud computing on that. It depends upon your frame of reference for a lot of the security controls that you're asking about on this. For many large enterprises who have the benefit of resources including technically competent, accomplished staffs that may be a good sized staff, the security capabilities of cloud providers for the most part probably don't meet those large enterprises — especially financial services which have fairly sophisticated information security programs, as well as audit and privacy programs that go along with that.

So that said, the perspective from many small and mid-size businesses (SMBs) is probably different. Many of those entities (SMBs) don't have the resources. They don't have the financial resources, they don't have the large, very competent staffs to actually have the sophisticated programs that larger enterprises do. And so for SMBs, what security is being offered by the cloud providers may in fact indeed be a step up the ladder as far as better security, better privacy protection that the provider is able to assure and provide to those companies than what the SMB is able to do on their own.

So it's important to keep that in mind, sort of where you're coming at this. What resources you have available, what staff you have, with what competency, to be able to make the decision on the point that you just asked.

So that said, I think again — is it sensitive, non-sensitive or regulated, non-regulated on the one hand?; and your perspective in terms of the SMB view versus the enterprise view, assuming that most SMBs don't put in the resources required for a really robust security program that most large enterprises do put in for a very robust security program. So that said, then we get to your security considerations.

Julia Allen: Right. Well I appreciate the distinction that you're making about both the sector that you're in, the kind of skills and competencies you have within the organization. I mean, it really comes down to mission/business objectives. And so if I was going to both assess risk and — I don't know if there's a concept of service level agreement when you enter into these kind of relationships. But what are some of the mechanisms that I can use to make sure that I'm protected?

Tim Mather: Well your choices unfortunately today are fairly limited. When it comes to SLAs, to be quite honest you're lucky if you even do get an SLA from many of the providers. And if you do get one, how meaningful is it? In many cases those so-called SLAs leave a lot to be desired. So in addition to the sensitive/non-sensitive, to the

SMB versus the enterprise viewpoint, there is also as we discussed earlier the private cloud versus public cloud perspective. And then very important to your question then is exactly what services are you thinking about using? Are you doing Infrastructure as a Service? Are you doing PaaS? Or are you doing SaaS?

And the reason why where you are in the stack, so to speak, becomes important is because the lower you are on the stack, so to speak — meaning if you were down at Infrastructure as a Service — then you have more responsibility for whatever security it is that you're looking for. Less security is actually provided by the Infrastructure as a Service provider.

Now as you move up to PaaS for example, you have less flexibility over the security because more of the security is provided by the platform provider. And therefore you have — you have less but you're hoping that they have more. And then when we get to SaaS of course, you have the least flexibility about the security controls and the most onus is on the application provider.

So another perspective that also has to be factored into your decision about what is it you're looking for? If I'm looking for SaaS and I go to a company — we'll use salesforce.com as an example simply because they're well-known — then I would be looking at a much longer checklist of hopeful security capabilities that salesforce.com is going to be providing for my organization than if I go to Amazon Web Services where much more of the onus is on me to provide those capabilities.

## Part 3: Tempering the Business Rush to "Just Use It"

**Julia Allen:** Okay. Those clarifications and distinctions are really helpful as we try to get our heads around some of the issues. So let's say that I looked out over the landscape, I talked to some of my peers, this seemed like a reasonable approach for either selected services at one or more of the levels that you described. Who are you typically finding in organizations are leading the charge to go to some form of cloud computing and what are some of the first steps they might be taking?

**Tim Mather:** So good question. Almost all of the people leading the charge, so to speak, towards cloud computing within enterprises tend to be business unit personnel. They are the ones who are looking at the promised cost savings and really getting excited about this. The security people are oftentimes being dragged along behind saying, "Wait, wait!"

**Julia Allen:** Yes, probably kicking and screaming. Right?

**Tim Mather:** Yes. "I haven't checked this out yet. Who are these people? What do they actually do?" So very definitely the business unit people are leading the efforts to actually use cloud services. And the security personnel are in a bit of a catch-up mode right now, trying to understand exactly what services are being provided. Again where are the trust boundaries? Who's responsible for actually providing what? What is the assurance out of that? Is that a third-party audit such as a SAS 70 framework? What about audit logs to assure that? All sorts of those decisions the security people

want to know to actually understand (a) what's going on and (b) how do they actually follow-up or who follows up to ensure that what the provider says is being done is in fact being done?

Julia Allen: Well are you finding that the security folks are even getting a voice in the decision process? As you said, cost is such a huge driver these days. Are security and privacy staff being asked about their thoughts about the risk exposure or the other things that need to be considered in terms of control, system of internal controls? Are the security folks getting asked about that?

Tim Mather: I think that they are for the most part simply because the CIOs themselves, who also get involved in these decisions themselves, have their own concerns with regards to cloud providers. Now security may not be their top priority. It may be for example availability. It may be interoperability of services or connecting your organizational infrastructure to the provider's infrastructure; how's that being done, etc.?

So the CIOs often are getting involved and therefore the security and the privacy people are also getting involved as well. I don't think that they're being left behind or they're not being left out of the decision entirely.

CIOs seem to, according to various polls that are out there, also have pretty strong concerns with regards to the security of the data, whatever data is being moved into the cloud. And just because it moves into the cloud, doesn't mean that that enterprise is off the hook for the controls around that data. They're still responsible for that. It's still their name, so to speak, that's going to be on any breach or any problem that occurs. And that does tend to focus people a little bit more on understanding exactly what controls are in place. How robust is the SLA? How is that actually measured?

Those sorts of discussions are indeed coming up and that is tempering the business rush to 'just use it', so to speak. "No, no, no. It's not 'just use it.' It's understand you want to use it but we, CIOs, CISOs, need to understand more about this before we just jump in with both feet."

Julia Allen: Well Tim, this has been great. I feel like we've just kind of touched the or described the tip of the iceberg. Do you have some other places that you'd refer our listeners for more information?

Tim Mather: Well one place I would start is Open Security Architecture and their website. They've done something rather interesting and try and look at cloud services and map those services against NIST 800-53 from an audit perspective. So that's certainly something that I think is worthwhile taking a look at as well.

But otherwise, I'm sad to say that it's fairly new obviously as far as not only cloud computing itself. But even newer to this is any really robust view or scrutiny of the security and audit considerations. And there's unfortunately not a whole lot out there at the moment. There are some things that have been put out but as far as anything

that is comprehensive, that is detailed, yet easy to read, gosh we're lacking that at the moment.

Julia Allen: Well that sounds like a great business opportunity to me.

Tim Mather: It is and I'm working on that. So I'll put in a plug here if I may. Myself and two colleagues in the high tech industry, one from Sun Microsystems and one from KPMG, are actually working on a book for O'Reilly to discuss exactly this. So we're working hard on that and we hope that that is available by Labor Day of this year.

Julia Allen: Excellent. Well we'll be posting your podcast well before then but we'll certainly add the link when you let me know it's available.

Tim Mather: Great.

Julia Allen: Well listen Tim, I so appreciate your time, your expertise, your perspective today. You have a nice, broad view of the landscape given your vantage point with RSA and with past roles I know you've held. So thanks very much for your time today.

Tim Mather: Thank you Julia. Great to chat with you.