

How to navigate the complex BYOD landscape



Bylise van den Berg

5 Nov 2014

The recent BlackBerry Experience Executive Forum, in partnership with ITWeb, provided practical and actionable insights into the latest issues, trends and developments in enterprise mobility. Keynote speaker, Head of Security at BlackBerry, Nader Henein, shared a few lessons learned from his and BlackBerry's experience with Bring Your Own Device (BYOD) customers.

It's been about two years since BYOD has been trialed, tested and deployed in companies. According to Henein, it has been a big pain for some, and, in some cases it's just ended up being far more expensive than originally envisaged.



© Roberto Rizzo - 123RF.com

The promise vs the problem

"The promise was that it would save you money. It sounded good on paper. The problem came when you had to maintain this, because initially you had one guy, the one guy who had more mobility. He had a BlackBerry, because back in the day it was what people in the enterprise space used. Then you had to go and hire more people or upskill existing people on iOS, Android and Windows phones, and you were not really sure what's going to come next, because, in the consumer space, things move a lot faster than in the enterprise space. If you remember 20 years ago, enterprise innovation drove consumer products: desktops started out in the enterprise space - they were very expensive and then made their way into our homes."

Things have changed a lot in the past 20 years in the technology space. Today we have to maintain so many things in the enterprise space that come from the consumer space. "Either you are going to hire more people, or you are going to upskill the people that you have to make sure that they can maintain those new operating systems and devices," says Henein.

It's a race against consumer innovation - which is really a very difficult race to run.



Regulation is not security

He says that many people mistake regulation for security. "Regulation is about compliance with a set of rules that ensure that a base-line is respected, but that base-line is the lowest bar. And you shouldn't really aim for the lowest bar..."

Companies should in fact aim far higher because that will ensure happy and satisfied customers, ultimately leading to more business for you. "Compliance is the stick, customer satisfaction is the target," says Henein.

It's therefore not the best idea to simply build products based on what you *think* your customers need - rather build products based on conversations. By finding out what customers want and need, and building products accordingly, you'll get a much greater return on investment on your spend and you'll be able to compete better.

When it comes to security, it all comes down to independent certification - how can you trust what a vendor tells you about a certain product is actually true? "A vendor's job is to portray their product in the best light possible. So why would you trust a vendor talking about a solution?"

"For this reason, we spend quite a bit of money, research and development and resources on certification." He advises that it's important when someone comes to you with a bunch of statements about their product, that you ask them to validate their statements with certification.

Modern-day threats

Henein identified three non-traditional threats enterprises must be aware of:

1. **Consumer applications in the enterprise space:** For example, most people have WhatsApp installed on their devices. Once you install it, it takes all your contacts, uploads it to its servers in Santa Monica, scans through your contacts, and maps them to the existing people who have WhatsApp. This is not malicious or wrong - it's the way it was built and it's clearly stated in the disclaimer.

"This is no problem at all in a consumer context, but in an enterprise context, that means you've shared all your customer details willingly with a third party," he explains.

WhatsApp is not malicious but it's a consumer application and that's what people need to remember.

2. **The 'good enough' approach:** This is when an enterprise adopts a solution with the attitude of "We've seen other people use it, so it must be good enough". This is setting the bar very low. Says Henein: "That's when you look at the compliance part and think that's what you have to aim for."
3. **Compliance vs overkill:** When it comes to compliance, we tend to think that an overkill is the solution - to lock everything down and then assume everything is secure. A locked down system is not doing anyone any favours and is not the solution.

Companies shouldn't overkill on compliance or on security. It should be unlimited capabilities for the end-user and at the same time no compromise on security.

The rise of shadow IT

Another point Henein highlighted is the rise of shadow IT - when people within an organisation start sharing work files among team members via a third party server such as Dropbox. He warns that the issue with this is that the files may contain sensitive or confidential information about your company or even the company you are doing business with.

His advice to be particularly aware of free services - nothing is ever really free. With free services things can actually become quite complex in terms of who actually owns the information.

When it comes to shadow IT, the first reaction most IT people have is:

1. **Data leak protection (DLP):** They feel they have to control the situation by blocking Dropbox or any other similar free services from the internal network.
2. **The requirement:** DLP is good, but it is better to figure out what the requirement is that is driving people to use these services. Did they approach IT? Is there a backlog in the IT department? Find out if there is a need for this internally.
3. **The delivery:** If you tell someone that you can offer them a Dropbox-like service where you can share information securely internally but it's going to take longer than a month, and have a cost attached to it, they will simply go back to using Dropbox. Therefore, speed of delivery is very important.

What to do from here?

Henein left attendees with the following advice on how to approach this landscape going forward:

- Set the bar high; aim for better security and better products. More employees will thank you for it, your customers will appreciate it, and you will do better business.
- Develop and REdevelop your mobile strategy *always*. "A strategy that is working today is not going to satisfy you in six months - so always redevelop. This also applies to your vendors. Whenever you are picking a solution, ask your vendors for their roadmaps - what they can offer you in six, 12 and 18 months, a list of features that are coming. You have the right to know what's coming next."
- Do your own homework. There are many analysts out there who want to give you their opinions. Remember that it's opinions and that they are all coming from different markets. Come to your own conclusions.
- Keep it simple. Piling solutions on top of solutions creates complexity that only one or two people in your organisation can understand and that is not the best way to move forward. A simple solution is much easier to maintain.



Nader Henein

■ ***You mentioned that it's been about two years since BYOD officially kicked off, that it's been an immense pain for some, and become far more expensive for others. What are your future projections for this landscape?***

Nader Henein: Well, there's not going to be any shortage of mobile devices or tablets if you look at the market today. That over-complicates the BYOD approach because someone will go on vacation to Japan and come back with a device and an operating system nobody has ever seen. If they are someone in a senior position, they will walk up to the IT department and tell them to make it work for them. So, BYOD is going to continue to increase.

What businesses are doing now, and I believe more and more will start doing, is adopting the Choose Your Own Device (CYOD) approach. Because organisations can't support all the devices under the sun, they test and select a series of devices which they will support and create a list for employees. That list is in constant change based on what's new in the market. This allows flexibility and some form of control to the organisation.

■ ***How would you compare enterprise mobility and the BYOD approach in South Africa to another African country like Nigeria with a very high mobile penetration?***

Henein: Countries like Nigeria are actually moving very very fast. The adoption rate is staggering. And Africa is in fact catching up to Europe as well. In Europe, the idea behind these sessions is that we take knowledge from the Middle East, from Africa, from Europe, from the US and all different parts of the world, and say this is what we've seen in terms of threats, in terms of experiences etc. Let's see if we can get ahead of the curve. Let's see if we can save you some of the pain that other regions have gone through and allow you to get ahead of that. So this is really the task of these sessions that we do.

So Africa I see moving forward very aggressively and that's good because you have a hunger for growth and you get productivity without having to go through the hurdles other regions had to go through.

ABOUT ILSE VAN DEN BERG

Ilse is a freelance journalist and editor with a passion for people & their stories (check out Passing Stories). She is also the editor of Go & Travel, a platform connecting all the stakeholders in the travel & tourism industry. You can check out her work [here](#) and [here](#). Contact Ilse through her website [here](#).

- #StartupStory: Aura security app to aid beleaguered Uber drivers - 13 Jul 2018
- #StartupStory: BlockMesh - 12 Jun 2018
- Taking telecoms to the next level: Who needs a long-term contract? - 4 Jun 2018
- Nokia makes a comeback in South Africa with new phones - 24 Apr 2018
- New Cape Town/Brazil subsea cable to boost SA broadband - 18 Apr 2018

[View my profile and articles...](#)

For more, visit: <https://www.bizcommunity.com>