BYOD - A Cloudy Adoption

Janine E. Mooney, Editor

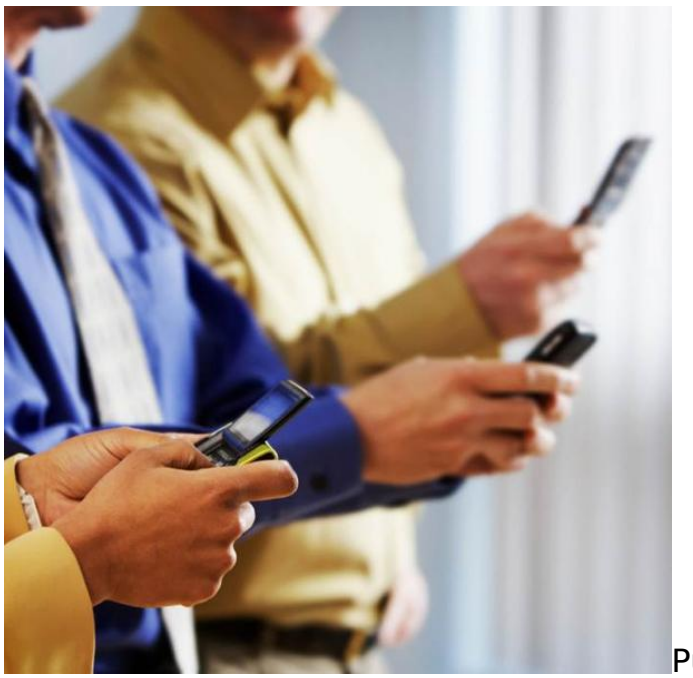
 Personal devices are popping up all over the office, and are quickly morphing from personal, to business and back to personal, all with the touch of a finger. Let's face it – from executives, to interns, employee's want access to their work at all hours of the day, every day of the week. Work is no longer a nine to five gig - employees must be "on" at (almost) all times. This is where the Bring Your Own Device (BYOD) initiative comes into play. Not only are employees insisting on connecting their personal devices to the company network, they are refusing to hand over control of the devices to IT security managers.

But can you blame them? Who wants the IT guy knowing what you're chatting about in personal emails and texts, who you're calling, or what photos you recently uploaded to Facebook?

Unfortunately for employees reluctant to hand-it-over, there is another side to the story. Ensuring data integrity is not an easy task for IT considering the traditional security issues associated with mobile devices, and now they have extra dangers to worry about with the addition of mainstream cloud services. Security managers have their work cut out for them as Malware creators can now gain access to loads of data on one network, which could tap into multiple mobile and fixed computers. This exposure to public cloud services is a risk that many companies may not be willing to take.

Companies also need to take into consideration the legal issues concerning the BYOD trend. Can employers legally monitor employee owned devices for data or

policy infringement, improper use of resources, device usage policies etc? Juniper Networks recently surveyed more than 4,000 mobile-device users and IT professionals. One surprising stat concluded: 41 percent of all respondents who use their personal devices for work are doing so without permission from the company.



Putting aside security and legal issues, it is fair to say that there can be significant advantages found in implementing a BYOD policy, such as, increased productivity in employees with customer-facing roles, lower costs and of course increased access for employees. Plus, BYOD devices tend to be more cutting edge, so you get the benefit of the latest features and capabilities.

Let’s look at retail and hospital environments, for example. The use of tablets can improve productivity immensely in answering customer questions, or make patient health-checks much easier and more time-efficient. This will certainly increase customer/patient satisfaction.

Next up – costs. Tablets are fairly durable (an IT delight) and, when ordered in bulk, tablets can have a fairly low corporate cost per unit, compared to laptops. At the same time, a BYOD policy can lead to less corporate control over what happens to the device, and concerns linger over physical security.

While the initiative might not be right for every company, it is quite compelling – but is it worth the hassle? Would you be willing to potentially sign away personal information to the IT department, or more importantly, do they trust you with a host of company data? Shifting the focus of the BYOD adoption, we must look at the productivity gains in the workplace, often thanks to the ability to access work anywhere, anytime. Mobile BYOD is one of the hottest trends in technology today, and with the big push from eager employees, BYOD could be implemented at a company near you – very, very soon.

June 1, 2012