The perils of BYOD

(“Bring you own device”)
Or why it always pays
to read the small print

MANAGED
NETWORKS

The perils of BYOD

BYOD, or bring your own device, is the trendy acronym of the day. It refers to allowing – or requiring – staff to use their own kit for work. Most often it's smartphones, but it can also include tablets, netbooks, laptops, home desktops, cameras and so on.

It sounds like a cunning way to save some money – after all, this way staff pay for their own tools – while enabling today's tech-savvy consumers to use their favoured devices.

Naturally, there's a catch or two.

Most IT providers and departments tend to focus on compatibility and connectivity – in other words, getting your people's personal kit to work with your network. They're right – this can be complicated and, if you account for the time spent on it, more expensive[i] than providing them with a standard item.

There's also concern around security – generally concerns about making sure users don't bring viruses[ii] and malware along with their personal devices, alongside finding ways to keep company information confidential when it's being accessed by devices outside your control. Again, these are real concerns, with real – and sometimes expensive – solutions.

"Bring your own terms and conditions"

Something that people seem to think about less often is the other baggage that comes with consumer devices. It's less a case of "Bring Your Own Device" as "Bring Your Own Terms and Conditions".

When you buy a smartphone, you're not just buying a shiny piece of kit, you're buying a lifestyle. Or so the marketing people tell us. What that this means is that the phone is a gateway to a wide range of services that are more or less tightly integrated with the hardware itself.

It's pretty well impossible to use a smartphone, whether it's Apple, Android, Blackberry or Windows, without signing up to a whole range of added-value services. As a minimum, you're going to need an airtime contract and an account with the relevant app store.

Most personal phones will also have a personal cloud-based email service, like Hotmail or Gmail, and apps for a range of social networking services like Twitter and Facebook. Some people will also use iCloud, or Dropbox, or one of the other cloud storage services to look after personal files; sometimes this will integrate with apps on the phone – like the camera – to upload content as soon as it's created.

It's pretty well impossible to use a smartphone without signing up to a whole range of added-value services.

The perils of BYOD

Do you read the Ts&Cs before clicking 'Agree'?

Every time you sign up for one of these services, you agree to a legal contract between you – the consumer – and the service provider. It's that long screed of text in a scrolling box that you agree to without ever reading[iii]. In it will be all sorts of provisions around the location of and access to your data, including copyright, use in targeted advertising, and waivers of privacy. Most people are prepared to compromise on the privacy (and sometimes ownership) of their personal data in return for free access to cool services. Most don't expect any real guarantee of availability or confidentiality – beyond whatever they think the provider will put in place to protect their reputation – because after all, it's only photos, junk mail and status updates, right?

Except, of course, when you let the user hook their smartphone (or tablet, or laptop) up to your corporate network. Suddenly their work email and work files share storage and processing space with all this cool free stuff. More importantly, that data inherits the terms and conditions that the consumer accepted. So the free bundled on-line backup software on the laptop starts uploading your corporate files out into the cloud somewhere. The mail client starts using your internal email to target advertising. The camera uploads photos of the flip charts from your internal marketing workshop to sit alongside holiday snaps and embarrassing nightclub moments[iv]. And location-aware services are telling any app with access to that data where all your customers are whenever your staff visit them.

All of which should be enough to give you pause.

It gets worse. For instance, tablets make great media consumption devices, and their easy portability has led to much greater corporate adoption than was expected. But since they weren't designed to act as laptop replacements, they don't all have secure ways to get files onto the device, apart from using email. So staff who want to use tablets to work on presentations upload them from your corporate network to a cloud file storage provider, and then access that provider from their tablet. In doing so, they actively subject your data to the terms and conditions of that provider, and rely on that provider's security[v] – however weak – to protect it.

7,500 people literally sold their souls to Gamestation, an online games console retailer, when they agreed to its terms and conditions without reading them.

The perils of BYOD

Another thing – how do you know that they have a legal licence for every application, app, applet and service they're going to use to work on your data? Not only do consumers sometimes have a slightly more relaxed attitude to licensing than a well-run company can afford to but also lots of "free" apps specifically exclude commercial use of their free edition[vi] – most free virus scanners, for instance. Who's liable if it's discovered – why, you are, of course.

Can you manage this risk?

But maybe you think you can manage all of this with strong security policies and attentive oversight from your IT security team? You can certainly mitigate the risk, although BYOD is sounding less cheap by the minute, but there's one last sting in the tail.

What happens when people leave?

First of all, your data is on their device, which you don't control – and don't always have access to.

Secondly, it's out in their personal cloud. In some cases it may be very difficult to delete it even if the departing employee is co-operating.

Thirdly, they've been working on your documents using whichever apps were installed on their devices. Do you have access to those apps? Will every piece of content, and every piece of carefully-crafted formatting survive the transition back to your corporate desktop tools? It's hard enough marshalling multiple versions of Microsoft Office, before you throw in Pages, Google Apps, Open Office and all the others.

And worst of all? Let's say you're a Microsoft Exchange shop, and you use Microsoft ActiveSync to connect to your iPhones and iPads. It's easy, it's reliable, and best of all it allows you to remotely wipe your data if the phone is stolen or the employee leaves.

What happened to my phone?

So why the long face? Because when you use this feature, *it wipes the whole phone*[vii]. All of it. Your data, their data, apps, photos, you name it. Exactly what you want if the phone belongs to you. Less welcome if it's theirs, and quite possibly illegal unless you've very specifically asked them to permit it.

"The Microsoft licences needed to use a tablet with Office in a work environment will probably cost more than the tablet itself. For full flexibility, for example, an iPad user will need Microsoft licences that cost up to $1,000 (plus ongoing subscriptions, worth about $200 per year) to access VMs and remote desktop sessions running Office applications."

(Paul DeGroot, TechTarget)

The perils of BYOD

Before you get excited about saving cash and attracting hip young things by encouraging BYOD, here's five key check points:

1. Is your **contract of employment** or employee handbook clear about your rights to inspect, modify and delete all and any data on any device connected to your network? Do your staff know what this means?
2. Does your **security policy** properly cover use of company data on personal devices and in personal cloud services? Have you made sure staff understand this?
3. Do you have **the staff and expertise** to check each personal device to ensure it's clear of viruses and is properly licenced, and that your data is excluded from personal backups and intrusive apps? If your industry requires you to monitor or record web or telecoms activity, can you do this for personal devices?
4. Does your **acceptable use policy** extend to personal devices? How will you stop users looking at porn, or spending their whole day on Facebook, if they're using their own device?
5. Are you comfortable that your systems and policies will keep your **confidential data** secure even if it's released – deliberately or accidentally – into the public cloud?

If you're not comfortable with the answers to these questions, you might need to consider sticking to company-issued devices – or you could call us to help you deal properly with BYOD.

The perils of BYOD

Contact us

Managed Networks
6-8 Bonhill Street
London EC2A 4BX

www.mn.co.uk

info@mn.co.uk

0800 7836170

Connect with us

http://www.facebook.com/ManagedNetworks

http://www.linkedin.com/company/managed-networks

http://twitter.com/itsupport4smes

http://blog.managednetworks.co.uk/

Notes and sources

[i] http://reddevnews.com/articles/2012/07/12/byod-to-increase-it-costs.aspx
[ii] http://www.liebsoft.com/www_liebsoft_com/4_0/Pages/Press_Releases/Lieberman_Software_Survey_Finds_43__of_Companies_Worry_about_Employee_Devices_Introducing_Viruses/
[iii] http://news.cnet.com/8301-17852_3-20002689-71.html
[iv] http://www.apple.com/icloud/features/photo-stream.html
[v] http://www.informationweek.com/security/management/5-dropbox-security-warnings-for-business/240005413
[vi] http://free.avg.com/us-en/avg-anti-virus-7-licence-agreement-eula (see paragraph 1)
[vii] http://technet.microsoft.com/en-us/library/bb124591.aspx