Bring Your Own Device (BYOD): Avoiding Anarchy

With Avaya

Recorded March 14, 2012

Discussion Transcript*

Participants:	
	***Gary Audin,* Moderator; Consultant at Delphi Inc.; and Author, Webtorials TechNotes**
AVAYA	***Rob Butters,* Senior Solutions Marketing Manager, Avaya**
	***To download or listen to the audio podcast version of this discussion, visit:*** http://www.webtorials.com/content/2012/04/byod-avoiding-anarchy.html

Steven Taylor: Welcome to the Webtorials Thought Leadership Discussion on "Bring Your Own Device: Avoiding Anarchy."

Hi. My name's Steve Taylor and I'm the editor-in-chief and publisher at Webtorials, and I'm very happy that you are joining us here today.

There's no question that BYOD has become one of the hottest topics around, because of the proliferation of smartphones and tablets/pad computers. Every organization's going to be dealing with this particular issue, and it's a case where the only sane approach is to figure out a strategy for controlling the use of these devices, because banning them from the organization just simply isn't going to work.

We're very fortunate today to have two industry experts with us to discuss this. We have Gary Audin of Delphi, Incorporated, who's been in the industry for over 40 years as a system and network implementer, consultant and analyst. Many of you may already be familiar with Gary also because he's the primary author for the *TechNotes on Unified Communications* that we publish at Webtorials.

We're also very fortunate today to have with us Rob Butters, who is a senior solutions marketing manager with Avaya. Rob has a really in-depth knowledge of customer needs because of his experience with working with real customers for Avaya for mobile collaboration solutions.

So, at this point I'm going to turn the program over to Gary for some introductory remarks and to start the discussion.

Gary Audin: Thank you, Steve. I think one of the points that's really important here is that the growth of "bring your own device" is almost unpredictable. Everyone says it's going to grow much faster, but we have no idea how much. One study that just came out a few weeks ago estimates that by 2016 there'll be enough mobile devices for everyone in the world to have one. Another study pointed out that for every person who has a mobile device, 40% have a second mobile device as well, so they've got at least two media. Trend Micro just did a study saying that BYOD actually delivers much lower IT cost.

But I think one of the points that's really important is that this is really a user-driven phenomenon rather than an IT- or enterprise-driven phenomenon. Which means planning for this is quite different than planning for the technologies IT normally would give out.

I'd like to start my first question with Rob. What's the single most problematic aspect of this BYOD environment?

Rob Butters: Gary, thanks very much for the question. I'll start with the security concern.

Give network access to a device that I can't control that is used by a teenager? Are you crazy? What we have is the millennials and what we're calling the new collaboration era of people coming into the workforce. And really, they're asking for a lot of things. They're asking for access into their social devices and applications. They're asking for access with their own devices.

And you really can't stop that trend.

What we have to avoid is what we used to do from an IT perspective – saying "no." We used to say no to the iPad; no, you can't connect outdoors; no, you can't bring in your fancy laptop; no, you can't use videoconferencing. It's all about saying "yes" now. Yes to an iPad; yes to mobile collaboration; yes to virtual desktopping; and yes, Wi-Fi is available to you.

But it's important to stay in control. What are the risky points?

You've got an increased risk of financial and informational exposure. You know, people hacking, getting on, stealing patents—really an issue of today. And we've got an increased risk of liability. So, the risk manager in the company is just shaking his head thinking, what are we going to do here?

But it has a reward side. There's certainly reduced CapEx. Employees bring their own devices. There's no cost there. Reduced OpEx. We have automated error-free network access. And ultimately, people use the devices that they're more comfortable with. So, it's a risk and security overlap.

Gary Audin: One of the questions I have about security is that most people focus on the access to information. What about the concern that people carry so much information in their mobile devices, and then can be hacked while they're just sitting…around in a room?

Rob Butters: Oh, absolutely. Now you're moving into really a mobile communications environment. You've got one-number identity both on your mobile and on your work phone. You've got office-number one-number identity. You've got office mail and voicemail. You've got enterprise dial plan versus external dial plan, all together. And guess what? You've got all that information, as well, on that computer.

I look at it in a factor of six: I look at IT compliance – who gets on, what do you want them to do, and where do you want them to go? You've got a user experience. How can I provide consistent user experience that will allow them to use that device to their best capability? But then you look at network capacity and how people are using it. You know, do you want to segment or put into queues how people actually use the data, access the data and search and exchange information? Are there pockets that you can store? And there are quality-of-service elements that you want to bring to bear.

But ultimately, you're looking at mobile device management and security, and the mobile device management is key. Your mobile device manager, and how you bring it in and overlay the security on top of the device, is absolutely critical.

Gary Audin: You've talked about several recommendations here. I'm sure there are many that are successful. What would you say is a recommendation you could make that would be most successful for managing BYOD?

Rob Butters: Well, you have to break it down. We're in a vertical world. So, I break this down into fours. I think that you need to understand the core business priorities. A financial arm or vertical is going to be a lot different than somebody in higher ed that's extending communications to their students.

In the company that I'm with, we've deployed a communications infrastructure from "A" to "Z." And the funny thing was that it's an engineering school. And…all of the engineering students try to get on and hack and hack away. So, you need to understand the core business priorities that change by vertical. You need to identify the key users in the business processes. What processes, what users, do you want to extend the best applications to, and how do you secure that?

And then you want to look at implementation across policies and technologies. What are the wireless roaming [policies]? What are the identity management and roaming access technologies available to meet your needs? You need to build in a common communications architecture. You want to look for a vendor that can do that. You know, how will mobility and new devices integrate into the common communications architecture, and how does it tackle all the users' requirements?

Gary Audin: One of the points that I've been worried about is, you know, you have to create policies and procedures here to handle this. And I think IT should not be the only ones developing these policies. Who should be involved in developing policies and procedures for BYOD?

Rob Butters: Well, that's a great question. I think that – again, it's situational-dependent. The risk manager should be there, of course. And you want, of course, the IT manager and the CIO involved.

But you also want to be looking at your operational extension. You want your sales operations manager as part and parcel of that, that says, okay, we need to be granting, as a 'for instance,' the sales rep access. And I think that you can even extend it a little further, because line of business is going to be having much more say. So, extending the voice at the table to the line of business person also takes care of their requirements, while still looking at the security and the risk management mitigation.

Gary Audin: One of the things that people love to talk about are standards. But when I look at BYOD, and I just look at the mobile devices, I find over half a dozen operating systems and dozens of different kinds of devices. Do you think we could actually create some standards as an enterprise, to manage this, or is that something which is theoretical?

Rob Butters: Well, I think that when you talk about secure remote access, you're bringing in one of the key standards that we're hearing more and more about, and that's SIP [Session Initiation Protocol]. And so, one of the key elements that you want to be aware of is how you expand the session border controller.

You also want to make it easier. What SIP brings to the table is making it easier to mix personal and enterprise devices into a secure single, call it SIP traffic [flow], with all of your apps and access to the network. And when you talk to the business side of the business, they'll talk about one thing. Hey, you've got all these great devices; but I need them to work; I need them to be easy to use and deploy; and they ultimately need to lower my TCO. So, SIP is one of those elements, and session border controllers on how you grant access is key.

Gary Audin: Getting back to the operating system, it doesn't seem like you can actually choose one or two operating systems to standardize on, with the proliferation we have out there. What's your comment there?

Rob Butters: You really need to be looking at controlling access and security and leveraging common identity management capabilities. From an access and control standpoint, you want to have the infrastructure that puts the Web over your communications infrastructure. But you also need identity engines and [to] identify each device that enters the network, and apply rules based on ID – device ID, device type, connection type and then, ultimately, you need to apply policies based on what you want to extend to those. BYOD devices may not need full access.

A lot of businesses have people that do hoteling—that come in as a guest. So, you want to make sure that your communications infrastructure extends guest access to make it appropriate for that guest but also extends just enough security so that they're not having access to things you don't want them to see.

I think that overarching here, you need to be selecting a vendor that has a professional services organization that doesn't look like a deer in the headlights when they're talking about BYOD.

Gary Audin: I've seen a number of products come out recently from mobile device management—MDM [vendors]. And I think there's value there, but I also think there's some problems with MDM. What has been your experience with MDM?

Rob Butters: The one problem that I've seen with MDM is how it integrates into the actual architecture. You also want to make sure that you've got compliance issues. E911 is a certain consideration that you absolutely want to address right upfront.

So, MDM and how it actually melds into the communication infrastructure, I think is the key. Because there's nothing that would put somebody more at risk than not knowing where they are within the business.

Gary Audin: Last question on MDM, and I'm going to be finishing with this one, is how mature is that market? Are we expecting to see more evolution of the products, or is it pretty stable already?

Rob Butters: I don't think anybody would have been able to guesstimate that, you know, you're going to have 1.2 billion users on social media. You're going to have 800 million smartphones. You're going to have 75 million tablets in 2012. I think that when you look at vendors that make it easy to adopt BYOD into the workplace, the real key here is that you're looking for a vendor that has BYOD as part of their DNA.

Gary Audin: Thank you very much. And – turn it over to Steve.

Steven Taylor: Okay. Thanks so much, both Rob and Gary, for those great insights and questions. We'll look forward to people hopefully not only listening to this and reading the transcript of this, but also continuing the discussion at Webtorials. Guys, thank you so much for the insight.

Gary Audin: Thank you, Steve.

Rob Butters: Thank you, Steve.

THE END

* *The discussion has been edited slightly for clarity and length.*