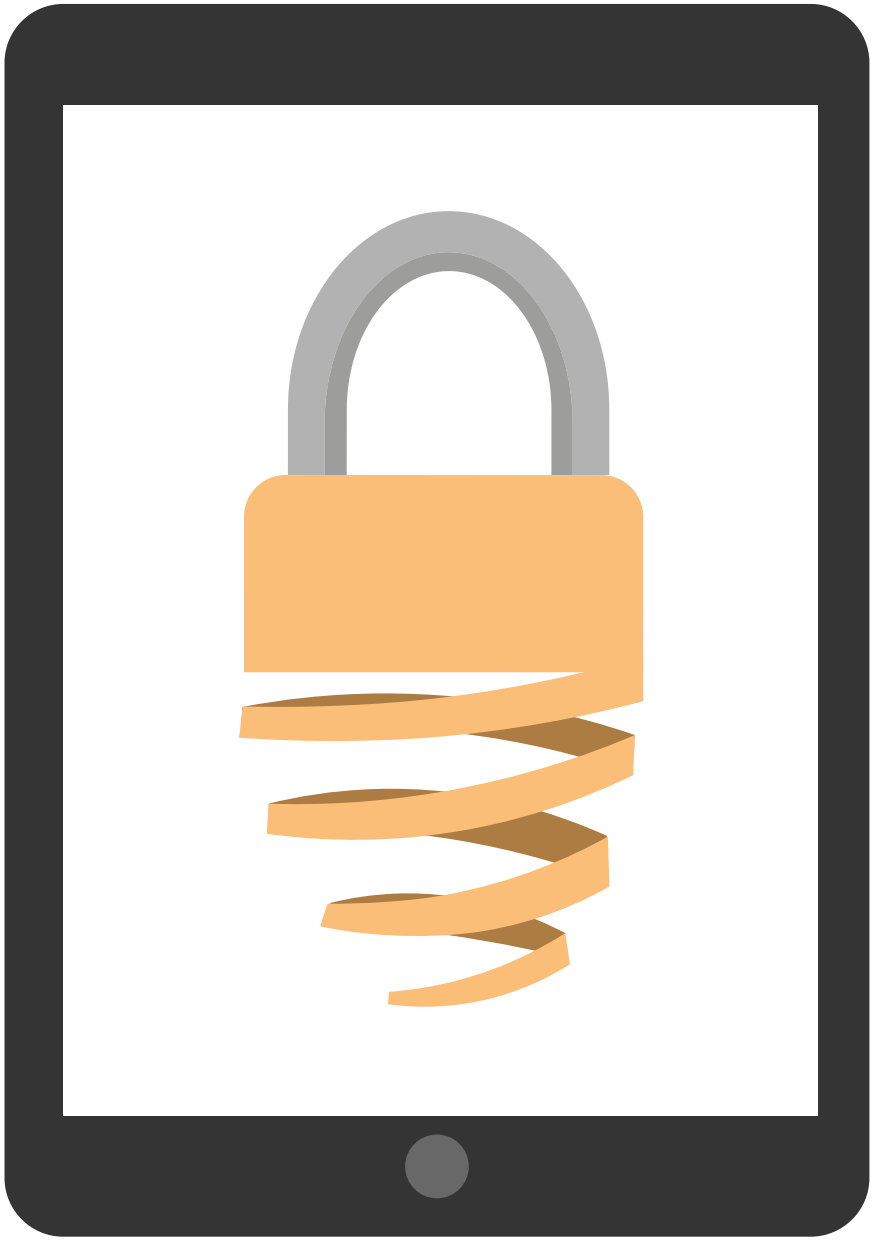
FREEFORM DYNAMICS

In association with SAPP



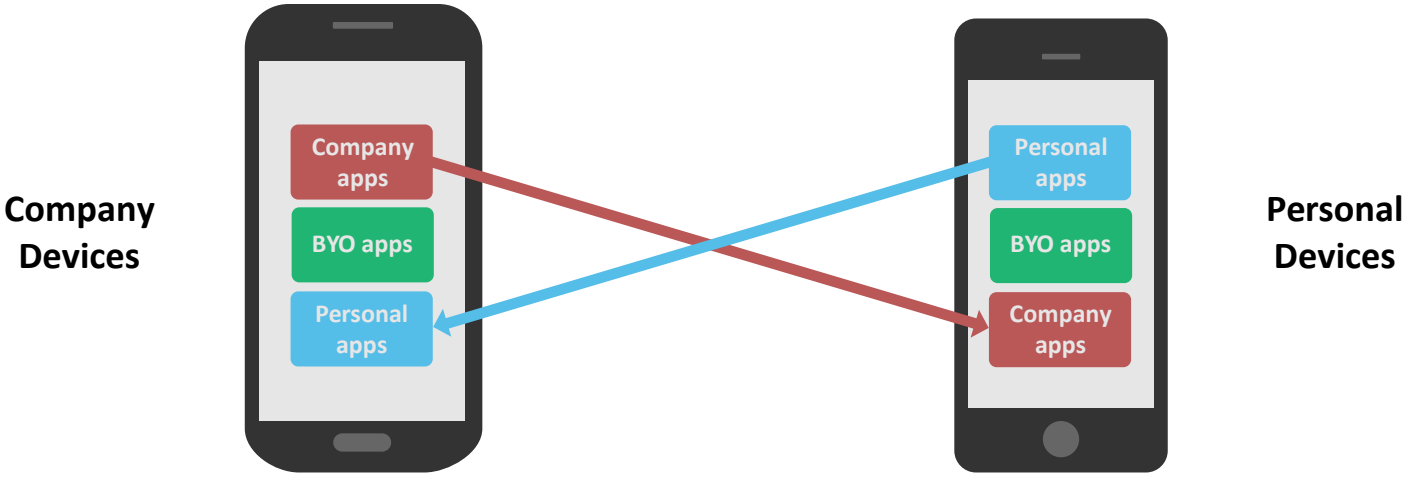
User-Centric Mobile Security

Don’t let the human factor unravel your efforts

Freeform Dynamics Ltd, July 2015

The Emerging Mobile Reality

Personal and business are increasingly inseparable



Not so long ago, many were speculating that 'Bring Your Own Device' (BYOD) would define the future of end user computing. Most organisations today, however, see a role for both company and employee owned equipment to meet the wide and varied range of needs and preferences that exist within the workforce. Meanwhile, it's becoming clear that the question of device ownership is only part of the discussion anyway. The emerging reality is that regardless of who owns a smartphone or tablet, the chances are that it will be used for a mix of both personal and business activity, the latter being based on both company-deployed and employee-selected (i.e. BYO) apps and services.

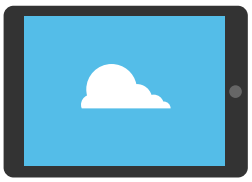
Significant cross-over has already taken place

70%

Access business email on a personal device

63%

Access personal email on a business device



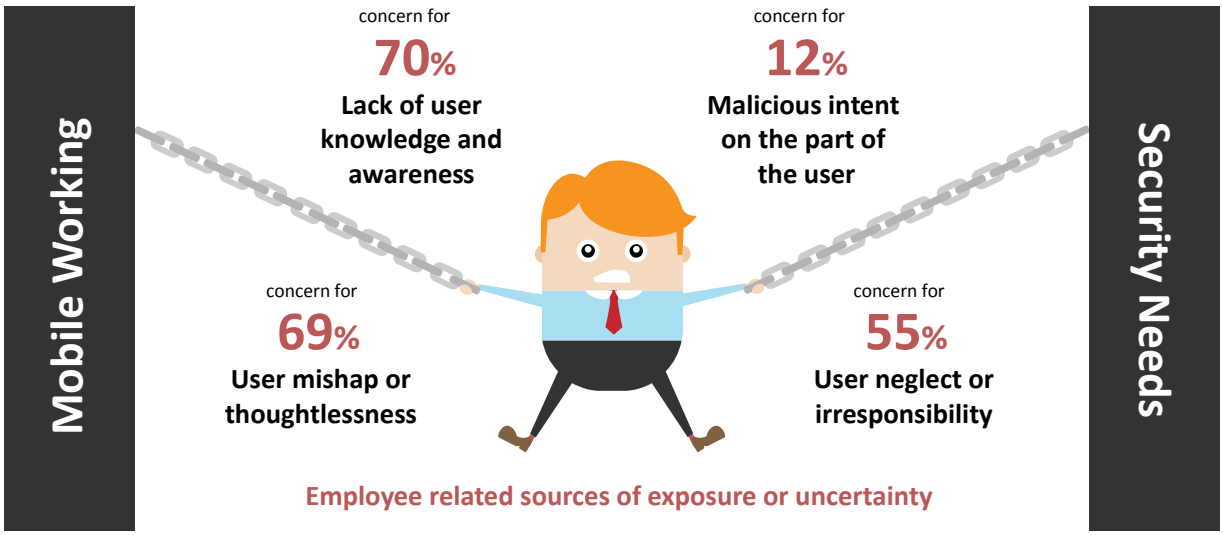
Over 40%

Use BYO cloud services on their chosen device

The crossover of business activity to personal devices and vice versa comes through in our research. 70% of the business and IT professionals taking part in a recent study, for example, cited significant levels of business email being accessed from personal equipment. 63%, meanwhile, reported a significant number of users accessing personal email from company devices, with similar crossover observed in other application areas. If we add to this over 40% seeing the use of BYO cloud, employees can easily end up with a device full of apps and data stores that are subject to different security requirements and used with different mindsets and levels of discipline. This translates to an accident waiting to happen unless risks are properly understood and managed.

Understanding the Risks

Users quickly become the weakest link in the chain



Employee related sources of exposure or uncertainty

It's great to see people making as much use of their mobile devices as possible. As they add more apps, services and data, however, mixing business and personal activity along the way, they aren't always aware of the risk implications and the need to think before acting in order to avoid mishaps. It's therefore not surprising that around 70% of study respondents report exposure or uncertainty arising from such issues. Malicious intent is far less of a problem, though 55% call out irresponsible behaviour as a challenge. The latter is often down to users knowing they shouldn't really do what they are about to, but under-estimating the consequences and going ahead with it anyway.

User-created vulnerabilities lead to greater exposure

Loss or theft of inadequately secured devices — concern for **64%**

Inadvertent sending or copying of sensitive data — concern for **64%**

Phishing and other deception methods — concern for **67%**

General malware infection — concern for **55%**

Device hacking and other direct forms of attack — concern for **38%**

Other sources of exposure or uncertainty

Shortcomings in user awareness, responsibility and general behaviour manifest themselves in terms of increased exposure to a range of specific risks. Lost or stolen equipment is never a good thing, but the business risk is minimal if data is encrypted and the device is appropriately locked. It is therefore telling that 64% highlight exposure in this area from inadequately secured devices.

Similar numbers point to mistakes made while handling sensitive data, as well as users falling foul of phishing and other deception methods - both aggravated by poor knowledge and awareness or lack of thought on the part of the user. When it comes to more direct attacks through malware infection or hacking, aggravating issues here range from users downloading malicious apps or visiting dangerous websites, to vulnerabilities resulting from poorly configured or unpatched equipment.

The point is that most threats are compounded when personal and business activities are mixed, and the consumer mindset takes precedent.

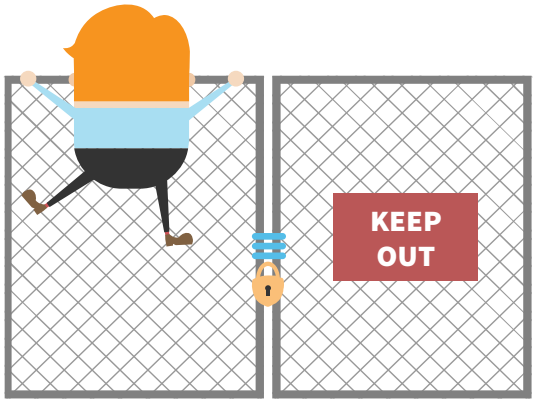
Dealing with the Challenges

Many are focusing on lock-down and control techniques

One way of dealing with the challenges and risks is to implement technology designed to lock-down or control user activity, or to mitigate the risk when problems arise. Myriad solutions of this nature are available on the market, and the research tells us many IT teams have implemented or are exploring these in an attempt to constrain what users are able to do or access with their mobile device.

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%

But you can only push a strategy of constraint so far



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

The problem with the lock-down and control approach is that it can lead to a false sense of security. It might feel as if the more measures you put into place to prevent employees doing risky things, the better the business is protected, but the opposite is often true. If you put too many barriers between users and what they want to do, you just motivate them to find ways past your locks and limits. Furthermore, the heavy-handed approach can easily lead to resentment and even less willingness to cooperate.

Given that 89% of the respondents in our study acknowledged this principle, the problem here is obviously well understood. So does this mean you simply back off, relax the controls, and compromise on the level of effective risk management?

Exploring different options

Some are addressing the human factor more directly

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

Technology-based protection measures can clearly be backed up with HR policies defining what's acceptable and what's not in terms of user behaviour. These are often written in a 'regulatory' manner, e.g. making it clear that certain actions constitute a disciplinary offence, with warnings and penalties defined in relation to policy breaches.

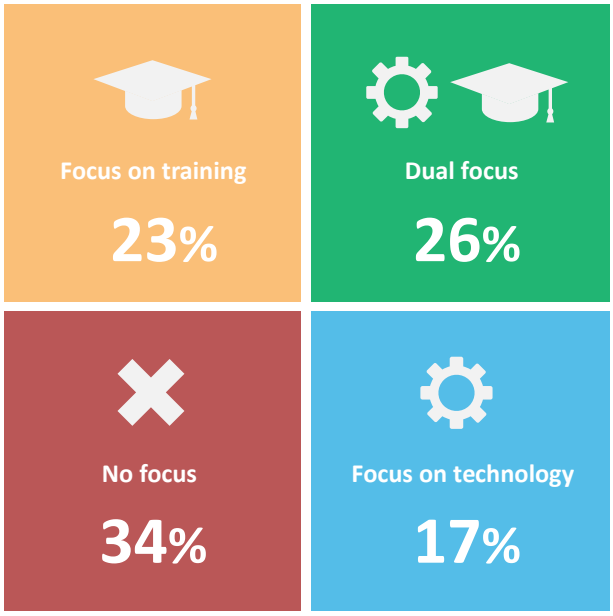
Defining boundaries and consequences in this way can be useful to send a message about the importance of security, and 65% in our study said they were taking this approach. Given that prevention is preferable to punishment, however, these policies would ideally be accompanied by training and support. The aim is to raise awareness of the issues and to both encourage and enable the right behaviour. Obvious, perhaps, but only 48% do anything meaningful in this area, and even within this the level of emphasis often isn't that high.

Organisations vary in terms of overall focus

Organisations vary considerably in terms of where they have focused their efforts in relation to mobile security. This is consistent with the rapidly evolving nature of activity, needs, technology and best practices in this area.

In order to explore this further during our analysis, we concentrated on two key dimensions - whether an organisation had put a significant level of focus on training (and subsequent support), and/or whether significant investments had been made in technology to control or lock-down user activity. Organisations were considered to qualify for the latter if they had implemented four or more of the technology-based control measures listed previously.

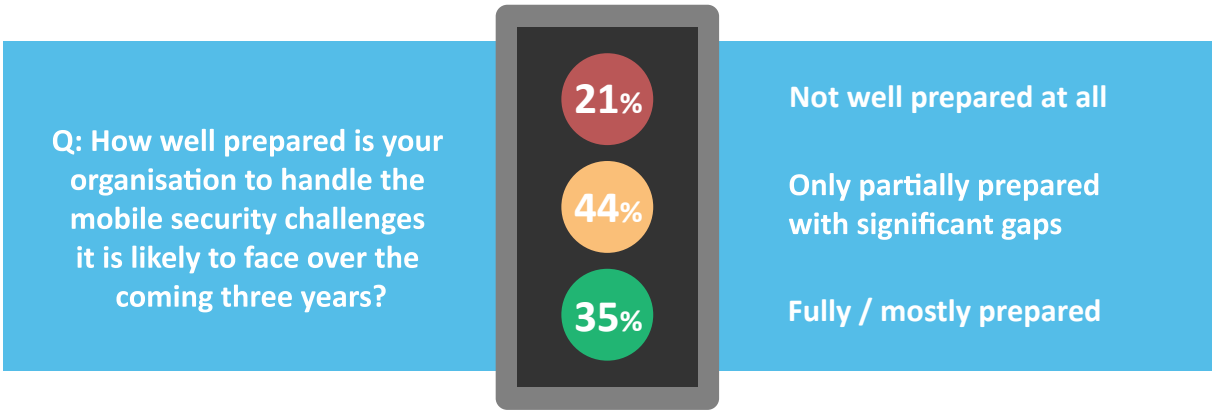
Of course these two types of effort and investment, are not mutually exclusive, so when we analyse the data we end up with a quadrant as shown to the right. This provides quite a nice high level illustration of how approaches vary. 23% focus predominantly on training and support, 17% direct their efforts almost exclusively at technology-based control, with 26% bringing the two together into a dual focus strategy. Meanwhile, the largest group is made up of those with no real focus on any aspect of mobile security at all.



But does any of this matter? The answer becomes apparent when we look at the results achieved by each of the groups in our quadrant.

Homing in on what really matters

Some achieve much better results than others



A good proxy to use for results is how prepared people feel to handle evolving risks. Overall, 35% said they were fully or mostly prepared (only 7% said 'fully' within this), with the remainder highlighting significant gaps or candidly admitting they weren't well prepared at all. This high level view illustrates the work still to be done within the mainstream business community. When we break out the data and look at how the approach taken to mobile security impacts confidence, however, we gain a good perspective on what's important to achieve results, i.e. to protect the business well.

Success stems from blending enablement with control

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%

The numbers we see here speak for themselves. Working up from the bottom, those with no focus on any aspect of mobile security not surprisingly fair the worst, with only 11% citing a good level of confidence (blissful ignorance?). An important finding, however, is that those simply throwing technology at the problem don't seem to do much better (12% fully/mostly prepared). Enabling users through training and support (even with limited technology measures in place) does drive results (44%), however real confidence (77%) comes from taking a dual focus approach.

Conclusions and recommendations

It's critical to appreciate and accept the new reality

This recent survey sharpens the view of a new reality that has been steadily emerging over the course of a number of Freeform Dynamics studies[1,2]. A few years ago, we saw some initial challenges to the status quo as a result of increasing consumerisation in the IT space. This evolved into a frenzy of hype from marketeers and pundits around BYOD, with some even predicting the demise of central IT teams as a consequence of users taking control.

Not surprisingly, many IT professionals pushed back, expressing strong feelings about the dangers of user anarchy in relation to mobile technology, highlighting data leakage and elevated support costs as particular risks. The view often expressed was that BYOD was false economy in the long run.

Since these debates, a measure of balance has entered the discussion. As it turns out, neither the evangelists nor the naysayers are proving to be universally right. The answer to whether company equipment or the BYOD approach makes most sense for mainstream businesses is "it depends". Both are likely to have their place in your workforce, and which is appropriate where will be driven by the user types and use cases that exist.

However, the new reality says that regardless of device ownership, you should expect, and make provision for, a degree of flexibility when it comes to how smartphones and tablets are used. This includes the accommodation of business and personal activity taking place on the same device, and the use of BYO apps and services.

Lay the right foundations sooner rather than later

It can sometimes seem as if smartphones and tablets have been with us forever, but the truth is that most organisations are still in the early stages of their mobile journey. Whatever is going on in your workforce today, you can be sure that over the next few years usage levels will escalate and usage patterns will change.

If you are going to keep up with evolving demands, and the inevitable risks that will accompany them, you need to lay the right foundations sooner rather than later. As the research suggests, success will depend on striking the right balance between control and enablement.

One of the challenges you will face in the short to medium term is the fast-moving nature of the mobile technology marketplace. Whether it's to do with the devices, apps, and services used within the business, or the solutions implemented to provide technology-based protection, new options and industry jargon are emerging every few months. The advice is therefore to assess and invest in line with your own requirements, and not be led by fashion.

And as you explore what's on offer, beware of overkill solutions that are complex to implement and manage, and risk locking you onto a path that may constrain you down the line. Given that control and lockdown technologies are only part of the equation, the trick is to implement just enough, and leave time and resources to directly address employee enablement. If you don't do this, you run the risk of the human factor unravelling all your good efforts.

When it comes to user training and support, apart from the necessary policies and processes, it is worth looking out for solutions that can help to automate and monitor the provision of learning material and policy-related reminders in context. The better you enable users to help themselves, the more the business will be protected.

Further reading

The following reports and papers are available from www.freeformdynamics.com

1. The Politics and Practicalities of End User Computing
2. Freedom without Anarchy: Empower your users while maintaining control
3. Mobile Working without the Tears

About the Research

The research upon which this report is based was independently designed and analysed by Freeform Dynamics Ltd. Data was gathered via an online survey executed in collaboration with a mainstream IT news site. 251 responses were gathered from business and IT professionals across a range of industry sectors, geographies and organisation sizes. The study was sponsored by 5app. If you would like to take a more detailed look at the research presented in this report see:

Mobile Working without the Tears

Download for free from: www.freeformdynamics.com

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, 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 visit www.5app.com