psi
Publishing & Design
Celebrating 20 years | 1997-2017

Corporate Blog Post

Management on the move;
refreshing your mobile fleet smartly

Refreshing your mobile fleet requires a mobile fleet management program. Direct costs, End user costs and productivity gains are all possible

Executive summary

Managing staff devices in the workplace is a constant dance. How do you balance the latest and greatest with BYOD principles and let your staff work how and where they want to get the maximum benefit? Direct and user costs and balancing productivity all play a part.

Client:

Optus/Ogilvy.

Content type:

Post for the Optus consumer blog.

Brief:

To inspire business customers to think about the challenges and opportunities of refreshing their mobile fleet, and suggest tips on how to start.

Deliverable:

500 word blog post with strict parameters around sections, section lengths, SEO and keywords, social, key takeaways, related content, CTA, etc.

Among the myriad other considerations managing the mobile fleet in your organisation, security is one of the biggest. The devices allowed to access the company network and the apps and policies you deploy to do so need careful planning and constant attention.

It's now beyond debate – letting staff work when and where they want will maximise productivity across the board.

But managing their devices is a dance. In an era where your employees expect to use their own tools for work, you need to fortify a huge range of operating systems and applications or suffer one of many consequences (https://smallbusiness.chron.com/business-risks-insecure-networks-41202.html). Firstly, older devices are more vulnerable and might not be compatible with your software and data. And while a fleet of up-to-the-minute devices sounds great, some late model phones or tablets can slow down legacy software.

How do you find the happy medium?

In our dealings both with clients and our own mobile fleets we've identified three areas where a little cost/benefit analysis (of time and staff satisfaction as well as just money) can benefit.

Direct costs

First are the direct and accountable costs that come with devices and their life cycles. This can include purchase, delivery, set-up, connecting to organisational infrastructure (software access, security, etc), support, repairs and more.

The age of your fleet lets you project costs easily, so it makes upgrade and maintenance schedules comparatively straightforward.

End user costs

Then there are less tangible costs at the user end. After an upgrade, your staff need time to learn new operating systems or deploy and learn new software. Old systems need fixes, updates or troubleshooting. It all takes time, and therefore costs money.

BYOD devices are also subject to the risks of other apps and data staff have on their device. It's a potentially hidden cost you can avoid on company-owned devices since you can lock them down according to approved apps or use.

Productivity gains

But the secret sauce – and possibly the hardest metric to measure – is the money and time staff will save by working faster and smarter because they can access and action work data how and where they please.

A simple example is the amount of time it takes to perform a task on an older versus a newer device with a better system or app. But a more esoteric upside might be how much better people work because they're simply happier when they can work the way they want.

Take millennials and their famous attachment to their own personal devices. As this Wired story reports, (https://www.wired.com/insights/2014/09/millennials-mobile-security), BYOD policies favourable to staff are more important to their workplace satisfaction than many other factors.

The way forward

In a perfect world we'd standardise the entire mobile fleet in our organisation and give everyone the latest, fully-secured device as soon as it's available. But in the world we have, new models of popular handset brands come out yearly (or less) and cost upwards of $1,000 a time.

The best way to strike a balance is to have clear, well-established mobile device management policies. Trying to manage data access, security and everything else on an ad hoc basis is a recipe for disaster.

You *will* eventually slip up, and anything from a malware attack on an old OS to 'cloud creep' (where a staff member sends data through an unauthorised data service and exposes the whole organisation to risk) could bring your whole operation to a halt.

It's tempting to put mobile device management in the too hard basket, but an ounce of prevention being worth a pound of cure has never been more applicable.

Conclusion

Mobile management is like housework – you're never finished. A central pillar of your strategy should be regular reviews of the whole picture, and the time you put in now might save a lot of money later if a vulnerability rears its ugly head.

Fold the cost and time of your management plan into your ICT budget and your mobile fleet will stay as secure as it can.

Get in touch with our mobile fleet management experts to see how we can help or see the website for some practical tools to help. ■