

Managing the 'Bring your Own Device' (BYOD) challenge

Use of mobile devices in the workplace is on the increase, offering countless business benefits from improved efficiency to a fully provisioned mobile workforce. However, it presents challenges in taking care of your business critical documents, data, IT network and print output. Our Professional Services Manager, **Ian Fox**, gives us his insight.



Mobile technology is advancing at lightning speed and the majority of people can now get their hands on a shiny new gadget at relatively low cost. Likewise, many businesses are investing in mobile devices for their employees to reduce their need to print whilst boosting productivity - providing tools to engage whenever, wherever. However, some new challenges are presented when it comes to managing business critical documents and data that are accessed or created on the move.

So, how will you support workforce desire to use personal apps and devices while allowing them to be productive in a secure environment that protects your data? Here's my whistle-stop tour of tips for building your BYOD strategy.

1. How do we monitor BYOD on our network?

37% of information workers are using technology before seeking formal permission (Source: Forrester)

You might have a policy that requires your employees to ask for permission before plugging any old device into your network but let's face it, they're doing it anyway. The better approach is to accept this and put technology in place to let you see exactly what's going on. Various software packages are available that can detect mobile access to your network and there is often a lot more going on than you would imagine. Dave Helm, Sales Director of [Blue Logic](#), agrees; "With the right technology in place, no devices will sync with your systems without your IT department knowing about it. Just ensure you let your employees know that Big Brother is watching them!"

2. How do we print from our mobile devices?

Are your employees creating documents on the move but then getting frustrated when they can't print them? Sometimes we just need ink on paper and you could be seeing some fairly imaginative workarounds including people putting their iPads on the photocopier glass to try and get a snapshot of the screen (just in case you were wondering, that doesn't work!) The most common thing we see is emailing of documents to network accessible inboxes where they can be printed to networked machines. This is time consuming and can be overcome using new technology that wirelessly connects mobile devices to your printers.

3. Can we control print output from mobile devices?

The next natural question! Enabling printing on your network from mobile devices can create another problem in that you may find that you can't monitor and manage output volume, colour usage, paper consumption, specific user activity and so on, like you can on your networked machines. Print control software can be configured to help you with this, controlling and reporting on activity from iOS and other mobile gadgets in just the same way as on your networked machines.

4. Can we manage data security on remote devices?

You may be concerned about employees accessing your business systems and data remotely, or even losing devices outside of the office. We've all read chilling news stories about laptops left on trains and accidents do happen.

Tools such as remote desktops can safeguard your intellectual property by ensuring that data remains on your server. Dave Helm comments; "As the corporate database grows, security of that data becomes increasingly important. Using Windows remote desktop can secure any data from being downloaded to local devices".

In addition to this, electronic document management software can help by retaining files in digital format on your servers whilst monitoring what's happening to them and controlling user access. It's still important to have strong password policies to prevent unauthorized users accessing your data and there are systems available that can remotely wipe mobile devices if they do get lost.

5. Finally ... Don't just ignore it!

My final tip is to embrace BYOD because it's happening regardless of your ability to manage it and it could be costing your organisation in terms of finance and efficiency. If you face it head on, get your strategy and systems in order and keep things simple then you simply can't go wrong!



About Ian Fox

Ian Fox joined the Arena Group as a Systems Engineer in 1996. During his time at Arena he has gained a wealth of experience in helping organisations with their document related workflows. He now heads up the Professional Services department, which was formed in January 2011 with the aim of ensuring that existing and future Arena clients receive the best possible advice, solutions and support to enable them to manage and control their documents effectively.



the document experts

Arena Group Armitage House Thorpe Lower Lane
Robin Hood Wakefield WF3 3BQ
Tel - 0844 863 8000 Fax - 0113 2880671
E-mail : info@arenagroup.net

www.arenagroup.net

