FREEFORM DYNAMICS

Community Research Report

In association with

5APP

Mobile Working without the Tears

The need for a user-centric approach to mobile security

July 2015

Management Summary

As both company and personally owned mobile devices are increasingly used in business, understanding and dealing with the associated risks has become a significant concern for many. But is the answer to just throw the latest security and management technology at the problem, or are other measures required?

Key points

The trend towards mobile adoption in business is clear

In a recent research study in which input was gathered from over 250 IT and business professionals, 4 out of 10 respondents reported that 'most' or 'all' of their workforce are using smartphones or tablets to access company applications, services, documents or data. The majority of devices are company owned, but a significant number of employees are using their own devices for work purposes (BYOD).

Personal and business activity are becoming mingled

Hooking into corporate email from personal devices is prevalent, but so too is accessing personal email on company equipment. Beyond this, a mix of official and unofficial apps and services are being accessed on most devices, regardless of who owns the technology. This can lead to potential security issues if left unchecked.

An inclusive approach to mobile management is required

With the research showing use of both company owned devices and BYOD being set to increase, our study respondents generally favour an inclusive and consistent approach to mobile security. The consensus is that it shouldn't matter who owns the device; the mechanisms and standards in place should be the same.

There are no magic bullets in terms of technology

Enterprise Mobility Management (EMM) solutions promise a comprehensive range of capability delivered in a pre-integrated manner, but most are not yet fully mature or complete. Meanwhile, study respondents are mixing and matching point solutions, an approach that will probably be necessary for some time to come.

Beyond technology, attention must be paid to users directly

The research confirmed that end users are the biggest source of risk when it comes to mobile security. However, this is more to do with ignorance, thoughtlessness or neglect rather than malicious intent. IT can help by defining safe ways of working and developing relevant guidelines, but senior management air-cover is necessary to ensure policy enforcement and adequate funding for security related investments.

The rounded approach is best, but training trumps technology

You can invest in technology to create a safer IT environment and/or train users to work in a safe and secure manner. Organisations that pay attention to both areas are significantly more likely to feel better prepared for the future with respect to mobile security challenges. However, if you have to prioritise, then the evidence suggests that training your workforce will produce better results than simply throwing technology at the problem. These findings confirm effective mobile security must address people issues as well as IT systems requirements.

About this Report

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.

Introduction

Advances in communications and devices have opened the door to new ways of working.

Mobile computing is currently one of the hottest topics in the IT industry. Advances in communications and devices have opened the door to new ways of working. This leads to significant business benefit in terms of both efficiency and effectiveness. But mobile working comes with its own set of risks, creating security issues if they are not properly handled.

In this report we will be exploring some of the trends in mobile technology adoption, the challenges they bring and some of the ways of dealing with them. Along the way we'll refer to the results of our recent research study on Mobile Security which gathered feedback from over 250 IT and business professionals (see Appendix A for more details).

To begin our discussion, let's have a look at some of the key adoption trends.

Adoption and ownership of mobile devices

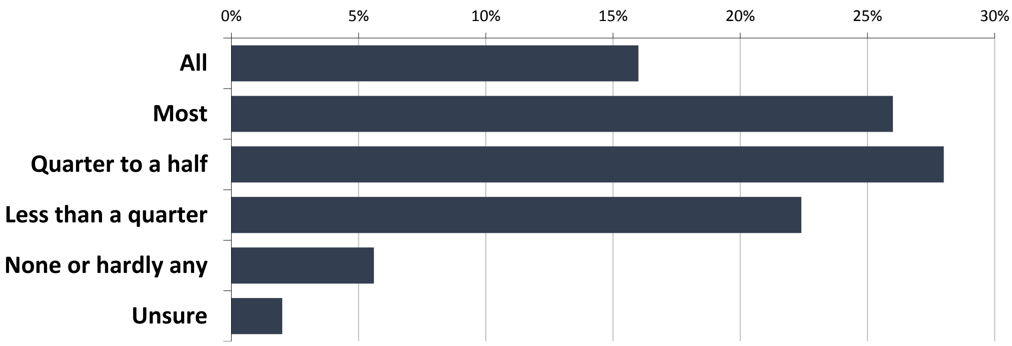
4 out of 10 say 'most' or 'all' of the workforce in their company uses mobile equipment.

During our research we defined the term mobile technology to mean smartphones and tablets. We specifically excluded full blown Windows, Mac and Linux devices. With the lines between device classes starting to blur, and with the increasing number of hybrids available in the marketplace, this helped to keep the discussion focused.

At the highest level, the trend towards mobile adoption in business is clear, with the majority of respondents reporting over a quarter of their workforce using smartphones or tablets. As part of this 4 out of 10 say 'most' or 'all' of the workforce in their company uses mobile equipment to access company applications, services, documents or data (Figure 1).

Figure 1

How many of your employees use mobile devices to access company applications, services, documents or data?



More and more employees are beginning to use their own devices for work.

When looking at the survey data we need to bear in mind the possibility of skew. In the case of an online study like this one, those with more knowledge of or interest in the area are increasingly likely to participate, therefore the above chart may over represent the level of mobile-related activity. Nevertheless, it is clear that mobile technology has found its place within business.

Developments in the consumer space are also relevant here with more and more employees beginning to use their own devices for business purposes. The popular

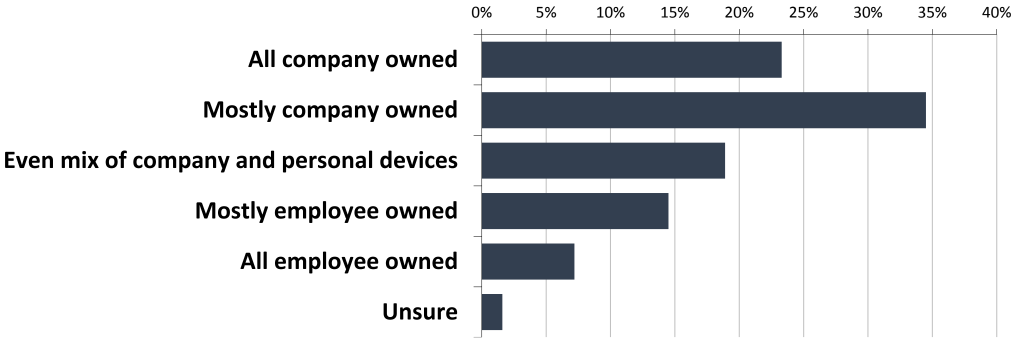
Relatively few organisations rely solely on BYOD.

term for this is 'Bring Your Own Device' or 'BYOD' and we can see evidence of this in the survey results.

Although the majority of devices used for business are company owned, we see significant levels of personal equipment being used to access company resources. However, relatively few organisations rely solely on BYOD for their mobile access at the moment (Figure 2).

Figure 2

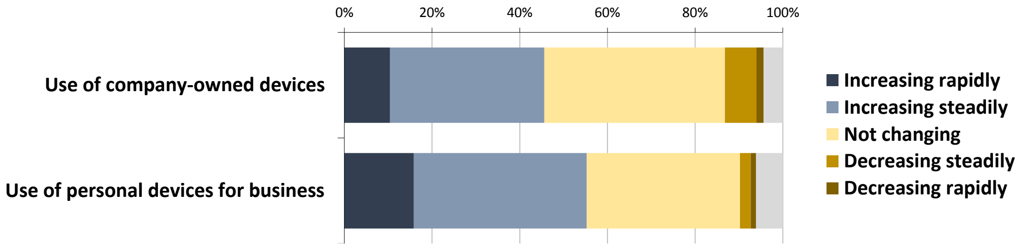
How many of the mobile devices used to access company resources are actually owned by the company versus the employee?



Having said this, while the use of mobile devices in general is on the rise, BYOD is increasing more quickly than company owned equipment (Figure 3).

Figure 3

How are usage levels in relation to mobile devices changing?



We need to be aware here, however, that the difference between the growth rates isn't huge and company-owned devices are growing from a larger base. This suggests that while the use of personal devices is clearly important we are unlikely to end up living in a BYOD only world. BYOD cannot fulfil the needs of all businesses in all circumstances, and for those that can make use of the benefits, it is still only likely to be used in relation to certain types of user.

While device ownership and adoption are important, they are only part of the story.

While device ownership and adoption are important, they are only part of the story. In order to understand the remainder we need to look at what devices are being used for.

Mix of business and personal activity

Company email is accessed almost as much from personal devices nowadays as from company owned ones.

We asked study participants to report back on the types of activity that were being seen on mobile devices to a significant level, and in particular whether applications, services or data were being accessed via business or personal equipment.

Not surprisingly the results indicate that company email is accessed almost as much from personal devices nowadays as from company owned ones. What's easy to overlook, however, is that the counterpart to this observation is also true, i.e. personal email is almost as likely to be accessed on company devices as personally owned equipment.

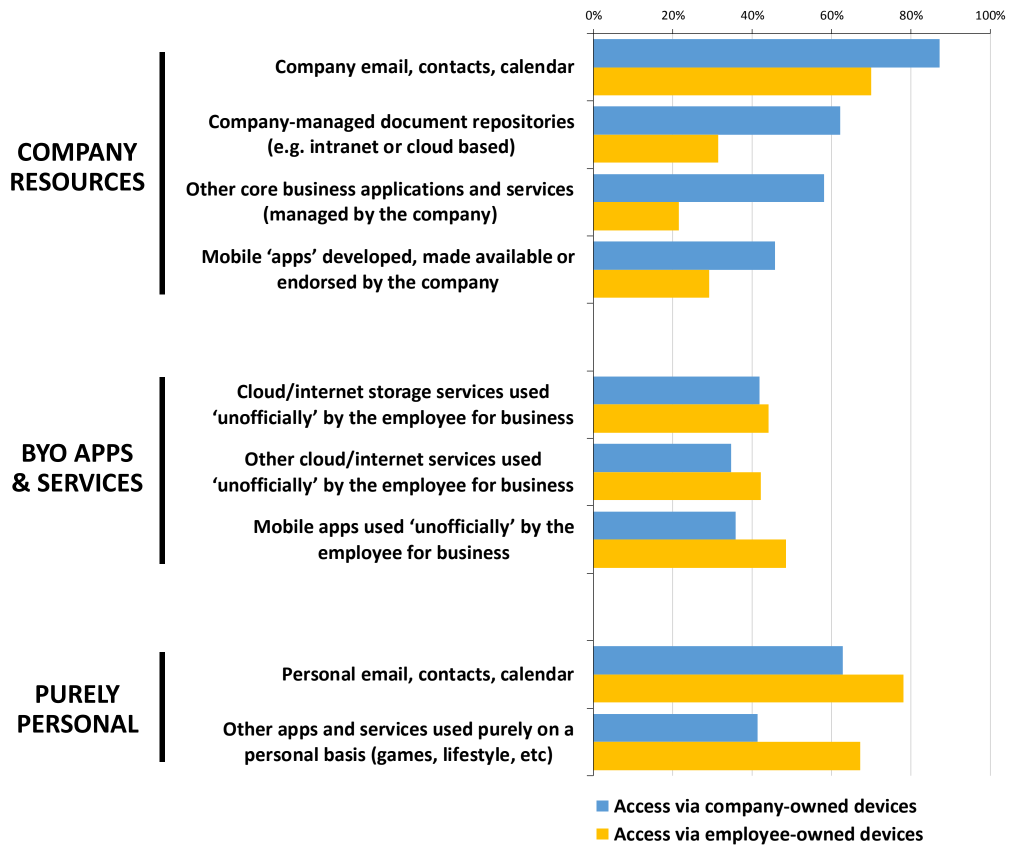
A broad range of both business and personal activity is often being mixed on the same device.

This clearly reflects the fact that all smart mobile devices typically come with a very versatile email client, and most email systems (both corporate and consumer) are now very mobile friendly. Provided a connection is enabled in the backend, hooking up any device to any email system is usually very straightforward for users.

Beyond email, the most striking observation regarding access patterns is that, regardless of ownership, a broad range of both business and personal activity is often being mixed on the same device (Figure 4).

Figure 4

Turning to how mobile devices are used, are you seeing the following being accessed significantly on company vs personal devices?



Users typically don't consider security, compliance and data protection.

The picture we see here obviously raises some potential concerns. Business solutions which may be handling sensitive or controlled data are frequently running in the same environment as user-selected software and services. Furthermore, some of that user-selected capability (the BYO apps and services) is then being used directly to process and store business information. Given that users typically don't consider security, compliance and data protection when choosing what they install or sign up to, the result is at best a questionable situation from a risk management perspective. And this doesn't just apply to BYOD – you are just as likely to see a mix of business and personal activity on company-owned kit.

So let's take a closer look at the specifics of what can go wrong.

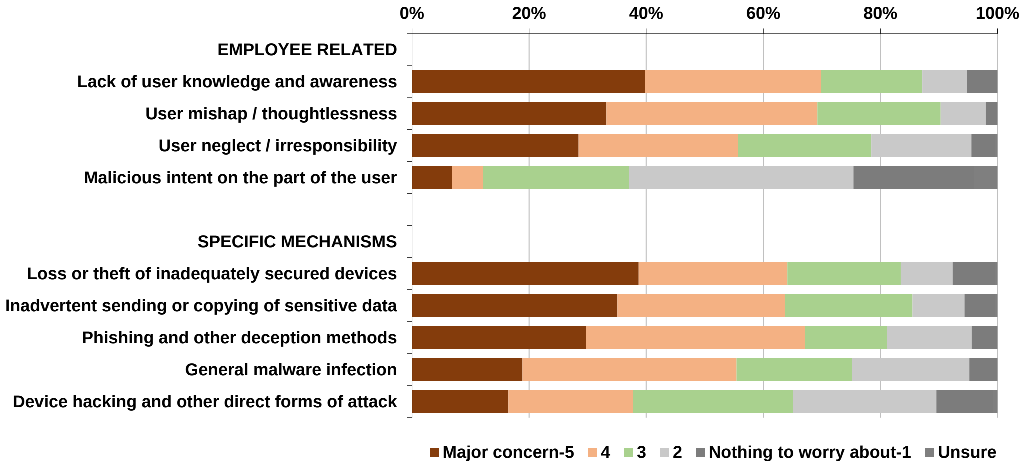
Most security risks are to do with ignorance, thoughtlessness or neglect.

Sources of exposure and risk

It is often said that the weakest link in the IT security chain is the end user. This is something that has been confirmed by our research. However, when it comes to employee related considerations, most security risks called out are to do with ignorance, thoughtlessness or neglect rather than malicious intent (Figure 5).

Figure 5

When it comes to the consideration of security risk in the mobile computing context, how much do the following represent a source of exposure or uncertainty?



A large part of mobile security involves protecting the business from the actions of its own employees.

When we turn to the lower half of the chart we can see that when it comes to specific mechanisms, direct attacks by third parties are at the bottom of the list, and once again the majority of exposure is related to the user. Phishing and other deception methods such as social engineering rely on the user being less than fully vigilant and malware infection is often down to thoughtlessness and/or neglect. This allows us to come to the conclusion that a large part of mobile security involves protecting the business from the actions of its own employees.

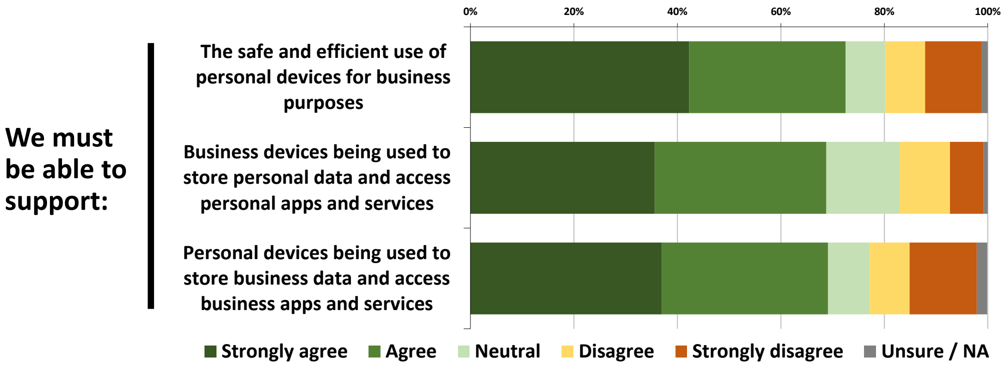
Given this, and some of the adoption and usage patterns we have been discussing, we can start to define the requirements for effective mobile security management going forward.

Defining the overall requirement

At the highest level, we see a significant number of study participants agreeing on a number of requirements. These include support for BYOD, and the ability to deal with both personal and business activity taking place on the same device, regardless of ownership (Figure 6).

Figure 6

Thinking of security requirements at the highest level, how much would you agree or disagree with the following statements in relation to mobile device use in your organisation over the coming three years?



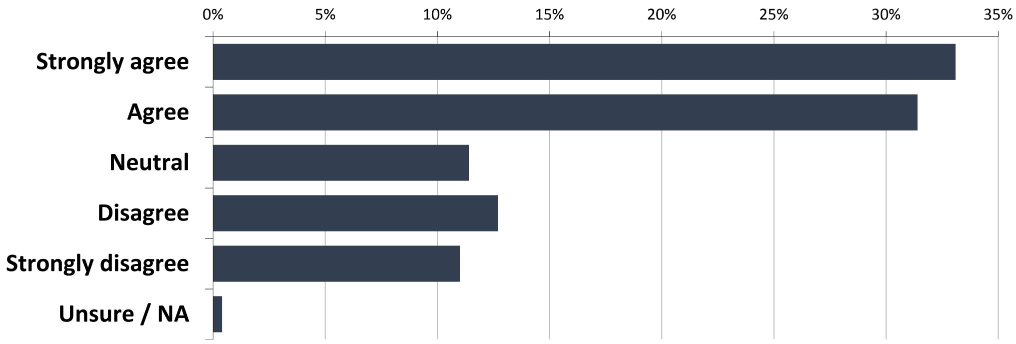
It shouldn't matter who owns the device.

Another fundamental that comes through is the importance of an inclusive approach. The last thing you want is to end up with dual mechanisms and dual standards by treating business and personal devices separately.

Respondents generally agree that with the right approach to security management, it shouldn't matter who owns the device (Figure 7).

Figure 7

AGREE/DISAGREE:
With the right approach to security and management, it should not matter whether personal or business devices are used



However, this is easier said than done and in the next section we will take a look at how the right mix of technologies and tactics can help to solve the problem.

Technologies and tactics

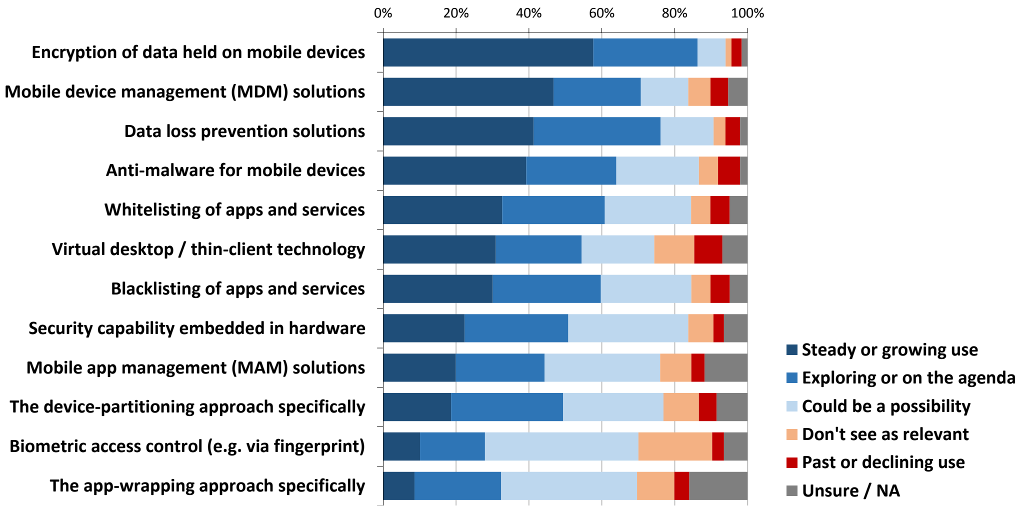
There are no magic bullets in terms of the solutions.

A point that comes across strongly from the research is that there are no magic bullets in terms of the solutions in this space and like all areas of risk management, implementing mobile security is about stacking the odds in your favour.

When it comes to doing this in practice, the relevance or potential relevance, of a whole range of technologies and approaches come into play (Figure 8).

Figure 8

Bearing in mind everything we have been discussing, how would you sum up your use or potential use of the following in relation to mobile devices?



It is beyond the scope of this report to go into details on specific technologies and techniques, and in many ways it could be argued that organisations are faced with too many options. Trying to work your way through what individual solutions do and where they fit into your business can be a challenge.

Trying to work your way through what individual solutions do and where they fit in your business can be a challenge.

Fortunately, we have seen the emergence of a concept known as 'Enterprise Mobility Management' or 'EMM'. The idea here is to provide a range of capabilities, including many of the techniques listed above, but delivered in a pre-integrated manner. This minimises the risk of things falling through the cracks between solutions.

However one of the most important aspects of EMM, is that it strives to provide a single point of management. This means you can define, apply and monitor all or most of your mobile security policies from a single place.

EMM solutions are still generally immature and/or incomplete.

The reality is that at the time of writing, EMM solutions and the best practices associated with their use are still generally immature and/or incomplete, so an element of mixing and matching will remain necessary for some time to come.

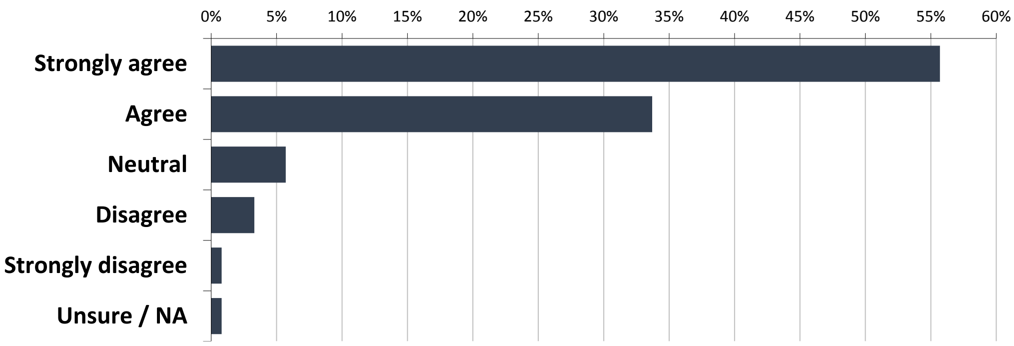
In the meantime though, there are some important things that can be done to deal with some of the user-related issues head on.

Directly addressing the human element

Whatever you put in place in terms of safeguards, no technology based approach can ever be fool proof. Alongside this, there is always a limit to how far you can go before users regard security measures to be too onerous and do whatever they can to work around them (Figure 9).

Figure 9

AGREE/DISAGREE: Users will always attempt to get around onerous security measures that they perceive to limit usability and utility



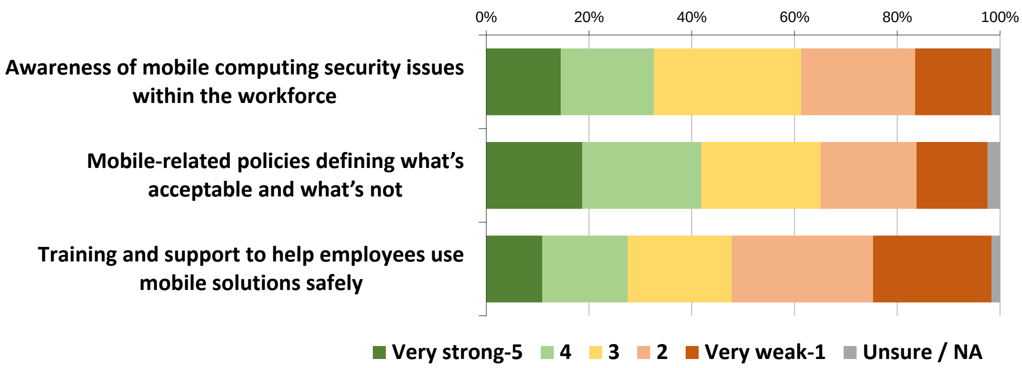
Ensure that users are made as aware as possible of the business risks.

With this in mind, it makes sense to ensure that users are made as aware as possible of the business risks and potential consequences, and provided with appropriate guidance. They are then more likely to behave sensibly and responsibly, and less likely to do risky things.

In practical terms, this boils down to defining policies, and educating users accordingly. Unfortunately, however, the research suggests that this is an area that is too often overlooked or inadequately dealt with (Figure 10).

Figure 10

Beyond technology, how strong would you regard the following to be in your organisation in relation to mobile security?



The IT team itself may not have the authority needed.

The question is, who should be responsible for the behaviour of employees?

While technology expertise is important for defining safe ways of working, the IT team itself may not have the authority needed to enforce security policies, even when the business risk is clear. Non-technical managers, meanwhile, often don't have the necessary level of awareness of mobile security issues themselves to

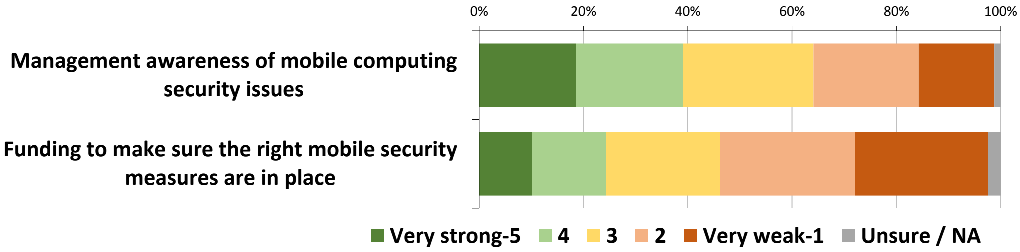
A lack of air cover often exists.

appreciate what needs to be done. Furthermore, even though securing the organisation's assets and activities is primarily a business issue, it's not one that's always front of mind.

As a result, a lack of air cover often exists when it comes to instilling the right kind of behaviour within the workforce, along with a shortage of funding to make sure that the right security measures in general are put into place (Figure 11).

Figure 11

Beyond technology, how strong would you regard the following to be in your organisation in relation to mobile security?



This highlights the need for those in IT to drive both awareness and responsible behaviour within management teams and the workforce as a whole.

However pleas to take mobile security more seriously often fall on deaf ears. So what can be done?

If this is a situation you are grappling with in your organisation, you may find some of the analysis from the research we are about to show particularly useful.

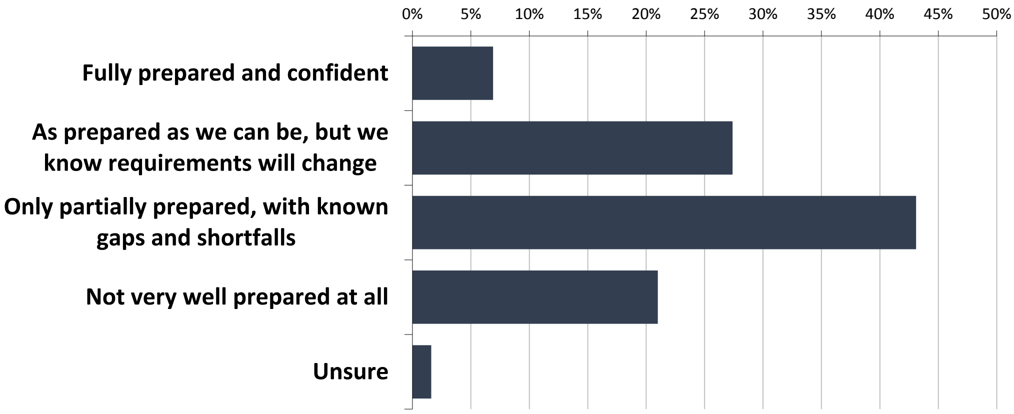
Only a small minority of organisations feel fully prepared and confident at the moment.

Pulling it all together

To begin with, it is important for all concerned, including both IT leaders and business stakeholders, to have an open and honest discussion about the organisation's true level of readiness to handle current and future mobile security challenges. The chances are that the need for action and/or investment will then become apparent, as only a small minority feel fully prepared and confident at the moment (Figure 12).

Figure 12

How well prepared is your organisation to handle the mobile security challenges it is likely to face over the coming three years?



Addressing capability gaps can be achieved in a couple ways.

Broadly speaking, addressing capability gaps can be achieved in a couple of ways:

- Firstly, you could invest in the kinds of technologies we have been discussing to create an environment as safe and secure as possible from an IT perspective.
- Secondly, you could train those in the workforce on at least the basics of what it takes to work in a safe and secure manner.

But which of these should you prioritise?

Some have focused their efforts differently to others.

Based on responses to various relevant questions gathered in the research, it is clear that historically, some have focused their efforts differently to others. Some have invested significantly in technology solutions, some have prioritised training their workforce, while others have invested in both. There are then, of course, those that haven't spent much time or money on either.

Segmenting respondents according to the steps they have or haven't taken yields four approximately equal sized groups (Figure 13).

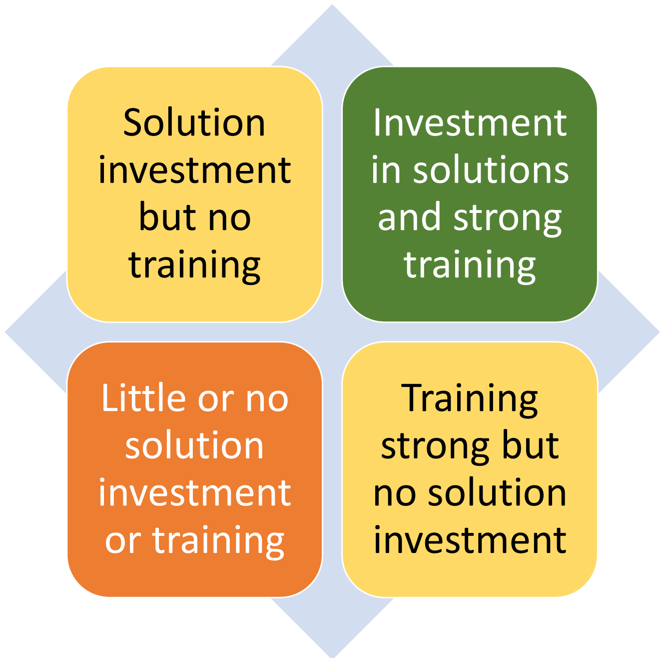


Figure 13

Security training/investment quadrant

If you're going to focus your efforts in one area, you're better off making it staff training.

When we look at the level of preparedness exhibited by each group, those paying attention to both areas not surprisingly stand out as being in a much better position on average. However, the data suggests that if you're going to focus your efforts in one area, you're better off making it staff training (Figure 14).

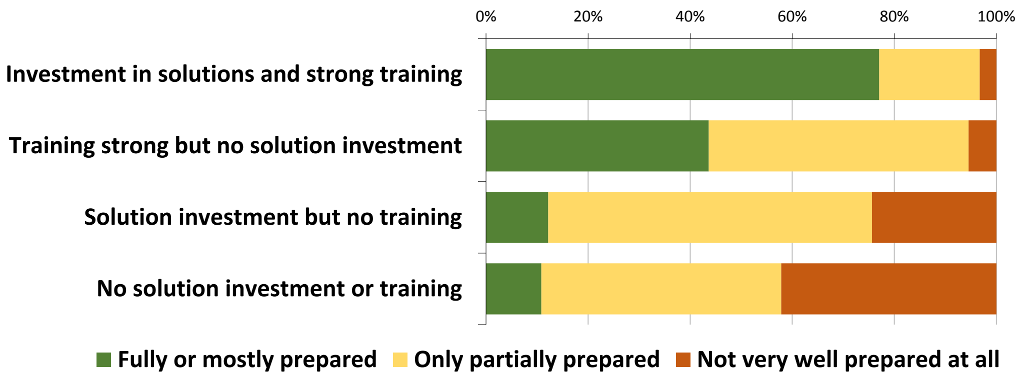


Figure 14

How well prepared is your organisation to handle the mobile security challenges it is likely to face over the coming three years?

The user really is the weakest link.

If the research we have presented here is anything to go by, then the user really is the weakest link in mobile security. While this won't come as a surprise to most experienced IT professionals, data like this can be useful to focus minds when discussing the nature of risks with business people, and the kinds of measures that need to be put into place to manage them effectively.

Final thoughts

Mobile technology is already playing a significant role in business, and it's only going to become more important over time.

What really matters as you define your requirements is understanding how devices are being used.

However, the noise we hear in the market around BYOD is largely a distraction when we take a longer-term view. Sure, there are tactical issues to do with the use of personal devices for business that need to be dealt with at the moment, but the long term aim should be to create an environment in which the ownership of equipment is irrelevant, at least from a management and security perspective.

What really matters as you define your requirements is understanding how devices are being used. In line with this, the consensus from the research is that your mobile security measures should be able to cope with business and personal activity being mixed on the same device regardless of who owns it.

IT vendors are working towards helping customers achieve this goal. They are looking to provide more integrated offerings that avoid the overhead that often results from stitching together a series of point solutions. While it is unlikely that one product or service will ever meet all of your needs, it does make sense to minimise the number of solutions you use.

The research screams out loud and clear that technology-based measures can only get you so far.

Meanwhile, the research screams out loud and clear that technology-based measures can only get you so far. In fact feedback from study participants suggests that you can achieve more by simply raising the level of awareness and competence within the workforce through appropriate policy definition and employee training.

With this in mind, it is not surprising that many organisations are looking to the vendor and service provider community for help beyond delivery of their core offerings. A real need exists for educational material, policy and process templates, self-assessment tools, and other forms of guidance (Figure 15).

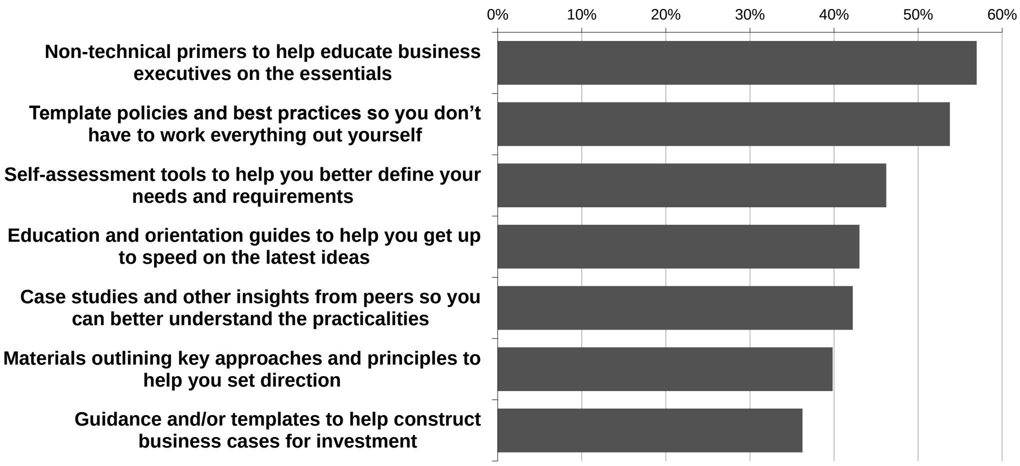


Figure 15

Vendors and service providers are always quick to pitch their offerings, but beyond the standard marketing, would any of the following be particularly useful from them in relation to mobile security?

The mix of help that's relevant to you will depend on the nature of your environment and the progress you have already made on your mobile security journey.

Wherever you are at the moment, however, we hope the insights provided in this report will help you to assess your current position, set or check your direction, and prioritise what's important to achieve both short and long term success.

Further reading

The following research reports and papers are available for free download from the Freeform Dynamics website (www.freeformdynamics.com).

1. **The Politics and Practicalities of End User Computing**
   Community Research Report

2. **End User Computing**
   A Management Perspective

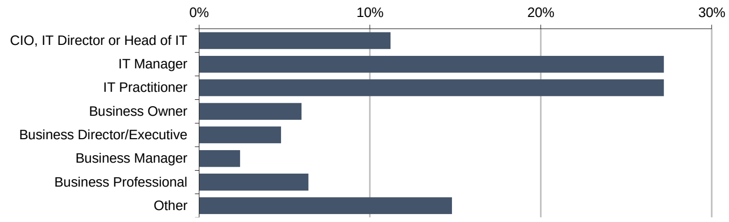
3. **Freedom Without Anarchy**
   Empowering your users while keeping control

Appendix A: Research sample

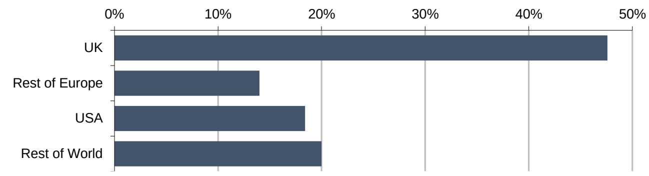
The study upon which this report is based was designed, executed and interpreted on an independent and objective basis by Freeform Dynamics Ltd. Data was gathered from 251 respondents via an online questionnaire hosted on a popular IT news and information website.

The sample distribution was as follows:

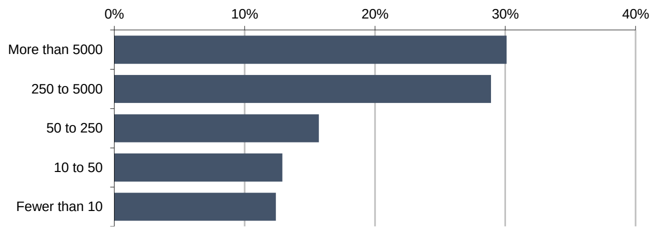
Sample by job function



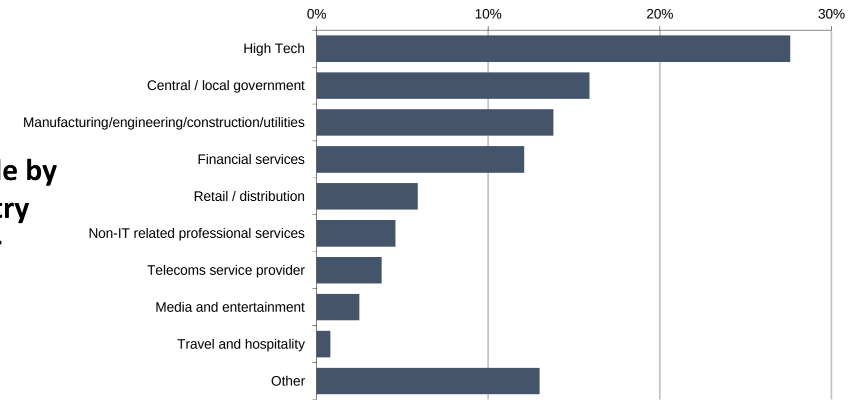
Sample by geography



Sample by number of employees



Sample by industry sector



Limitations of methodology

As with all online research, self-selection of respondents into the survey means there is a possibility of the data being skewed towards those who are more advanced with the topic or have more of an interest in it. Please bear this in mind when looking at specific percentages shown on the charts.

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.