



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 #002*

(Transcription services provided by [PWOP Productions](#))



**David Sengupta on Exchange Email Policy issues  
April 18, 2007**



## David Sengupta on Exchange Email Policy Issues April 18, 2007

**Carl Franklin:** From [runasradio.com](http://runasradio.com) you're listening to RunAs Radio – The weekly Internet Audio talk show for IT professionals, with Richard Campbell and Greg Hughes. This is Carl Franklin, introducing show number 2, with guest David Sengupta, recorded April 12<sup>th</sup>, 2007. RunAs Radio is produced each week by Pwop Productions – Offering professional media and Podcasting services, online at [pwop.com](http://pwop.com).

**Richard Campbell:** This is Richard Campbell, you are indeed listening to RunAs Radio, and I'm here as always -- at least for the second time anyway with my cohort Greg Hughes.

**Greg Hughes:** Hello Richard, how are you?

**Richard Campbell:** Happy to be here; glad to be onto another show, we're making our way.

**Greg Hughes:** I think we have some really interesting things to talk about today. We're going to enter the world of exchange.

**Richard Campbell:** Yes indeed, and I've got a bit of email, not the way we were supposed to get it. We put together the website, and we had [info@runasradio.com](mailto:info@runasradio.com) but for some reason it's broken, so I got some comments on my blog that were supposed to be emailed. Let me read this one to you, "Great show Richard, I tried to send some fanboy style email congratulating you in a more private arena, but it seems that the [info@runasradio.com](mailto:info@runasradio.com) email address is not working properly. Here is an excerpt from the email. 1) Will you be getting a schedule up on the website as you get up and running, and based on the answer to that, 2) Will we be able to sit make questions for you to ask your guests?"

**Greg Hughes:** I think that is a question.

**Richard Campbell:** That is a question, isn't it? And that's from Mike Minutillo. Thanks Mike. Sorry the email didn't work.

**Greg Hughes:** We already have fanboys.

**Richard Campbell:** It was only going to be fanboy style.

**Greg Hughes:** It's great to hear from you Mike.

**Richard Campbell:** So, absolutely I'll be putting a schedule up; as we start to get some shows booked then we can let you know what's coming, we'll put that on the website. We will fix the email address. For now, if you want, you can email me at my Pwop address [richard@pwop.com](mailto:richard@pwop.com). The comments is fine, if that's the way you want to go on the blogs. Definitely, please send us your

ideas for shows. We've got lots of thoughts as well, but we'd love to hear your feedback, are we getting the right format, are you hearing the show the way you want to hear it, do we need to go longer, do we need to go shorter, are we talking about things you care about? In the end, if you don't like it, we've got nothing to do.

**Greg Hughes:** It's nobody's show if it's not for the listeners.

**Richard Campbell:** That's it. Alright, so let's get to our guest. David Sengupta is a Global Director of Product Management for Messaging and Migration Products at Quest Software. He is responsible for all aspects of product strategy for email, instant messaging, unified messaging and related solutions. A Microsoft MVP in the Exchange Server category since 1998, Sengupta has contributed to most Exchange and Windows magazines and numerous books and whitepapers. He is a regular speaker at key international events including Microsoft TechEd and IT forum. He has worked with Microsoft Exchange since its inception. David has an MTS from Tyndale Seminary, Canada and a BSc from University Ottawa, Canada and an MCSE in Messaging. David is also an analyst for Ferris Research, runs a blog on email compliance news, is a columnist for [searchexchange.com](http://searchexchange.com) and is a technical editor for Windows IT Pro Magazine. He is on the PR committee of the Electronic Discovery Reference Model project, a member of the information system audit and control association, and a member of the Institute of Computer Forensic Professionals. His publications are read daily by English and Mandarin speakers around the world. Welcome David.

**David Sengupta:** Thank you, glad to be on the show.

**Richard Campbell:** Wow, 1998, you've been involved with Exchange since the beginning pretty much.

**David Sengupta:** Yeah, since Beta of Exchange 4.0.

**Greg Hughes:** You've been through the painful days of Exchange as well as the more pleasant recent days.

**David Sengupta:** That's for sure.

**Richard Campbell:** Back then it was a very, very different product; it has gone through quite a lot of change.

**David Sengupta:** Yeah, Exchange has definitely matured and changed a lot over the years, from



just doing email and moving into Instant Messaging and then backing out of Instant Messaging, the Web Store and then now into Unified Messaging - definitely exciting.

(00:05:04)

**Richard Campbell:** I haven't had a chance to do a migration to Exchange Server 2007 yet, although I'm itching to do it. I think the 64-bit requirement is spooking me a little; and just in general, I think Exchange has this knack for being a bit frightening as a technology.

**David Sengupta:** Yeah, I mean definitely Microsoft has gotten a lot better as far as making the upgrade path a lot easier. The 64-bit requirement is affecting -- I mean people think about it and initially when Microsoft first announced it, it was a bit of an issue, but nowadays we don't hear of it as a huge issue from our customers though. It's not like 80% of our customers have to buy 64-bit hardware for the migrations, but at the end of the day things work out well, because they can scale up more users on their Exchange 2007 boxes.

**Greg Hughes:** What are the big reasons to go to Exchange 2007 over Exchange 2003?

**David Sengupta:** Well, I mean 64-bit as I mentioned is definitely one pro; there's a lot more flexibility from a compliance standpoint. Things like transport rules allow you to control email flow throughout your exchange environment. So, when you think of the rules available within Outlook, where you want to be able to control or take action based on certain criteria in a message, you can do that now at the Enterprise level and control traffic routing throughout your organization and setup Chinese walls so that one part of the organization can talk to the other, that kind of thing. So, definitely a lot more controls around email.

Things like Unified messaging are getting a lot of attention, so the ability to store voicemail -- I mean unified messaging has been around for a long time with numerous third parties, Avaya, Cisco and others that have had solutions, but with Microsoft moving this way, it's definitely been a move towards the mainstream. And then if you look at just what Microsoft is doing across the platform, end to end around voice and enterprise telephony, you see devices such as the new Tanjay phones, that Microsoft has at least released some information around, and Office Communications Server, and other text and speech related and video conferencing type solutions. There's just a lot of momentum happening around the Microsoft platform.

**Richard Campbell:** I know you mentioned this on your blog and I was at the MVP summit as well, where Bill Gates said in the sort of keynote presentation, "Imagine a world without PBX's." Do you really see this whole unified messaging approach that Exchange is taking as a move towards that?

**David Sengupta:** Yeah I do; when you look at some of the technologies even today with -- you can sub link Exchange 2007 Server with just an IPPBX - full connectivity there, and just looking at where Office Communication Server is going and where Microsoft is driving pretty hard, I think it will be, in a few years or even sooner, we'll start to see enterprises deploying without a PBX. And we're already hearing of companies -- so I now work for Quest Software and we're hearing of companies in Europe for instance that are setting up entire buildings, but have no PBX in the entire building and are just relying on Exchange 2007 unified messaging.

So, it will be a while until it becomes mainstream, but when it does, I think you'll see environments without PBX's.

**Richard Campbell:** And you mentioned the Tanjay phones; is Microsoft actually producing this or is it a third party?

**David Sengupta:** Microsoft is working with a number of third parties; and so the Tanjay is a code name for a certain form factor of devices, and like I say, not a whole lot has been publicly released around them, but if you look at some of the partnerships that Microsoft has established recently - so companies such as LG with Nortel and others, where Microsoft is obviously working with those partners to look at phones that support name-based dialing or Office communication server integration from a present standpoint, integration with Exchange 2007 voicemail and calendaring and such. So, you will start to see name-based dialing popup on these phones, where you don't have to actually remember the number, but you can just dialup someone based on name, and you'll be able to see people in your team whether they're online or offline, and if they're online then just the ability to push a button and very rapidly just dial those people from your USB enabled phone.

**Greg Hughes:** IT pros all over the place more and more are reviewing and taking a look at the possibilities of doing VoIP, replacing PBX's with something more flexible, less expensive potentially, and as we are talking about more integrated -- what do they need to be thinking about today, let's say they're already in Exchange house, they're looking at moving to Exchange 2007. In order to take advantage of



what Exchange 2007 has to offer, what kind of things do they need to be keeping in mind?

(00:10:03)

**David Sengupta:** Yeah, that's a good question. So, definitely one of the things that companies need to think about off the bat is just organizationally the teams that handle telephony and phone systems and Patch clauses and all that kind of thing are typically very different from the teams that run Active directory and Exchange and Messaging within the organization. So, probably one of the first places to start is just to just get those teams talking to one another, and then just understanding each other's requirements and starting to look at whether Exchange 2007 is a viable solution in those scenarios. And some of the early indications that we're hearing is that there's just a lot of ROI opportunity around -- there's a lot of cost associated with provisioning phones whenever someone moves around in an organization and someone actually has to go over to the desk, put a phone in place. In some cases that's a third party that's actually hired at a fixed price per phone, that kind of thing, and then running through the patch clause and making sure it's patched through.

So, there's definitely an opportunity there from an ROI perspective. So organizations need -- like I said, just need to start with those teams talking to each other and starting to talk the same language and understand each other's worlds.

**Greg Hughes:** Yeah, I think it's a good point; and we tend to think about IT projects as being truly technology-driven when really there's quite often some critical people and process components to any IT project.

**David Sengupta:** For sure.

**Richard Campbell:** You were bringing up the whole issue of telephones; and I've always loved the idea that I would be able to dial from Outlook and things like that, and it brings back the thoughts of the old tappy interfaces, which sort of fell by the wayside. Those never worked quite right, and it seems funny that the solution was not to integrate the phone with the computer so much as to turn the phone into just another part of the computer; it's just another part of the network.

**David Sengupta:** Yeah, and that's one of the reasons I think Microsoft will end up being successful with their attempt is because they own so much of the platform. I mean, they're already on your desk in many cases with Word or Excel; they've got the operating system. Making the phone part of all that just means that you can be

sitting in a Word document, type someone's name in the document and then potentially right click, phone them, all that kind of thing. So, it just becomes yet another object within the world that we work in everyday.

**Greg Hughes:** Yeah, the presence information of the Calendar and their Instant Messaging status, Direct-Dial telephone -- for example, on SharePoint and all the different -- the office integrated applications is really pretty powerful.

**David Sengupta:** For sure.

**Richard Campbell:** Maybe we should talk a little about how instant messaging fits into this equation. I meet more than one organization that simply does not allow instant messaging at all on the platform inside of the organization. But, I think that's a little archaic these days.

**David Sengupta:** Yeah, so from an Instant Messaging standpoint, I think what happened is, there was a proliferation of solutions both out of Microsoft and from third parties outside of Microsoft for instant messaging. And obviously, Instant Messaging took off a lot faster than I think most of us expected it would. The industry was right -- just the world was right for that kind of communication modality. So, I think what happened is, things just got out of control, and on one side you had the financials with their need for regulatory compliance and Instant Messaging was abused in those scenarios and so, they had to lock all that down. On the other hand, you just had organizations -- typical corporations or enterprises where instant messaging started to either become a violation of -- or at least a perceived violation of just general productivity and that kind of thing.

Just the fact that it was out of the control of IT organizations in many cases I think was a concern. What we are seeing now, is organizations, at least from an Office Communication Server perspective are really taking a hard look at -- and in many cases have deployed or in the process of deploying enterprise Office Communication Server deployment that are under their control, and then just making sure those are enabled to whichever people within the organization need that capability in it. I think we're starting to see a lot of productivity restored where they had to block it for whatever reason and just companies getting ROI out of Instant Messaging.

**Greg Hughes:** I think one of the big concerns, especially for the financials has to do with the requirements to log all Instant Messaging if you're going to do it. And one of the beauties of a live communications server -- office



communication server is the ability to do that logging, but also to bridge over to the public instant messaging networks and exercise some control over that.

**David Sengupta:** Absolutely.

**Richard Campbell:** Yeah, a little bit of both. We're dancing along the concerns around regulatory compliance and general liability exposure, and email just seems to be in the news constantly on the exposure side, and electronic discovery is something I worked with a number of years ago. I know that's an area you've done some things as well with David. Maybe we can talk a bit about where Exchange is going in supporting those issues.

(00:15:20)

**David Sengupta:** Yeah that's a good point. So, email definitely is something that we're seeing literally everyday in the news. I mean, just today in the news, we've been reading about the White House and how there was -- I have the story right in front of me, where there were at least 22 people who were using laptops and email accounts for official purposes that weren't part of the typical or the approved email system at the White House. Regardless of what's true and what isn't true and what's rumor and all that kind of thing, it just underscores the importance of email in our day-to-day business communications and also personal communications.

So, just being able to control that from a compliance standpoint, understand what email is being used -- so, doing things like reporting and analytics is becoming more and more important, and then from a discovery standpoint, when there is either a public enquiry in the cases of government or a lawsuit or whatever type scenario, discovery is just becoming more and more important within organizations.

**Richard Campbell:** I guess the trick here is, you don't want to find out what your email exposure is like after you get the writ for discovery.

**David Sengupta:** Absolutely.

**Richard Campbell:** You want to know ahead of time. So, Exchange 2007 specifically, you talked a bit about, there are some new rules engines in there to facilitate supporting rules around protecting yourself in discovery scenarios. So, what do they look like; what kind of software are we talking about here?

**David Sengupta:** OK. So, before we talk really specifically about the technology, again, similar to what we were talking about earlier, a lot of times

its people, process and technology working together that really end up being a solution to a business problem. So, with the discovery problem, again, it's no different. So, just taking whatever approach you take towards legal discovery in your organizations, especially if you're subject to -- either potentially or having a lot of lawsuits, and some of the large organizations that we deal with at Quest, and we'll have 50, 60, 70 lawsuits ongoing at any particular time in some of our large customers. So, those organizations tend to take a proactive approach to discovery and so they'll all protect their environment, both Exchange and other systems, since discovery doesn't just apply to email, it applies to process and data, and in some cases, database information as well. And so, just having to be proactive and setting up that environment in a way that minimizes risk and minimizes attack surface and ensures that if there is a requirement to preserve information under a duty to preserve or some other requirement, that the procedures are in place, that the right people are in place and that the people know what the procedures are, and that they have the technology to put that legal hold in place when discovery is actually required.

Again, if an organization is being proactive, it will put the pieces into place, and in some cases, there are elements of Exchange 2007, which I'll touch on shortly, that definitely help out from that perspective. What we see a lot is, organizations that are in a reactive scenario, that maybe they're not as large organizations, or maybe they just never -- maybe they don't fall under any particular regulatory compliance or SOX or anything like that. But they've got a lawsuit, or they have had something unexpected come up where all of a sudden they're thrown into the spotlight or thrown into a scenario where, for whatever reason, whether it's corporate risk or risk of arbitration, or just having to respond to a particular issue at hand, they have to discover evidence. In that reactive scenario, if the organization has not set things up with discovery in mind, things can get a lot more complex and a lot more expensive; and that's where we hear of organizations that either cannot comply and cannot produce the evidence that is required. In which case, sometimes reputations comes into question and all sorts of issues. Or, you hear of just very, very expensive legal discovery scenarios where companies have to just ship truckloads of tapes or whichever -- in some cases cell phones and other data devices, whether it's servers or laptops or whichever off to third party forensic firms for recovery purposes.

**Greg Hughes:** So, what is Utopia in that sense then, what would be the industry best practice if you will for being prepared?



(00:20:00)

**David Sengupta:** So, best practice again, is being proactive. So, when you think from just an Exchange standpoint -- and I'll leave file system and all that kind of thing out of it -- but when you think of Exchange, and you think of -- you need to think about where your data is stored. Typically, there's four main silos that I like to think of as far as email within an organization, at least from an Exchange standpoint; you've got data that's in your production mail servers, you have data within PST's and other offline -- in some cases stored as MSG or TAX or other formats on people's laptops and computers and in some cases on the network tape, and that's not really recommended by Microsoft. Thirdly, you'd have in some cases, archives, if you've got companies that are using email archives, or some sort of in-house archiving solution, and then fourthly, backups. I mean, backups are not intended as an archive, but just the nature of tape-based or VSS -- or in some cases CDP backups means that there's email data there that you need to think of from a discovery standpoint.

So, your first layer of defense is minimizing your attack surface. So, look at all those different silos, think of where the liability is, and then cut down, a) How long do you hold on to your tapes? If you don't have to hold on to them too long, maybe just hold on to them for a month and then destroy them afterwards. Archives, what kind of data has to go into your archive? Do you even need the Archive? In some cases, organizations need to, and in other organizations, their legal counsel will make a decision not to archive. So, those kind of decisions need to be made. Keeping data in your production exchange servers can be a real liability, especially if you've got a lot of exchange servers, and if they're widely distributed. Because again, having to find information across all those servers if they're distributed can be very hard and very complex. And you may not be able to do that within the time that is allotted and -- if there is a legal scenario that comes up.

And then finally, PST's -- again, just incredible amount of risk associated with people being able to create PST's. And again, it sort of depends on what the organization's tolerance is for risk and how much value they place on risk is associated with email. But, if PST's are enabled and if thumb drives and other removable storage devices are available, then people can put a PST on there and take the data outside the organization quite easily. So, yeah, you need to reduce the amount of data that's out there and the amount of different silos, and then finally you need to be able to discover against whatever silos you do have. So, organizations may decide to lockdown

all PST's, may have an archive, and may minimize how much mail is in their exchange servers for instance, and only keep 30 days there before archiving it out and may delete all of their backup tapes after 30 days. So, in that scenario, you would need some sort of a solution to search across Exchange, and PST's wouldn't be an issue because they've been locked down. Archives typically have a mechanism for searching and then backup tapes -- typically with just 30 days worth of backup tapes, if they only have a few servers, then there shouldn't be a huge issue or a huge liability as far as having to get data off of inaccessible media.

**Greg Hughes:** You know, you have mentioned PST's several times, and that's a pretty common set of questions I know that I get related to how do I control PST's, how do I lock them down, what does lockdown mean? - Often seen as a very large area of liability, and with a big surface area for a problem. Maybe you can touch a little more detail on some of the different things that are available nowadays for exercising control over PST's?

**David Sengupta:** Sure, good question. So, from a PST perspective, there is a switch available with Outlook today; it's a registry key that you can lockdown the ability to create PST's and so we see organizations doing that just to completely block the ability for end users to create them. There are also some different tools on the market for actually going out and harvesting PST's off people's laptops. Archive vendors typically will have a tool built in to the archive to actually move data off and into the archive, and in many cases delete the original PST, or do any sort of throttles -- migration of the PST's into the archive over a period of a week, or two weeks or whatever depending on how much volume is involved.

So, that would be one aspect. A lot of the archive vendors, or some of them at least have offline clients and so, replacing PST's which are out of the control of IT with an offline client that is tied into a central archive in many cases provides a much more robust and a much more controllable scenario. And then in some cases -- especially, organizations that have highly mobile sales forces for example, that kind of thing, if they haven't got an archive deployed, they may find that allowing PSTs is acceptable for certain communities within the organization, and so they might say, "Sales reps can have them," and then every once in a while, they do an audit of what's out there and maybe copy the stuff into a central network share, so at least they have the data. But, really the best approach, if legal compliance is really an issue, is either migrate everything to the archive or block it completely.



(00:25:24)

**Richard Campbell:** Yeah, you could definitely see your mobile guys are going to end up with PST's some of the time, but if you have some policy around there and some control over those machines, you're going to have an opportunity to clean them up once in a while.

**David Sengupta:** For sure.

**Richard Campbell:** You mentioned the registry control over Outlook; do you know – is that only 2007 or is it earlier versions that had that capability?

**David Sengupta:** It was earlier. I've forgotten exactly which version it was introduced in, but it wasn't just Outlook 2007.

**Richard Campbell:** Good, so it's been around a while.

**David Sengupta:** Yeah, it has.

**Richard Campbell:** I got to think that feature was exactly along the lines of dealing with compliance issues.

**David Sengupta:** Absolutely.

**Richard Campbell:** So, you get into a situation where you're dealing with a discovery case; is there features in Exchange 2007 that are going to help you?

**David Sengupta:** So, one of the things that's new as you know with Exchange 2007 is the fact that Windows PowerShell has been built in to provide -- it's actually a command line scripting interface for all of the functionality within Exchange 2007.

**Richard Campbell:** Right.

**David Sengupta:** Within the PowerShell script, there's the ability to run, what's called an 'Export-Mailbox cmdlet' and when run in a certain configuration, you can actually go in and say, "Search all of my mailboxes across a particular scope, whether it's the entire organization or certain servers," that kind of thing, and search for certain criteria in those mailboxes. You could say, "Go out and find anyone who's got a message with a subject line that contains 'Finance'" or anyone who -- any mailbox that meets certain criteria, go and search those, or a specific user's mailbox, and then find the information that's there and spit it into a target investigator's mailbox. So, it's pretty powerful functionality that's been built into Exchange 2007 that's based on the full text indexing, that has been dramatically improved in

## David Sengupta on Exchange Email Policy Issues April 18, 2007

Exchange 2007, and that is turned on by default now. And it really gives an investigator the ability to go out without having to actually configure Outlook to logon to someone's mailbox or anything like that - to actually go out, search for data and then spit it into a target mailbox.

One of the things that Microsoft is working on in SP1 of Exchange 2007 is actually being able to support 'exported PST', which is sort of that missing piece that a lot of corporate - office of general counsel or lawyers really are looking for, for investigational purposes.

**Richard Campbell:** Yeah, that sure sounds like the kind of discovery tools that were being built a few years ago, to go and harvest kind of, information from email forms now built into Exchange.

**David Sengupta:** Yeah, and so you maybe familiar with the product -- with a Microsoft tool called ExMerge, which Microsoft used to ship, and it's still available and still works on Exchange 2007. They haven't locked it down or anything like that, but they have stopped development on ExMerge, and really the export-mailbox cmdlet replaces that functionality, and so the exported PST will show the last step as far as trying to get feature parity with what was in ExMerge.

**Richard Campbell:** Well really, all ExMerge could do was pull up mailbox out as a PST, or put it back. This is way more sophisticated.

**David Sengupta:** Yeah, just the ability to go and script it all, and automate it all. There's definitely a lot of power there. One of the interesting things that we are going to see over the next while is as -- there's now voice data stored within voicemails within Exchange. I think we're going to start seeing the whole text-to-speech and speech-to-text interaction becoming more and more important, especially when it comes to search. So, when you think of legal discovery, right now, we're used to searching things like email and all that kind of thing, which is hard as it is. Add on to that the whole modality of speech and -- I don't know whether it will be iFilters for speech or what, but some sort of technology is going to be needed to be able to go in and either transcribe speech into text, so that it's searchable or actually search it in place. And I'm sure that Cambridge Labs and other labs out there are well into working into stuff like that. I'm sure Microsoft has been working on that as well. So, it will be interesting to see how that happens.

**Richard Campbell:** Well, the other side of Unified messaging is going to be, that all this information is one place, so the exploration of it,



or the discovery of it so to speak is going to be that much easier.

**David Sengupta:** Yeah for sure. If you look at Microsoft Office SharePoint Server (MOS), they have a skew called MOS-FS or codenamed -- short for MOS-FS or Microsoft Office SharePoint Server for Search. It will be interesting to watch how Microsoft develops MOS-FS. They seem to be leaning towards enterprise search and providing sort of a lower level of feature type skew just for search. I'm sure that Google Compete is part of that, and Google's enterprise search capability is that kind of thing. So, it will be interesting to see how they develop that and whether -- or when they come out with something speech related from a MOS-FS standpoint.

(00:30:24)

**Richard Campbell:** Yeah, that's a good place to pull that in, and Microsoft has the advantage of controlling most of the data that people are searching. So, it makes sense that they would ultimately provide the search tools for it as well.

**David Sengupta:** Yeah, definitely a lot of pieces that have to come together -- I mean, look at Windows Desktop Search (WDS) as well; all of those different teams within Microsoft are all -- to some extent they talk, to some extent they don't. So, it will be interesting to see how well Microsoft can execute on getting those teams to all work together, and in a way that facilitates the kind of enterprise search that is sort of the holy grail of legal discovery or just Enterprise Information Management if you use a Gartner term.

**Richard Campbell:** David, thanks very much for your thoughts on this; anything you want to close with? Have we touched on sort of key issues around this, or are we missing a few points?

**David Sengupta:** No, I think we have covered a lot of ground, and like I said earlier, people, process and technology are really important, and so organizations looking to get control over information, whether it's from a legal perspective or other perspective, really need to look at the process that they have in place, from a risk mitigation perspective, and in general, and Exchange 2007 plays an important piece of that, as do other technologies as well.

**Richard Campbell:** I do think that it's important that IT teams get together with their legal groups once in a while to make sure we're all thinking about the same key issues.

**David Sengupta:** Absolutely.

**Richard Campbell:** Well David, I appreciate your time today, and hope we will be talking to you again soon.

**Greg Hughes:** Thanks David.

**David Sengupta:** Thank you.

**Richard Campbell:** And we'll talk to you again soon on RunAs Radio.