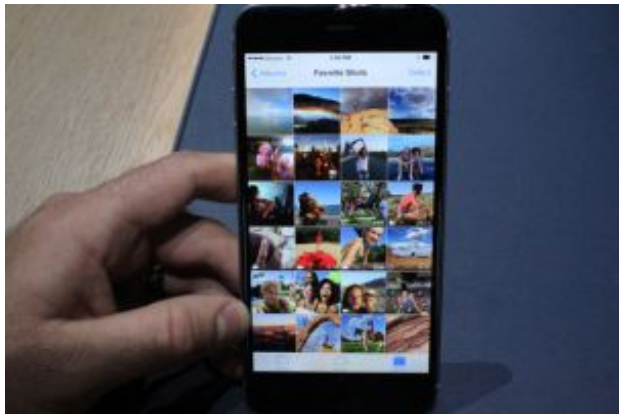
iOS 8 and iPhone 6: Businesses might not be quite as ready as their employees

By now, we have all become well accustomed to Apple's unique style when it comes to releasing a new version of iOS, a new iPhone, or other gadgets. Each release creates a lot of buzz, with crumbs and hints being strategically left to build anticipation and get people excited about what comes next.

Last week, Apple delivered a show that will probably have people lined up outside Apple stores once again.

How will the new features affect businesses?



Tech-savvy people will start updating iOS 8 within a few hours or days of its release. Others will buy the new iPhone 6 or iPhone 6 Plus and will probably want to bring their new toy to work to show it to their colleagues. This means IT administrators will go to work the next day and need to manage another version of OS.

Only two things can happen. First scenario: IT administrators will embrace the wave of change and seek ways to incorporate iPhone 6 and iOS 8 into their network. Second scenario: They will restrict the use of Apple's new technology, which would probably be a bad idea.

In the end, businesses want to keep their employees happy.

So, getting back to the first scenario. Let's see how businesses can benefit from the new features and what security measures they should take in order to safely allow employees to enjoy their new devices.

iCloud Drive: More documents in the cloud

To quote Apple: "The good news is you can work on any file, anywhere. The bad news: You can work on any file, anywhere."

iOS 8 now offers iCloud Drive, which can be a double-edged sword. Employees will be able to store any file types, from presentations and PDFs to photos and other documents, on iCloud Drive and access them from their iPhone, Mac, PC, iPad, etc. from the same iCloud account.

It's pretty similar to Dropbox, the main difference being that there isn't a dedicated app.

So, besides the obvious advantage of easy access, users will be able to share personal or business documents between devices, and it's most likely that confidential information will be uploaded to iCloud Drive among those documents. Some level of control has to be established to avoid highly classified information being uploaded onto a platform that's out of the company's control.

Let's face it: Even though Apple iOS, respectively its apps, are considered to be safer than other operating

systems/apps, data still ends up on a third-party platform, where our power is limited if anything happens with their security systems. Information security staff should pay attention to how they manage this type of situation and enforce internal regulations and immediately update their Mobile Device Management (MDM) and Data Loss Prevention (DLP) solutions when updates are available.

Hand-off: Does this feature sound encouraging to security people?

Integrating Macs into more businesses has been Apple's goal for some time now, which is why users expected them to announce new business-friendly features, such as Handoff.

With Handoff, users can start working on a Mac with Yosemite OS X and continue their work on their iPhone or iPad as long as all devices are connected to the same iCloud account. The same thing happens with SMS and MMS text messages: People can respond to a text message from any compatible Apple device.

Handoff is a pretty impressive feature and it will easily win users over. But the line becomes blurrier between work and personal life.

We cannot help but wonder whether this a feature you want all your employees to have access to.Like most good things, Handoff also comes with a cost.

Let's say that an employee is composing an email with confidential information on his/her iPhone and realizes that he/she wants to attach a presentation that's stored on his/her Mac. So, he/she switches to using the Mac to attach the presentation and finish writing the email, but suddenly, he/she receives a phone call. Unless he/she answers from his/her Mac – which is possible with the Continuity feature – he/she steps out of the office to answer the phone call on his/her iPhone but forgets to lock the computer.

In the meantime, a malicious colleague could easily copy the information enclosed within that email. Since Handoff depends on iCloud, once iCloud is disabled with a MDM solution, users will no longer be able to use this feature.

So, it's a matter of deciding the level of authorization IT administrators want to give to employees.

Apple Pay

This is just another feature provided by Apple that makes you wonder what else will they develop in the next iOS.

It remains to be seen if it's going to be a widely adopted feature. Although the number of card transactions is constantly increasing, there are still concerns and distrust in card payments. However, the fingerprint identity sensor adds a strong layer of security, and the fact that Apple Pay is backed by MasterCard, Visa and Amex could encourage people to use it.

Still, if businesses want to be on the safe side when employees or managers want to pay with Apple Pay using company cards, they should be ready to remotely wipe and/or block the device in case it is lost or stolen or to disable the option since this is allowed by iOS 8.

Overall, iPhone 6, iPhone 6 Plus, Apple Watch and iOS 8 present some interesting features which will help Apple maintain their fans' loyalty, at least until the next release. IT managers and administrators will probably have mixed feelings about these Apple advancements, knowing they will have an additional OS version to manage and more devices to handle.

Roman Foeckl is the founder and CEO of CoSoSys, a data loss and device protection company.
