FREEFORM DYNAMICS

Inside Track Research Note

In association with

5APP

Mobile Security and the Challenge of User Resistance

Striking the right balance

August 2015

In a nutshell

Mobile security is becoming more of a headache as the crossover between business and personal activity continues to increase, and employees generally expect more freedom. Research suggests, however, that you can only push technology-based protection so far before users rebel and try to find ways around it. To manage risks effectively, you therefore need to address the human factor.

Opposing pulls

Modern mobile devices are both extremely powerful and extremely versatile

Many IT professionals are of the opinion that the world would be a better place without mobile technology. Life was so much easier before users, particularly the more influential ones, discovered what they could do with smart phones and tablets.

One of the problems from an IT perspective is that modern mobile devices are both extremely powerful and extremely versatile. Users can connect them up to pretty much anything they want to very quickly and easily - unless, of course, you take steps to lock things down.

A big part of the appeal for users is the freedom, flexibility and convenience offered by mobile technology, so if the IT team constrains what they can do with their devices on risk and compliance grounds, much of that perceived value is undermined.

And there's the rub. A big part of the appeal for users is the freedom, flexibility and convenience offered by mobile technology, so if the IT team constrains what they can do with their devices on risk and compliance grounds, much of that perceived value is undermined. Conversely, if users are allowed to run amok and some horrible data breach occurs, then IT will have to sort it all out. They may even get blamed for not having the necessary controls in place.

Who wins and to what extent varies between organisations, and even between IT and different groups of users. Senior managers and other users with political leverage usually get their own way; it’s hard to say no to the person who controls salary rises and bonus payments, or the sales team that puts food on the table. Everyone else is fair game for locking down – IT can get its own way here, despite the disharmony likely to result among the users concerned.

A hollow victory?

While IT teams often yearn for a standardised, locked down environment, recent research casts some doubt on whether being allowed to implement this, even for a subset of users, can be regarded as a solid victory for IT (Figure 1).

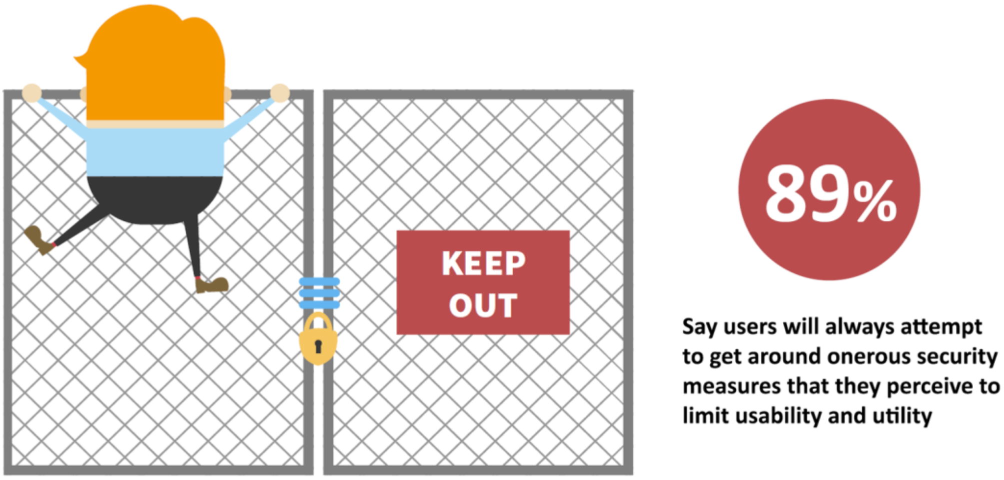
KEEP OUT
89%
Say users will always attempt to get around onerous security measures that they perceive to limit usability and utility

Figure 1
You can only push users so far, before you lose their cooperation and prompt them to find creative ways to undermine your efforts

The statistic we see here comes from a study in which just over 250 IT professionals provided feedback on various aspects of mobile security. It illustrates that users are not always as stupid as they sometimes seem. Try to get in the way of them doing what they want, and they can be pretty inventive about ways to get around the measures you have put into place.

Alien though the concept might be to some IT professionals, the evidence tells us that working with users rather than purely against them can create a safer mobile working environment.

Working with users, rather than against them

Against this background, findings from the same study suggest that the answer to this problem is not to get better at locking things down, but to adopt a different mind-set and approach. Alien though the concept might be to some IT professionals, the evidence tells us that working with users rather than purely against them can create a safer mobile working environment.

Sceptical? Well let's walk through it.

To begin with, many in the study reported they were using a range of technologies to help control the mobile security risk (Figure 2).

Figure 2
Many are implementing or exploring technologies to constrain user activity

Technology	Using	Exploring
Encryption of data on devices	58%	29%
Mobile device management (MDM)	47%	24%
Data loss prevention solutions	41%	35%
Anti-malware for mobile devices	39%	25%
Whitelisting of apps and services	33%	28%
Virtual desktop / workspaces	31%	24%
Blacklisting of apps and services	30%	30%
Hardware based security	22%	28%
Mobile app management (MAM)	20%	24%
Device partitioning	19%	31%
Biometric access control	10%	18%
Mobile app wrapping	9%	24%

Some had also taken steps to define usage policies and/or train and support employees to enable and encourage safer behaviour (Figure 3).

Figure 3
Policies are often in place, but are not always backed up with proper training and support mechanisms

65% **Have mobile-related policies defining what's acceptable and what's not**

48% **Provide training and support to help employees use mobile solutions safely**

Now for the sake of disclosure, we should point out that the numbers we see here in relation to both technology adoption and the presence of policies and training are likely to be inflated. Those with more of an interest in a topic are more inclined to fill out surveys on it. But that doesn't matter in the context of our discussion here – we can still legitimately look at how approaches correlate with outcomes.

During our analysis, we used the technology adoption data to identify the subset of respondents investing significantly in physical control and lock down. We ignored the presence of policies because we couldn't be sure of the form these took. Ringbinders gathering dust on shelves or documents buried deep in your intranet don't really get you anywhere. We therefore homed in on training and support.

Ringbinders gathering dust on shelves or documents buried deep in your intranet don't really get you anywhere.

When we netted it out, we ended up with four groups – those focused on technology, respondents emphasising training/support, those combining the two into a dual focused approach, and others doing little or nothing. We were then able to look at how well respondents in each group felt they were prepared to deal with evolving mobile security challenges. The picture that emerged was pretty striking (Figure 4).

Figure 4
The key to success is taking a balanced approach

CONFIDENCE vs **FOCUS**	Fully / mostly prepared	Only partially prepared	Not well prepared
Dual focus	**77%**	**20%**	**3%**
Focus on training	**44%**	**51%**	**5%**
Focus on technology	**12%**	**63%**	**24%**
No focus	**11%**	**47%**	**42%**

Not surprisingly, most (77%) of those with a dual focus felt they were in a good position. What's more interesting is that the group focused mostly on training and support on average felt significantly more confident than those relying mostly on control and lock down (44% vs 12%). In fact, comparing the bottom two rows, it would seem that simply throwing technology at the problem doesn't get you very far at all.

Simply throwing technology at the problem doesn't get you very far at all.

The bottom line

The reality is that most security risks associated with mobile technology stem from user ignorance. Non-technical staff just don't see the dangers as IT professionals do. Rather than write them off as being stupid or irresponsible, it therefore makes more sense to provide users with some straightforward pointers on how to be safe. Simple written guidelines coupled with short, sharp training delivered in context works well.

Technology-based measures still have their place, but don't just focus on lock down and control. Monitoring tools can help you spot undesirable behaviour and step in as appropriate. Equally valuable are enterprise versions of popular file sharing services and app stores, or better still, digital hubs that provide users with a safe one stop shop for key documents and software. One way to break bad habits is to give people something even more convenient than the service you are trying to wean them off.

All of the above is a long way of saying that there is no single answer to the mobile security challenge. It's about blending different measures in the right combination.

There is no single answer to the mobile security challenge. It's about blending different measures in the right combination.

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.

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 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