ZixCorp: A Fresh Perspective on BYOD Security

Recorded October 16, 2014
Discussion Transcript*

To download or listen to the audio podcast version of this discussion, click here.

Nigel Johnson
ZixCorp, Vice President of Business Development and Product Management

Larry Hettick
Webtorials® Analyst

Patte Johnson: Welcome to our Webtorials podcast. Today, our Webtorials analyst, Larry Hettick, will be speaking with Nigel Johnson, Vice President, Business Development and Product Management for ZixCorp. The discussion today will feature a fresh perspective on BYOD security. Welcome, Nigel and Larry. I'm going to turn it over to you.

Larry Hettick: Thank you, Patte, and thanks, Nigel, for joining us today. I've got several questions to ask. Let's start with a baseline, because we know that employee mobility is really critical for today's business operations and that many organizations are supporting BYOD to enable that mobility. Why is BYOD, or Bring Your Own Device, important to business?

Nigel Johnson: I think there are three things, Larry. And this is not in priority order. But companies want to attract bright young minds, and bright young minds have a very set way. Isn't it funny that bright young minds – you'd think they'd be flexible – but they're very set, in that they like to communicate with the rest of their peers through a device that they know and own. And the device isn't just about it being an iPhone® or an Android™. It's about all of the apps that they have on that device. And they want to use their device. So, if you want to bring those people into your company, you need to accept the fact that they want to use their devices for doing work.

The next is productivity. People are very happy to take emails or calls when they're out of the office, when they're off the clock. They want to help the team. So, they

don't mind a five-minute conversation or a quick email to answer a question while somebody else is working in the office.

And the third reason is cost. There are savings to be had by allowing people to bring in their device, even if you give them a stipend to pay for the extra bandwidth.

Larry Hettick: What is it about BYOD that employees actually like? I mean, why do they like to be able to bring their own device?

Nigel Johnson: Employees like to bring their device because it's theirs. They don't want to carry two devices. And it's a funny thing. We like to carry one device, but we actually like to use many. I'm sure that this happens with you, Larry. You had an older iPad®, and you buy the new iPad. You didn't throw the old one away; you just have that in a different part of your house. And it's the same for me. I have two phones and two iPads. The phones are mine. The iPads are shared amongst the family. But we all use them to connect into our work and into our lives.

Larry Hettick: Thanks. So, what are some of the employer concerns about BYOD? What are some of their issues with BYOD?

Nigel Johnson: So, you have the hiring managers and the employers who say, let my people have their own phones. And then you have the people responsible for security. This is a good example; when you read an email on your phone, the email is pulled onto your phone and held on your phone, and every time you connect, all the emails in your inbox are pulled onto your phone. So, IT's really concerned about all of these emails sitting on people's phones.

With 113 phones being lost or stolen every minute, IT is right to be concerned about what happens to the data that's in their emails. And so, they want to control the phones that people bring in. And that's where we start to see a conflict between the desires of the employees and the true needs of the IT security group.

Larry Hettick: So, you mentioned that there are some concerns on the employee's part, but what might those be, with BYOD?

Nigel Johnson: Oh, for the employees? Because IT now feels that they need to control a phone, they're going to ask for the employee to do something to secure their phone. IT wants to control the phone. The employee doesn't want that control, because it means, generally, that they have to have a password to be able to get into their phone. Which means that their phone is no longer quite as smart and convenient. They're used to being able to get in, ask a quick question, get out; take a video; take a picture. And now, it's become cumbersome.

Employees are often asked to sign an agreement that allows the company to wipe data from their phone, should they ever leave the company or lose their phone. And that alarms employees. Some mobile device management solutions even go so far as be able to restrict apps that people are allowed to have, or even monitor their location. And that could become very concerning for somebody who really

enjoys the convenience of their $600 phone, as well as the privacy that they had before they joined the company.

Larry Hettick: So, those are, as I understand it, sometimes referred to as mobile device management security. How do those solutions work in the traditional sense? I mean, how does the IT department control that phone for traditional mobile device management?

Nigel Johnson: In traditional mobile device management, there are tools that allow these mobile device management solutions, or MDM solutions, to control the phone. And they have a broad amount of control. They're literally able to wipe the device down to its factory settings; or, say you cannot load these apps; or, you must use this complex security.

Larry Hettick: So, how do traditional MDM security solutions address both the business concerns and the employee concerns?

Nigel Johnson: They really can't, Larry. You can't do both with the traditional MDM solutions. In the beginning, the traditional MDM solutions, which take control over the phone, were solving a need for the employers. But nobody was thinking about the employees. And over the last few years, more and more employees and more and more of the media have been talking about the importance of privacy. And now employees are pushing back and saying, I don't want anybody controlling my phone.

And so, while they've been making money selling into the corporations, the employees are pushing back, and it's really slowed down. In fact, it's stalled many BYOD implementations, because the employees just won't accept it. And that's why we're going to talk about this fresh perspective—being able to bring a balance between the needs of IT and the desires of the employees, so that we can have effective BYOD programs.

Larry Hettick: That makes sense. So, this solution that you're talking about is provided by ZixOne. How is ZixOne different from the traditional MDM solution?

Nigel Johnson: Remember we were talking at the beginning about, emails are loaded and stored on the phone, and that created the need for IT to control the phone. Instead of allowing email to stay on the phone, we allow people to read, reply, forward, open attachments—do everything they would normally do with email. Except, when they're finished, there's no email left on the phone. IT doesn't have to worry about emails residing on the phone, which means they don't need to control the phone. So, now we have employees who are happy to have a work-related email solution and to use it at any time, but without fearing that anything bad is going to happen to them or to their phone.

Larry Hettick: Right. So, how does ZixOne address business concerns and employee concerns?

Nigel Johnson: With ZixOne, a business never has to worry anybody ever losing their phone. And with 113 phones lost every minute, there's a lot of risk there. They don't have to

worry about what to do when an employee calls in and says, I've lost my phone and it's got 10,000 emails on it. They don't have to think about all of the regulatory requirements, all the risks of IP laws, for all 10,000 emails.

With ZixOne, there won't be any emails lost. And there is a tiny chance that perhaps a person is still logged in and reading the email when their phone gets swiped off of a table. Even in that case, we produce compliance reports for our customers that tell them exactly which emails were read at which time. We don't have access to the emails. We can just identify the email– who's it to, who's it from, and the date and the time, and they can go look it up on their Exchange servers.

Larry Hettick: So, can you see a place where someone might want both the traditional MDM and ZixOne to work together? And how would that approach work, and does it make sense?

Nigel Johnson: It does make sense. ZixOne is a solution that's built for email, contacts, calendars, tasks, notes—the things that you traditionally do with Exchange and all the productivity you get with Exchange. But there are some cases where some companies—and we have a number of customers who do this—they have a need for a subset of their employees to have access to more than that. And in that case, they have to have a big, heavy MDM solution that controls the phone. And that happens for perhaps 20% of the cases.

We have different studies from different people. Some of the studies say that more than 50% of people just need email, contacts and calendars; and then we have really large industry analysts saying that it's more like 80% of the people who only need email, contacts and calendars. But there's always going to be a subset who might need more. And either they're going to have to have a company-controlled device, or they're going to have to give up the control of their device if they want to have access, for example, to electronic medical records.

Larry Hettick: So, what's next for ZixOne? It's a relatively new approach. What are you guys going to do next?

Nigel Johnson: We love the idea of allowing people to see, process, and access their work productivity applications. We've started with the most useful tool that we have today, everything around Exchange. All companies are doing something with email and contacts and calendaring. And we can see that the world will continue to want something that has this very fast, quick, almost virtual approach.

We know that we have large companies like Citrix and VMware who tout this virtual world. But they don't do it well on mobile devices, and we do it extremely well.

Larry Hettick: Interesting. So, would you like to add any closing comments to our discussion summarize what we've talked about today, or what we've discovered?

Nigel Johnson: To have a really successful BYOD program, you need to let people have access to the tools that they use the most, in a way that doesn't detract from their experience

with their phone. And to do that, you need to have a solution like ZixOne, where you have – the company has a small footprint on the phone and employees know that the company can't see what they do, restrict their apps, or force them to change their behavior with their phone when they're not doing work.

Larry Hettick: Very good. Thank you. Patte, with that, that answers all the questions I had today. I'll turn it back to you.

Patte Johnson: Well, thank you, Nigel and Larry. Today's discussion was most informative. It has provided interesting thoughts to address the concerns of many, and we encourage our listeners and readers to post your questions and comments regarding this podcast on our website. Thank you for joining us today.

THE END

**Discussion has been edited for clarity.*

Webtorials® is the premier Internet site for IT-related education and resource-sharing. We provide an interactive communications platform that unites all members of the broadband networking and IT ecosystem: enterprise and small/medium-size business (SMB) IT professionals, solutions companies, service providers, analysts, consultants and press. Here, they all share their favorite documents, exchange problem-solving tips and participate in community discussions.

For over 15 years, Webtorials has provided its worldwide community of networking and IT professionals with a wide range of resources, including **White Papers**, **TechNotes™**, **Thought Leadership** , and **Research Reports**.

For editorial questions and concerns, please contact **Steven Taylor**.

For questions concerning marketing and highlighting your products on Webtorials, please contact **Sales@Webtorials.com**.

About the Webtorials® Editorial/Analyst Division

The Webtorials® Editorial/Analyst Division, a joint venture of industry veterans Steven Taylor and Jim Metzler, is devoted to performing in-depth analysis and research in focused areas such as Metro Ethernet and MPLS, as well as in areas that cross the traditional functional boundaries of IT, such as Unified Communications and Application Delivery. The Editorial/Analyst Division's focus is on providing actionable insight through custom research with a forward-looking viewpoint. Through reports that examine industry dynamics from both a demand and a supply perspective, the firm educates the marketplace both on emerging trends and the role that IT products, services and processes play in responding to those trends.

For more information and for additional Webtorials® Editorial/Analyst Division products, please contact Jim Metzler or Steven Taylor.

Published by Webtorials Editorial/Analyst Division
www.webtorials.com

Division Cofounders:
Jim Metzler
Steven Taylor

Professional Opinions Disclaimer
All information presented and opinions expressed in this publication represent the current opinions of the author(s) based on professional judgment and best available information at the time of the presentation. Consequently, the information is subject to change, and no liability for advice presented is assumed. Ultimate responsibility for choice of appropriate solutions remains with the reader.