FREEFORM DYNAMICS

Inside Track Research Note

In association with

The Escalating Mobile Security Challenge

BYOD was just the beginning

August 2015

In a nutshell

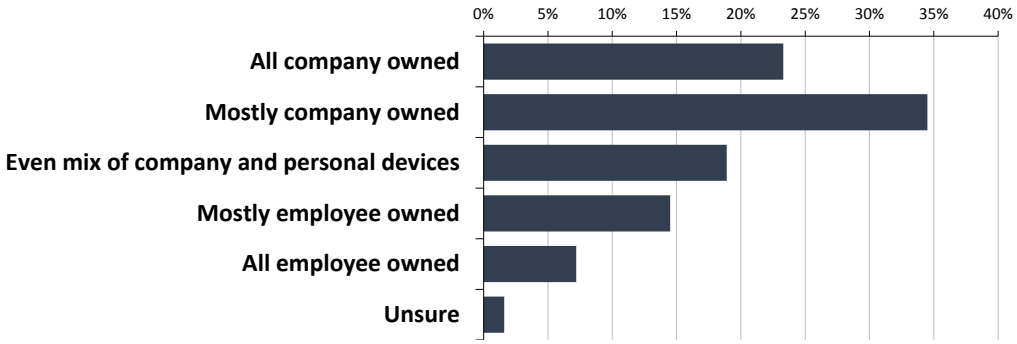
Just as IT professionals and others responsible for mobile security have come to terms with BYOD, the problem has moved on, with the lines between business and personal activity blurring even further. Against this background, effective management of mobile risk will increasingly require a user-centric approach.

Soothsayers mistaken?

Those who predicted that BYOD would take over the whole world of mobile working appear to have got it wrong.

Those who predicted that BYOD would take over the whole world of mobile working appear to have got it wrong. A recent research study (251 respondents) confirms that company devices still predominate in the business environment by a convincing margin (Figure 1).

Figure 1
How many of the mobile devices used to access company resources are actually owned by the company versus the employee?



The research also suggests that this picture won't change in a hurry. While the use of personal equipment is on the up, it is misleading to focus on this alone (as some commentators do). Study participants tell us that deployment of company devices is growing at approximately the same rate, and this is obviously off a larger base.

BYOD in perspective

The emerging consensus is that core business needs are generally best met through equipment procured, deployed and ultimately controlled by the company.

The truth is that mobile technology use in business is rising across the board. As part of this, BYOD has found its place among certain types of user, often in relation to non-essential secondary devices. However, the emerging consensus is that core business needs are generally best met through equipment procured, deployed and ultimately controlled by the company. This realisation is now acknowledged by many of those caught up in the original BYOD frenzy, hence the recent reduction in levels of industry noise on the topic.

If you are an IT professional involved in managing or supporting mobile activity this may seem like welcome news. Not quite as good as BYOD dying out altogether, but still better than the total anarchy some have feared. But don't relax too soon.

The emerging new reality

But don't relax too soon.

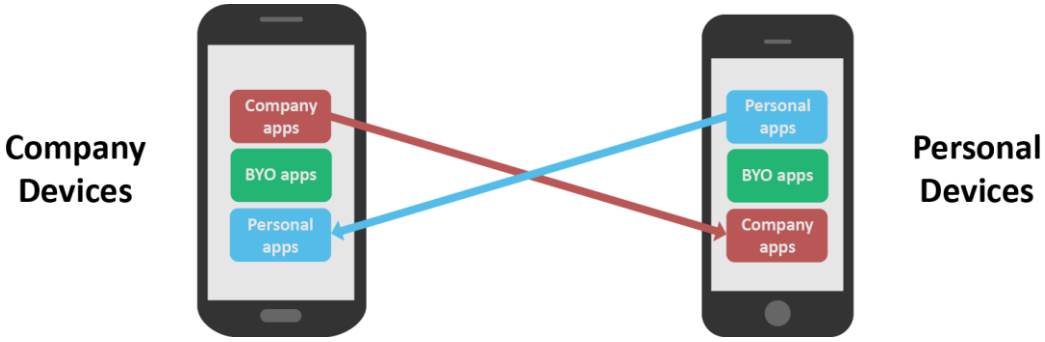
With all of the attention paid to BYOD, which is essentially about accessing business applications and services from a personal device, it's easy to overlook a parallel trend that goes the other way – the use of company equipment for personal purposes. As a simple example, over 60% of those taking part in the research said company devices were being used by a significant number of their employees to access personal email.

The concept of a pure business device is increasingly being challenged.

Put this together with employees using their company smartphone or tablet to access other personal messaging accounts, social media, and even entertainment content, and it's clear that the concept of a pure business device is increasingly being challenged.

Bring BYOD back into the equation, add in the use of user-selected software and services (BYO apps), and the picture we end up with is one of extensive crossover between business and personal assets and activity (Figure 2).

Figure 2
The emerging reality is one of extensive crossover between business and personal assets and activity



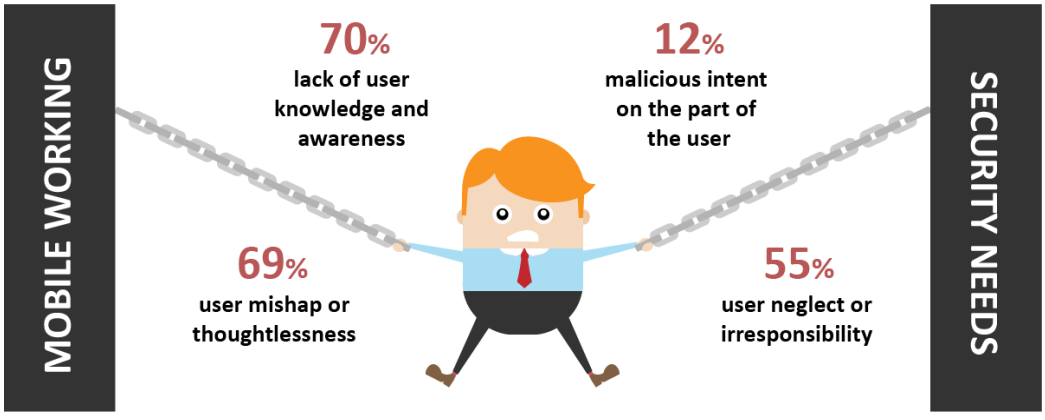
Against this background, who owns the device is probably the least of your worries from a cost and risk perspective.

Users are generally not brilliant at the best of times when it comes to protecting themselves and the business from IT-related risk.

The weakest link becomes weaker

Users are generally not brilliant at the best of times when it comes to protecting themselves and the business from IT-related risk. This comes through strongly in the research in relation to mobile security in particular, with respondents highlighting lack of user knowledge and awareness, along with general thoughtlessness, as the most common causes of exposure or uncertainty (Figure 3).

Figure 3
Employee-related sources of mobile security exposure or uncertainty



The risk of misunderstandings, misjudgements and accidents is higher than ever when the user's two worlds become intertwined.

The challenge here is aggravated when employees mix business and personal activity in the same environment. Personal apps are often used with an open, sharing mind-set, whereas anything that touches business data requires much more in the way of discipline and control. The risk of misunderstandings, misjudgements and accidents is higher than ever when the user's two worlds become intertwined.

As a result, the weakest link in the security chain arguably becomes even weaker unless you take appropriate measures.

Taking a hard line approach

One way of dealing with the challenges and risks is to go into lockdown mode.

One way of dealing with the challenges and risks is to go into lockdown mode. This could be done through strict policies that outlaw the mixing of business and personal activity, backed up by technology measures that restrict certain types of user behaviour. There's no shortage of options here, from basic mobile device management (MDM), through encryption, content filtering and access control technology, to full-blown enterprise mobile management (EMM) solutions.

Respondents in the research, however, alluded to cost and complexity problems with the lockdown approach. Pushback from users, and even security measure avoidance tactics (employees working around your attempts to constrain them), can then come back to bite if you get too heavy-handed.

Directly addressing the human factor

The best results seem to be achieved by those who blend technology protection with investment in user awareness and training programs.

The best results seem to be achieved by those who blend technology protection with investment in user awareness and training programs. In fact, given the choice between throwing lockdown technology at the problem, or focusing on user understanding and awareness, the evidence suggests that you should do the latter. This makes sense when you consider that no set of protection technologies can ever be totally 'fool proof'.

The bottom line

It can sometimes seem as if mobile technology has taken over the world of business. The reality, however, is that the majority of organisations are still only scratching the surface of the potential, and most IT departments are still figuring out how best to deal with the trends and developments we have mentioned.

Effective mobile risk management means working with and enabling users as part of the solution, rather that treating them purely as the problem.

While it's impossible to predict how activity will pan out in many areas, one thing for sure is that personal and business activity will become increasingly harder to keep apart, even with lock-down and control technologies in place. With this in mind, safe and efficient mobile working depends on addressing the human factor directly by finding ways to close the user knowledge and awareness gap.

It might go against the grain for some IT professionals, but effective mobile risk management means working with and enabling users as part of the solution, rather than treating them purely as the problem.

Further reading

If you are interested in reading more about the research referred to in this document, we would encourage you to download the study report entitled 'User-Centric Mobile Security', which is available from www.freeformdynamics.com or www.5app.com. You'll also find a more complete presentation of the research entitled 'Mobile Security without the Tears' on the same websites, along with an additional document 'Safe and Secure Mobile Working' which provides mobile security guidelines for end users.

About this document

The insights presented in this document are derived from an online research study in which 251 respondents (predominantly IT professionals) provided feedback on the topic of mobile security. Data from the research was interpreted independently by Freeform Dynamics. Previous findings from a broad range of other market studies were also taken into account, along with input gathered from ongoing briefings with IT vendors and service providers.

About Freeform Dynamics

Freeform Dynamics is an IT industry analyst firm. Through our research and insights, we aim to help busy IT and business professionals get up to speed on the latest technology developments, and make better informed investment decisions.

For more information, and access to our library of free research, please visit www.freeformdynamics.com.

About 5app

At 5app, we love simple and straightforward. Our goal is to help employees overcome their 'data overload' and find what they need, when they need it.

We understand the challenges mid-market companies face when trying to embrace a mobile enabled workforce. The consumerization of IT has resulted in the perennial problem of a 'digital overload'. So many apps to choose from, so many ways to find and store content. This is a major problem for data security, and a massive headache for IT.

We offer businesses a unique solution. Utilising our mobile application management background and adding into the mix our ability to curate and share all types of digital content, online and offline, The Digital Hub can help you achieve a simple and straightforward digital strategy. With our user centric approach employees will find the Digital Hub intuitive to use, easily finding what they need whenever they need it, without IT having to manage complex MDM solutions.

Our background as a company is steeped in the mobile world and we want to help organisations of all sizes embrace the benefits of mobile technology to create happy and effective workforces.

For more information, please see www.5app.com.

Terms of Use