



RUNAS RADIO



<http://www.runasradio.com>



Richard
Campbell

RunAs Radio is a weekly Internet Audio Talk Show for IT Professionals working with Microsoft products. The full range of IT topics is covered from a Microsoft-centric viewpoint.



Greg
Hughes

Text Transcript of Show #123
(Transcription services provided by [PWOP Productions](#))



Andy Malone Battles Security in the Clouds!
August 26, 2009



[Music]

Brandon Wenn: From runasradio.com, you're listening to RunAs Radio, the Internet audio talk show for IT professionals with Richard Campbell and Greg Hughes. This is Brandon Wenn, announcing show #123, with guest Andy Malone, recorded Saturday, August 22, 2009. RunAs Radio is produced each week by PWOP Productions, providing professional media and podcasting services online at pwop.com. You can follow the boys on Twitter at twitter.com/runasradio.

Richard Campbell: Thank you Brandon. You are listening to RunAs Radio and I am Richard Campbell, with me, as always, my co-host Greg Hughes.

Greg Hughes: Hey Richard, how are you?

Richard Campbell: I'm fine sir but then I'm not trying to sell my house, get married, move, my life is pretty calm compared to yours.

Greg Hughes: Wow, that's really saying something, come to think of it.

Richard Campbell: Well, I'm in the end of my renovation my friend. The new driveway is in with the heated driveway surface, so we're just about done, I'm getting normalized here.

Greg Hughes: Heated driveway surface? You never cease to amaze me, my friend.

Richard Campbell: I am never shoveling my driveway again.

Greg Hughes: You're weird in the best kind of way.

Richard Campbell: Yeah.

Greg Hughes: That's really cool, yeah you're right, I'm getting married in October, selling a house to move, travelling, work is crazy right now...

Richard Campbell: Yeah.

Andy Malone: Yet, it's been pretty insane but it's always good to be able to take a break and to sit down and do this.

Richard Campbell: Absolutely. Let's jump right to our guest now. Andy Malone, a motivated technical speaker, Most Valuable Professional, consultant, Microsoft speaker and recently, what was it, 2006 won Speaker Idol at TechEd IT forum in Europe.

Andy Malone: I did, good afternoon, good morning wherever you are yes, hi.

Richard Campbell: Yeah, time zones are funny thing my friend, we're scattered all over across the globe today, you're in the UK right?

Andy Malone: Yes, I'm in Scotland in the UK and at the moment it's about 4PM in the afternoon.

Richard Campbell: Yeah, it's bright early in the morning here on the West Coast of North America. So Andy, what have you been working on these days?

Andy Malone: Oh, quite a lot actually, I'm getting ready now for kind of gearing up for TechEd in November there and so I've got a couple of sessions going on there this year, maybe two, maybe three, I'm just waiting to hear for the final count.

Richard Campbell: Sure.

Andy Malone: We've also got the Cyber Crimes Security Forum, that's been going around Europe. We're really excited because we've got the first one come in to the United States in October and that's in Washington DC. So we've got a big three day event going on there, so that's going to be a lot of fun.

Greg Hughes: Cool. How do people find more information about the DC event?

Andy Malone: Probably, the company that's actually hosting our event in the US is a company called Global Knowledge, one of the big, big ones over there and you can go to their website at www.globalknowledge.com. So if you go there and have a look for the Cyber Crimes Security Forum, it will give you all the scoop.

Richard Campbell: Andy, we've been talking briefly before the show about Cloud Security, and this sort of stuff is coming to fruition now as we're getting in there and a lot of the problems here seem old like, when we we're doing shared computing or even the old application service router, we had this issue around who owns what and who's responsible for what, maybe give us your take, what do you think on Cloud Security?

Andy Malone: Sure. Well this is, I was just saying, is becoming a bit of a minefield. I was just telling Richard before we came on air that I was having a conversation with a lawyer yesterday and this guy was saying that cloud computing seems to be a complete minefield. As you just said there, the days of shared computing, where you had a contract for a company to store your data, you had a service level agreement and everything was fine, you knew exactly where that data was. Of course, now in the cloud, of



course the whole idea of cloud computing is that you could have companies like Google, Microsoft, whoever and they've got data centers all around the world so it could be that your data is replicated to data centers all around the world. So therefore, you've got to start saying, "Okay, well, who is responsible? What are the legal ramifications of it and are each country's laws different and so if you need to, who is basically, where does the buck stop and in such cases?" And this is the kind of things that we'll be talking about and unfortunately, there are not a lot of the answers out there at the moment, purely because this is fairly new. I mean I don't know what was your take on it Greg because this, in the States is becoming fairly big to you I think, isn't it?

Greg Hughes: Yeah, I mean this touches on so many different areas of expertise. You have compliance questions, you have legal questions, you have security questions and then there's just the classic IT infrastructure, how do we make this work? It seems to me this is one of those examples of things where there's a shift in the way that we do things and everybody has to get back together and have these conversations about, there's an awful lot of different kinds of requirements that go into using an infrastructure that crosses jurisdictional borders and physical borders and just geographic distribution, I think you're right it's an interesting question to think about.

Andy Malone: Sure, sure, I think the development, I mean I know that this year at TechEd, there are a couple of sessions on it. I, for myself, we're about to propose a session but it wasn't really insular. After I've submitted all of my sessions, I thought, "Hey, that's one session I should have actually submitted but this may be is something that I'll do in the future because I think it would be a very interesting area and certainly when we do the cyber crime event in DC, there's going to be a round table discussion on it. So that's going to be interesting to see what the take of the folks are?"

Greg Hughes: One of the buzz words that I haven't heard a whole lot in the past year and a half or maybe two years but it was the buzz word for awhile in the security circles was Deprematurization, remember that one?

Andy Malone: Yeah.

Greg Hughes: They're talking about, sort of we have our classic data center protected network -- a DMZ -- and then we have the internet or the unsafe network and thinking about things in terms of if we're going to be more and more distributed in our computing and really and truly having to let things just sort of be where they are, then we're going to have to redefine what the "perimeter" is?

Andy Malone: Sure, I mean look at Windows 7 and Windows R2, it's all kind of branch network, people are no longer in the office anymore. You've got technologies like Direct Access, the way that people are accessing data and externally, has really changed because obviously we have a much faster infrastructure. So it seems like we're just kind of catching up with all of this technologies but I guess this is what happens, anyway.

Greg Hughes: I'm curious, what did your lawyer friend that you were speaking to about the minefield, did you get into how is it defined? Why is it a minefield? What are some of the specific problems that we need to think about?

Andy Malone: Basically, they need to have a good service level agreement, so for example, if you have a service level agreement with Microsoft, you need to know that that particular agreement covers your data no matter where it lies. So for example, if your data is stored in a data center in Brazil, you need to make sure that it's covered by International Law, not just by Brazilian law or by United States law, there needs to be an international kind of law. Like for example in the United Kingdom, we have the Data Protection Act and that's recently being or been updated and to take into account cloud computing and also we have the Freedom of Information Act in the UK, so how does that kind of work in with Cloud computing? And I was actually thinking, I was talking to somebody the other day and we were saying, "Okay if we've got a bad user on our network and they've basically hacked the network, Cloud computing is going to be a minefield for forensics, how can you, who can go in to find the information? What security agency is responsible and how do we actually get the process of forensically looking at the evidence and he kind of just threw his arms up in the air, he says, "Well, this is something that needs to be discussed."

Greg Hughes: Sure, and then of course you have the sort of the general term cloud computing that gets applied to a variety of different types of infrastructure and without really talking about exactly how things are designed and exactly how the distributing, what we mean when we say "cloud computing", those security and compliance in business requirements questions may change substantially from one cloud computing discussion to another?

Andy Malone: Sure, sure, absolutely.

Richard Campbell: Guys, doesn't this get addressed when we simply set geographical boundaries on where our data can be stored, I mean



I've already read Microsoft talking about the fact that they're running multiple data centers in the US...

Greg Hughes: Right

Richard Campbell: So that a customer can say, "Hey, my data simply cannot leave the United States."

Greg Hughes: Absolutely and that's, the reason they're doing that is because they recognize the legal and especially for a lot of US companies, the compliance and the regulatory need to just not even have those questions come up at all.

Richard Campbell: This is an issue that I don't think is specific to cloud computing. As soon as I deal with a multinational entity of any kind, I have serious problems, international law is not clear.

Greg Hughes: Well it's not clear and it's not very enforceably strong.

Andy Malone: The problem is, there's no regulatory bodies either.

Richard Campbell: Right.

Andy Malone: Yes because you've got a company like Microsoft and they'll say, "Okay, we'll put your data in the cloud," and I mean every company, different, Amazon, Google, Microsoft, they've all got different service level agreements. So at the moment there is no kind of international regulatory body and I think this is something that's missing and it's something that will have to be addressed.

Greg Hughes: I think you can make an argument one way or the other is missing and that's a good thing or it's missing and that's a bad thing. It's going to be interesting to see what happens here but Richard your point is a good one. I mean we have to, when we make decisions, if you have a bank in the United States for example, keeping it inside the United States from a custodial control of data and information stand point is really important but I think kind of to, I'm sorry I'm thinking out loud here pretty in length, I'm sorry about that but what about the fact that if we're doing cloud computing, how do you really know where your data really is?

Andy Malone: Indeed.

Greg Hughes: I have an agreement or a contract or an SLA or whatever it is that says, "My data will reside inside the borders of the United States," but if the person running that Cloud infrastructure does have extensions outside the United States, then how do you, there's trust but then there's also, there's the model of trust, I trust my

infrastructure provider for cloud computing but then there's also the model that tends to come into any regulated environment and any reasonably secured business environment which is trust but verify, so how is that 'but verify' part work?

Richard Campbell: Well, it makes me think that, as soon as I get into any significant regulated industry, banking, health care, what have you, cloud computing is off the table. I look at my work I did around banking, I know you've done a lot more than I did and how crazy people got about SSL certificates inside the network and it's regulatory compliance, I mean, it's a minute thing and how hairy they were, I just thought that cloud computing is even an option.

Greg Hughes: Yeah, I mean if hey my blog is going to be running on a cloud computing infrastructure or if RunAs Radio is going to be distributed by a cloud computing infrastructure, the risk is so very, very low but we're talking about HIPAA or health care in the United States regulations or if you're talking about Gramm-Leach-Bliley in the US, there's another in Canada but banking regulations and certainly the UK has theirs but if you look at something else like let's just take e-commerce which has payment card industry standards, PCI compliance issues associated with it and the ability to be able to very specifically and with great, with absolute certainty say, this is exactly what's happening with this data and here's exactly where it's happening and here's the control I have over it. If you want to take credit cards that are United States credit cards and do business like that, you have to be PCI compliant. It would be really interesting to see what the story is and this is not a strict security thing, it's a compliance thing which is sort of an adjunct to security and legal issues but what does that mean, how do I do those types of transactions if I'm relying on a third party cloud computing infrastructure? If Amazon is using their own infrastructure, then they can make statements and attest to exactly what their infrastructure is doing for them but if I'm relying on Amazon's or Google's or Microsoft's infrastructure, what does that mean for me if I want to be able to process credit cards, for example?

Andy Malone: Sure and also which country's law prevails if there are issues.

Greg Hughes: Sure, sure.

Andy Malone: Is it the company or is it the country where the transaction's taking place, is it the country where the data's being stored?

Greg Hughes: And it may not be an "either/or," it might be a this plus this. It may be that there are laws even competing or overlapping or conflicting laws in different countries which may, you



can get into a situation where they could both prevail and that would be really interesting.

Richard Campbell: But I'm thinking that a company's perspective on this when they move to the cloud is that their onus on compliance now is in the service level agreement with the cloud provider. So in some ways, they've dropped their responsibility for securing their data in the lap of their provider so they don't have to deal with that. If there is a breach, they can now turn to the provider and say, "According to my Service Level Agreement, you were taking care of this, what happened?"

Greg Hughes: Well, maybe to a certain extent but Andy tell me what you think. All I know is if I have my credit card and I use an e-commerce provider and the e-commerce provider is relying on a third party infrastructure provider as far as where the system runs, that if my credit card and my identity gets stolen and I have damages as a result of that, I don't care that XYZ e-commerce company that I was interacting with, I don't care who they're backend provider is, I'm going after XYZ company and maybe that backend provider as well.

Andy Malone: That's right and the series of, a credit card, you see you've got organizations like Visa and Mastercard and American Express which are international organizations, so it doesn't really matter anywhere in the world you do a physical transaction, it comes back to a service level agreement with Visa, the actual credit card provider and because it's kind of an insurance scheme for the bank. So all you need to do is then go to the bank and say, "Hey look, I've been hacked in Venezuela and somebody in Venezuela is using my credit card but they don't care about that because they then send the law enforcement in that country," but the point is that because they have this international agreement, you are protected. At the moment cloud computing as an industry doesn't have that kind of protection so it's going to be interesting to see what's going to happen and where that's going to go.

Richard Campbell: So are we talking about some sort of international body that and obviously, UN related that's going to establish these standards?

Andy Malone: Yeah, I hope so. I mean I think it needs to be cleared up because the technology is moving very fast. Certainly, at the rate these data centers are going up in the last two years is immense but it all comes down to this at the end of the day is, "Okay, where is my data, who is responsible for it and if something, if somebody steals your data, how can I as an investigator forensically prove that this event has taken place because you don't know where your data is and there is a lot of confusion and this is something that needs to be cleared."

Greg Hughes: Do we need a regulatory body, Andy says yes, I say I hope not but that's a matter of opinion and probably gets into politics and a bunch of other stuff. You know from a pure forensic standpoint, to be able to do that work if there's a regulatory body that works, maybe it would make it easier. I think from a business stand point, it could be confusing or it could be difficult, ultimately there are ways to deal with this whether it's because the payment card industry, for example, decides to expand, change or alter their standards and directly address cloud computing, I mean I can't imagine that that won't happen in some way, shape or form but one thing is for sure, whether it's a regulatory body with international capabilities or if it's people who's just coming up with a good set of standards, ISO standards or whatever for doing things well and then adhering to them and then being able to prove they're adhering to them, we're going to have to make changes and just as we've had to over the last 20 years make big, big changes in the way that we do things. It's going to continue to happen as that core infrastructure evolves, we have to evolve with it.

Richard Campbell: I'm not that convinced, when I think about PCI regulations, I think they apply equally well to non-cloud scenarios as cloud scenarios, they really don't need any changing there.

Greg Hughes: They do, they do, I agree, they apply, however well, I'll go back to and then Andy tell us what you think, I don't want to speak for you that's for sure but my thought and I deal with PCI on a daily basis right, PCI standards, so is that, there's the trust but then there's the trust but verify and the real question there is how do I know for a fact that what I believe is happening in an infrastructure that I don't control. How do I know that that is true?

Andy Malone: That's really what it boils down to.

Richard Campbell: But in a PCI process, there are auditors right? So aren't we just saying that the PCI auto process has to happen within the cloud infrastructure?

Greg Hughes: The purpose of a PCI audit is to do a review and ensure and attest to the fact that the system, if you will, which could include a cloud portion of a system is sufficient and effective. Those are kind of my words but those are words that tend to be used, so in that case, if I am the bank for example right, that is processing transactions or taking processed transactions or issuing cards or I'm the business that's processing e-commerce transactions, my auditor is not going to go to my cloud computing provider and ask them questions, they may go to them but ultimately, my auditor is going to ask me, not



my cloud computing provider or I'm not going to rely on my cloud computing provider to speak for but maybe to back me up but ultimately, I have to attest as the business that's doing business with Visa and Mastercard or American Express or whoever, that what I am doing is sufficient and effective, those are kind of my words but those are words that tend to be used. So in that case, if I am the bank, for example, right, that is processing transactions or taking processed transactions or issuing cards or I'm the business that's processing e-commerce transactions, my auditor is not going to go to my cloud computing provider and ask them questions, they may go to them but ultimately, my auditor is going to ask me, not my cloud computing provider or I'm not going to rely on my cloud computing provider to speak for me but maybe to back me up but ultimately, I have to attest as the business that's doing business with Visa or Mastercard or American Express or whoever that what I am doing is sufficient and effective.

Andy Malone: Yeah and I agree with that. I'm saying, maybe not a regulatory body but maybe something just so that there is a safety net for people, just so as you said earlier, if for example HIPAA information has to be retained within the United States you go to the cloud provider and say, "Okay can you prove to me?" There needs to be some kind of evidence from the cloud provider saying, "Look, we guarantee that your data is going to remain in the United States and not have an accident and end up in China.

Greg Hughes: Right. Yeah, there are ways to do this, so Richard don't get me wrong, there are definitely ways to do this and there are ways to use cloud computing very, very effectively but what I wouldn't want to do is just simply blindly trust, again, without verification that what I believe to be true is actually true, does that make sense?

Richard Campbell: But I also think that as a customer of cloud computing, my cloud computing provider is going to say, "Hey, don't you worry, we're PCI compliant and we're going to go through this audit process for you, you're going to be able to see all this and I'm thinking that these sorts of verifications are one of the selling points for the average person moving to cloud.

Greg Hughes: It can be but I would have a hard time figuring out how a cloud computing backend infrastructure could be called PCI compliant. I mean that's kind of like saying my data center that I built with, is PCI compliant when really data centers maybe SAS 70 level 2 type of certification is what I'm interested there but payment card industry, PCI compliance is much more about the data. So I mean a PCI compliance, could it be conferred upon a cloud

computing infrastructure? I think that might be a bit of a stretch but a cloud computing provider can provide services in a way, especially if they do it 100% of the time, that could certainly facilitate being PCI compliant for the cloud computing customers.

Richard Campbell: I mean in the end...

Greg Hughes: So that means...

Richard Campbell: It's the software that's compliant right? The fact that it runs on a cloud infrastructure is a second thing, the two things that have to go together, though.

Greg Hughes: And even software is not compliant, PCI compliance is about the system right, which can include infrastructures, software, process, people, how do you do things, why do you things the way you do it, how is stuff stored, how is it moved? There's the data security standard in the PCI compliance but there's also more to it than just that.

Richard Campbell: All right, we've gone flying off the side here but I like it because it's an important element to it and honestly guys I'm still getting back to when I think of the major regulatory regimes I think nobody's going to be willing to even experiment with cloud computing because they don't want to push the boundaries of regulation.

Andy Malone: I think it's a very, very interesting subject and every time I've heard a conversation on cloud computing and security I just sit up and listen but it's the same, I mean every conversation I've heard is everything the same thing that we're going through today and I think at some point somebody needs to stand up and say, "Okay, that is the way that we're going to go, this is what we're going to do." I think it needs to be cleared up, it does have to be cleared up somehow.

Greg Hughes: So Andy I guess one thing that crosses my mind, I'm curious what, you know about cloud computing and sort of what's available and maybe conversation that you've had but am going to divide cloud computing in to two sort of big chunks, right? One of them is cloud computing as a service that I can buy right? So I go to Amazon or I go to Microsoft or I go to Google and I buy, I don't have the infrastructure but the other one is really leveraging the power of cloud computing and all of that infrastructure and the technology that goes into that but I still exercise control over that because I'm a company that is going to sort of build my own cloud, does that makes sense?

Andy Malone: Yes, yes.



Greg Hughes: Now in that case, the security and compliance questions are substantially different in terms of tackling them because I can exercise much more control.

Andy Malone: Because you have control. Exactly.

Greg Hughes: So I think it's possible to take advantage of the technological and business benefits of cloud computing in ways that where for some business it may be very difficult to be able to use the classic ASP model of infrastructure providing...

Andy Malone: True.

Greg Hughes: Because in the past, it has been a little bit different but to be able to exercise that level of control so that you can have verification that things really are happening the way that you want them to.

Andy Malone: True and I'm sure, in a years time, or a year or so, we'll come back and have this conversation and it would all be sorted out because I have a feeling that this will be the year they sort this out.

Richard Campbell: Okay, Andy, you're an optimist. Greg, in your second scenario there, aren't you talking about me buying data storage services from Microsoft but I own the app, I run the app but I still am not entirely sure where my data is?

Greg Hughes: Well, it could be that way, that's maybe the hybrid, I'm also thinking that if you can buy, if you can setup and build your own cloud, does that make sense? So I have data centers that are scattered all around the world that are already in use and what I can do is now I can just, I can build a, leverage the cloud computing technology that's being built and sold now, in a limited fashion, right, but I think isn't Microsoft, sort of effectively making that available? I can sort of effectively making that available? I mean I can sort of build my own cloud if I wish, I mean I don't have to use Microsoft's data centers or Google's data centers or what have you, I could use my own and do a more virtual distributed type of infrastructure but still have that within my realm of control.

Richard Campbell: But then you're still just running your own data centers, I don't think our rules are any different than what we've always done with our own data centers.

Andy Malone: I think that's the difference between the data center and the cloud, though.

Richard Campbell: Right, right, right.

Andy Malone: A data center is the way that we've always done it, you have service level agreements so you control it yourself but the cloud, this is totally different because in the cloud your data is distributed worldwide. I mean its like active directory, okay we all know how active directory works, it's a multi-master domain model but you can't certainly in one domain say, "Okay, let's shut this bit down and shut that bit down." You don't have that level of control because your data is distributed everywhere and that's how a lot of people see cloud computing.

Greg Hughes: So I guess what I'm saying is that I'm sort of taking a hybrid approach, I can, there's the Utopian cloud computing where everything just kind of floats where it fits and everything comes up and I can bring up all my everything anywhere I want and it's all distributed and if one data center gets bombed, then it doesn't matter because everything is just working right?

Andy Malone: Yeah, that's a great model.

Greg Hughes: And then there's a classic data center model where I have two data centers and I'm doing, I don't know and I've got data bases that are replicating between data centers and I have these really nasty pipes and a kind of the school way of doing things right, but the hybrid is, is that if the technology infrastructure that's being used to build the public if you will, cloud could also be leveraged to do private cloud computing and that may allow me as a business and granted, small businesses aren't going to do this but as a large business, maybe one that's doing big business and really does have a lot of compliance issues, I may choose to leverage that type of infrastructure that does provide the services for the cloud computing that you're talking about, I may try to leverage it in a private data center kind of way but still to get all of the technology and business benefits that can come from distributing cloud computing?

Richard Campbell: I'm not convinced that that model exists yet, Greg.

Greg Hughes: No, I don't think it does exist, I'm just saying that it could and it wouldn't surprise me too much if in the future it does. I don't think it's going to be the standard way that it gets leveraged but I wouldn't be too surprised if that happens.

Richard Campbell: All right gentlemen we're getting down to the wire here, Andy are there places that folks getting in the cloud should be going to really understand what their liabilities and concerns should be around this?



Andy Malone: Yeah, sure. I mean if you have a look on various websites, for example, the Microsoft website, if you go on and you look at their Azure platform for example, there are some white papers and on Technet there are some quite interesting white papers as well on cloud security but again there's a lot of debate. In fact if you go to Google's site as well, they also have some good white papers on it and there's a few security websites. So I'll actually might put, stick a few on my blog, I did actually do an entry in the blog recently on cloud computing and I had quite a bit of feedback on it and so I might actually put some of those white papers out there so folks can go and take a look.

Richard Campbell: But I think the first point you made is really significant which is we only have a handful of significant cloud providers yet and you can argue how significant one way or the other but each of them are doing this their own way whether they're Amazon or Google or Microsoft, you've got to go look at their documentation to decide where you want to go.

Andy Malone: Sure. I mean you have to look deep at the service level agreement. So where is the data going to be stored and in the case of HIPAA, the US says, I only want my data in the US; what kind of provisions is in the contract so that some of the providers don't actually do that.

Richard Campbell: Right.

Andy Malone: I've seen one of the UK cloud providers and there's no provision in that, they just said, "Basically, your data in the cloud, it can be in any of our data centers." So obviously that's going to cause problems. So I think you need to look at the various providers, you need to look at their service level of agreements in detail, as well.

Greg Hughes: Probably a quick note that we haven't really touched on is for a cloud computing provider, anyone who's considering a cloud computing provider has a lot of other questions that need to be asked even beyond just where the data is going to lie but how is the infrastructure built, how has it been reviewed, what is the security model that you run this under, what regulations is it governed by? Who is auditing it, who is doing the review, the certification process and all of those big picture things. I mean it really is, to use Andy's term it's a minefield.

Andy Malone: Hey, doesn't it sound like Skynet?

Greg Hughes: Oh boy, here we go.

Andy Malone: We're taking over the world soon.

Greg Hughes: But it can be done and I know that I don't recall specifically when it was published but I know that I read a Gardner Group analysis of cloud computing security that was pretty good and maybe I'll try to find that and give that to Richard for show notes but the or at least a summary of it because, but there has been some analysis, some industry analysis done, even outside of the providers, so the provider's analysis is good to read and what are they doing, they're white papers but looking at the sort of the industry analysts that sort of do the outside looking in type of views, is probably good to look at as well.

Richard Campbell: Yeah, just poking around the search engines for PCI compliance in cloud computing has turned up really recent discussion on how to do this. It's interesting to think that this is only really come to fruition as of the end of 2008 and early 2009 that we're finally getting into...

Greg Hughes: Sure.

Richard Campbell: Can an application pass a PCI audit if it's running in the cloud? Andy thanks so much for coming on.

Greg Hughes: Yeah, thanks Andy we'll talk to you soon.

Andy Malone: No problem, thank you very much Richard, nice to see you too again, Greg.

Richard Campbell: You bet and we'll talk to you next week on RunAs Radio.