Don’t let a BYOD policy create an OMG moment for your small firm

Many firms now let their employees use their own mobile device, like an iPad, for work. Although it might appear like an easy win for your small business, having a ‘bring your own device’ (BYOD) policy can create some risks for your business.
Don’t let a BYOD policy create an OMG moment for your small firm

Many firms now let their employees use their own mobile device, like an iPad, for work. Although it might appear like an easy win for your small business, having a ‘bring your own device’ (BYOD) policy can create some risks for your business.

There are some big advantages to having a BYOD policy: you don’t have to pay for the devices but your staff will tend to spend more time working on them while they’re away from the office, even if they’re checking their work messages before updating their Facebook profile.

But although these devices increasingly resemble mini-PCs, their security is almost certainly behind that of an average computer. This doesn’t matter much to you if your employees simply want to use one to keep in contact with their friends, but it is a problem if they use it for work, because these devices can be much more vulnerable to hackers than a laptop.

Cybercriminals are increasingly targeting mobile devices in the hope of stealing the owner’s banking details. But if they hack into one of your staff’s devices they might unwittingly find a wealth of confidential business data stored on it that could be far more valuable on the black market than the user’s credit card number.

That may sound far-fetched if your firm has only a handful of employees, but as computer security expert Tyler Durden recently wrote in a blog: “cybercriminals are not crazy cowboys with keyboards fighting for freedom of information anymore. They are businesses based around data and money stealing.”

As many of us have our own devices that we use every day for work “today is a true paradise for attackers,” says Durden.

So it’s important you consider tightening up security on the use of mobile devices in your firm.

**View a mobile device as a company PC or laptop**

People rarely bother to set up passwords on their mobile devices. You’d never let them do that with an office laptop or PC, so why would you allow them to do it with a smartphone or tablet which they use for work? Nearly half of UK adults use a mobile device for work, but barely more than a quarter of them have received any advice from their employers on how to use them securely or the risks they face of losing their personal data or having it stolen, according to a YouGov poll conducted for the Information Commissioner’s Office. It’s a good idea to encourage your employees to use a login on their mobile device that is at least the same strength as that on their work computer and to change it regularly, just like on their office PC.

**Encourage all your staff to use the same device**

It’s much simpler for you to keep on top of security updates for one manufacturer’s phones and tablets. If everyone has the same device, you know they will all need the latest security patch. Then you only have to send out one email to every staff member with a link to download it.

**Act quickly if a device is lost**

It would be very embarrassing for your firm to admit to its biggest client that you have lost an iPad containing some of its confidential data. But firms have just as much of a legal responsibility to keep people’s private data secure on their employees’ mobile devices as they do on their own IT servers.

The simplest and most effective method of eliminating any security risk to your firm is to wipe a device if it is lost. It's easy to do: you simply send it a message to delete all the data it contains. But you must tell your staff members that this is what you will be forced to do if they lose a device which they also use for work. You should also spell out what that means: that doing so would erase all their personal files, such as their music and photo collections stored in the cloud. They’re unlikely to be happy about it, but it might make them take more care of it if they know what the consequences would be if they lose it.

I’m not saying you shouldn’t let your employees use a mobile device for work. They’re great gadgets, which can make your employees feel like they’re getting a perk by working for you and allow them to work better while they’re on the go. But there are potential pitfalls in encouraging your team to use them, so you need to know how to protect your firm if a device goes missing.

**Author:** Matthew Webb, Head of Technology

**April 2013**