Utelize®

Planning BYoD Beyond Device Security

Prepared by
Utelize Communications Limited
Managed Mobile for Business

www.utelize.co.uk

Why are you adopting BYoD?

Any organization ether considering or revisiting their BYoD policy will primarily and rightly be considering the security-related issues surrounding BYoD. Securing corporate data and applications, and deciding which variant of Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) software will best meet IT security requirements has been at the heart of most BYoD discussions for some time.

The MDM software has come a long way since 2011 when Gartner released its first MDM Magic Quadrant. Back then the "leaders" included Good, Mobileiron and Airwatch. Between 2012 and 2014 the market grew substantially, and a few joined the "leaders" however as of the latest 2016 report the key players still included Mobileiron & Airwatch closely followed by Blackberry (Blackberry acquired Good), Citrix and IBM.

The truth is that the software has matured. Most of the key vendors have comparable functionality, and whilst not widely accepted, the biggest real differentiator is now more about how an organization implements and manages its MDM solution and policies rather than the platform that it selected.

So, this article is going to place aside the MDM software debate and instead looks at a number of key day-to-day financial, administrative and HR challenges that cause BYoD policies and ambitions to fail, and encourages organisations to look beyond security before progressing with their BYoD plans.

Let's be clear, BYoD is still a confused message and it depends on who you talk to. Everyone has a different view of what it really means and what can be achieved as a result of BYoD. And by everyone, we mean even within IT teams in each organization, not just within different organisations.

There are arguments for cost savings, reduced IT support, improved employee satisfaction, increased productivity, enhanced business continuity. Each has, from what we can see, a solid case for adoption and an equally good case against case. In practice; however, defining exactly what BYoD means in your organization and why you are considering deploying a BYoD strategy is critical to avoid wasted efforts, resources and employee confusion.

So, we would recommend starting with an honest appraisal of the premise for BYoD adoption. Is it employee driven? Does it relate to mobile phones or is about having corporate email on personal tablets? Is it finance driven? If so, what assumptions or business case is the finance model based on? Is yours the type of organization that always provided staff with mobiles to perform their role – what changed?

Being able to clearly define where the demand or requirement really came from, and what benefits it will truly deliver to your organization and employees is critical. Just because a senior exec heard that company XYZ got rid of all their mobiles and went BYoD didn't mean it really happened that way, or importantly, was successful. This decision is not one to base on market or competitor hearsay, and in our experience, there is no free lunch on BYoD business case that is based purely on perceived finance grounds.

Who is paying?

If your organization currently pays for business mobile devices and airtime and you're moving to BYoD for financial cost savings, then it's important to understand the real financial impact. Not just on your bottom line, but on where the costs will actually go to. Assuming your people will still use phones, there will continue to be a cost, whether it is recognized on the budget line or not.

Will your organization instead provide the employee with a stipend or allowance? Or will it allow for mobile charges to be reclaimed in expenses? Will you insist the employee uses a corporate SIM? Or as some organisations are doing, are you simply mandating or enforcing BYoD with no expense or payment to the employee?

Depending on the model selected the organization may end up simply transferring its mobile costs from a central IT/mobile budget to a different and unclear expense budget. Or in some cases it's simply going to end up with costs being transferred to the end user (i.e. a pay cut). In many scenarios removing the corporate airtime contract actually has the reverse effect and drives everyone's costs higher where expenses can be claimed. As the real price consumers pay can often be higher for a corporate traffic profile.

The only scenario that exists where the business financially benefits, and the employee doesn't lose is where the employee already has their own unlimited voice/data package on their smartphone, and they only ever make inclusive calls for business, and they simply want to give up their legacy mobile, and avoid using two phones. Or where the business doesn't already provide a phone. BYoD does have a clear model with tablets, where many users will have invested in the tablet personally, and this offers the business an opportunity to benefit from this investment at relatively low cost.

BYoD Expenses Policy

For organisations that elect to reimburse their BYoD users for business related usage, then a whole new range of issues present themselves. Administering employee expenses relating to BYOD is complex. Determining business vs. personal cost; addressing VAT on charges, ensuring all employees accurately submit claims; the lack of visibility for costs and itemised data to validate claims.

All of these issues will ultimately lead to greater administrative costs which will often be hidden from view. It's also likely that where employees are allowed to reclaim business usage that the cost of that usage will be materially more expensive than corporate negotiated pricing.

Finally, if you are a UK based organization then currently whilst there is no income tax, national insurance or benefit in kind on corporate provided mobile devices and airtime, it's a different story for reclaimed mobile expenses. Currently if you simply reimburse employees for their mobile costs, or pay a fixed stipend or allowance, those payments are treated as taxable income. So, if you incur £100 of legitimate business costs on your mobile, then you're going to get taxed on that £100 if you're compliant in the treated of those expenses.

Who really funds the device?

BYoD, (especially in the UK), often misses the critical issue that most consumer mobile devices are funded not by individuals, but by mobile phone networks as part of a long-term contract. If employees can reclaim the cost of airtime incurred (partially or fully), then it's likely that the monthly network charge will include the cost of the device also.

For a typical UK smartphone user on an 'Unlimited' bundle, this device cost will represent £15-£20 per month of a £35 bill - so unless the expense policy is well-structured, the business risks paying for the device, negating a significant financial BYoD benefit for the business.

Where the business mandates that a corporate SIM needs to be used in the device, then in many cases the device is going to be locked to a different network, and unless the user bought the device outright then they will still have to continue paying their personal airtime agreement – so they possibly won't be able to user their device with a corporate SIM and with have little incentive to do so.

'Out of Bundle Charges and Recharges

Whilst 'Unlimited' domestic plans work well for consumers, who prefer a fixed monthly cost, the 'Out of Bundle' (OoB) charges, which are applied for usage in excess of bundle limits, or for calls not included in the bundle, can be very expensive compared to a corporate contract.

Calls to International and Non-Geographic destinations as well as roaming (especially outside of the EU) can be as much as 10 times more expensive than with corporate negotiated contracts. As a result, it does not take much out of bundle charging to drive costs back up.

Personal Usage on a Corporate SIM

If you're considering issuing corporate SIM's as a hybrid solution to address the cost issues with employee BYoD expense claims, then it won't be long before the issue of personal use becomes a real problem. Five years ago, the issue of personal usage was still largely focused on personal voice calls, today it's all about data consumption.

The average business email user with some browsing consumes about 250 – 500Mb of data per month. Personal usage drives this figure to between 1Gb and 2Gb for the typical user. However, where users have more consumer- focused devices (e.g. Apple /Samsung) and a quality 4G network, then usage in the 2Gb – 5Gb range is common.

Corporate shared data tariffs are not built to support high volume average data consumption, and individual user high volume tariffs drive up the corporate mobile costs too significantly. As a result; personal usage starts to quickly become a cost issue. For a corporate owned device, simply stating that personal usage is not allowed is one mechanism for dealing with this issue, however you can't tell a BYoD user that they can't use their device for personal usage.

So, any BYoD policy that involves the use of a corporate SIM is going to need to have a clear set of BYoD policies that make sense, and some form of charging mechanism to enable users to consume more personal data if they are going to be successful and avoid the corporate costs increasing significantly.

Damage, Loss, Repairs & User Support

The downside to touchscreen smartphones is that they are prone to damage and cost a lot more to repair and replace than legacy phones. If an employee loses their device, or it is broken, who is responsible for its replacement or repair?

Most consumers are oblivious to the real cost of replacing their devices without network subsidy. The cost can often range from £300 to £600, and the employee simply may not be able to afford, or be willing, to replace the device immediately - a major issue for the business, especially if it is the user's primary devices.

Establishing who is liable for repairs to devices damaged at work is also essential, to avoid future HR issues. If the damage is caused whilst performing work for the business – is the business liable?

Aside from the cost it makes sense to also establish processes for managing repairs, possibly through a centralized service. The alternative is that users waste significant time (business time) arranging for repairs and often they will be without a device during the repair. Having access to loan devices, reinstatement of email and company apps, and potentially a corporate streamlined repair service will all remove the impact of damage, loss and repairs when they happen or are needed.

Whilst the concept that employees will maintain and support their devices is, in theory, good for the business, the reality is that this burden will often be passed to an IT team as soon as there is a problem. Often that IT team may not have the tools/knowledge to support the device. Alternatively, the employee may spend significant, unproductive time addressing the problem, leading to greater hidden cost.

As a result, some organisations are limiting the BYoD programme to a defined list of devices, which can (a) be supported if needed and (b) better comply with the device security requirements of the business.

It may be that the real issue to be addressed, is that users want iPhones and high-end Android devices, however businesses simply don't have the budget for £500+ devices. So possibly the future lies in changing the finance model to a lease/rental model, where the business pays a flat monthly value, and the user can upgrade the monthly lease to support a higher value device. In effect a similar model to business car allowances.

That way the business limits its mobile device expenditure to an affordable level, devices can be standardised to a supportable range of devices, and users can choose to upgrade, but spread the cost monthly. This model is also now being adopted with inclusive insurance and end of life recycling to reduce the monthly costs.

BYoD Strategy & Planning

Planning for BYoD requires businesses to look at the wider picture of how mobile telecoms are managed within their organisation. To be successful, we recommend that organisations develop a joined-up strategy for Mobile Device Lifecycle Management that brings together Finance, IT, Procurement, and HR departments. Without this approach, BYoD can easily create new security risks, employee dissatisfaction, and excess costs.

Utelize – Managed Mobile for Business

At Utelize we specialise in providing managed mobile services that enable our customers to gain control of their mobile airtime, devices and security, helping them to:

- Streamline the administration of mobile airtime and devices
- Reduce mobile network and device charges
- Free up IT resources for more strategic projects
- Cost effectively finance mobile devices
- Secure mobile devices and data
- Manage in-life device repairs as well as end of life trade-in and device recycling
- Control mobile data usage and roaming charges
- Evaluate which mobile telecoms technologies and services can best support their business needs

To arrange a no obligation meeting and health check, get in touch …

E: hello@utelize.co.uk
T: 03300 240 444
W: www.utelize.co.uk

Utelize®