Mobile technology and security

Reducing the risks of mobile deployment

By Josie Sephton, June 2010

In a nutshell:

The issue of security when thinking about flexible working practices such as mobile working and home working is of paramount importance to companies. However, while some companies see security as an insurmountable challenge, others have been able to address it comfortably and successfully. This ability to deal with security challenges is not simply down to chance, but rather is a reflection of how well a company is managed, the extent to which it operates in a high-capability IT environment and, of course, its approach to mobile technology.

Key points:

- In spite of an ongoing shift in the way that people work, many companies struggle to deal with the security challenges that arise as part of a shift to flexible working.
- Companies with a much broader deployment of mobile technology, which are much better managed and more IT-capable, will also have less security challenges: all of these areas are inter-related.
- Issues such as developing proper procedures for identity and access management, keeping systems up-to-date, and protecting them against external threats are critical elements which need to be included.
- Companies that aren't there yet with security issues can't ignore them forever, but may need to think about more rigour with IT and management practices. However they can move forward with confidence in the knowledge that other organisations have benefited from putting the right management and technical measures in place.

The research upon which this report is based was designed and interpreted on an independent basis by Freeform Dynamics. During the study, which was sponsored by Symantec, feedback was gathered from 700 small businesses across EMEA via in-depth telephone interviews.

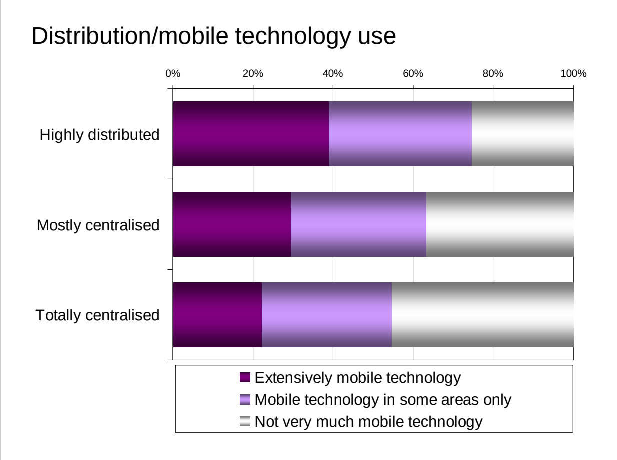
Research sponsored by

symantec.

Mobile security has become a much bigger issue

Mobile technology within the enterprise has long since moved from being about mobile phones for the senior management. As working practices have changed, mobility touches many aspect of working life, from the road warrior connecting back into the company resources with his laptop while on the move, to home based workers, and field forces that update schedules and customer information via their PDAs direct from customer sites. Even device sourcing is changing, with staff increasingly bringing their own devices into the organisation. This increase in endpoints that touch internal systems is likely to increase over time, and brings with it an increasing need to deal with security issues throughout the business.

While mobile technology is increasingly pervasive in the workplace, variations in use exist based on the extent to which a company is distributed geographically. As might be expected, there is a direct correlation between distribution and mobile technology use, with highly distributed companies more likely to use mobile technology more extensively than companies that are mostly or fully centralised (Figure 1).



In line with what we would expect, there is a direct correlation between how distributed a company is and how much mobile technology it uses

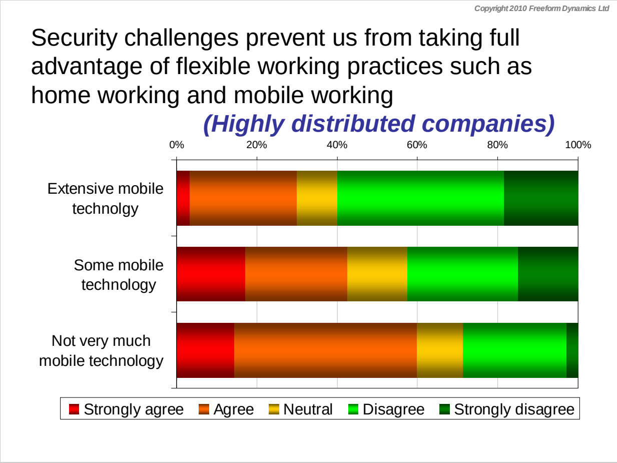
Figure 1

This in itself is not remarkable. After all, we would naturally expect distributed companies to need to move staff, goods and data across sites, with mobile technology providing a support function as part of this process. But if we look more closely at these highly distributed companies, is there anything we can learn about their use of mobile technology and correspondingly, how they organise and run their businesses?

To answer this, let us consider this subset of companies from our research, and further subdivide this into companies that have deployed/use mobile technology extensively, have some mobile technology in place, and make very little use of mobile technology. The bottom line, as we shall see, is that more mobile companies are better able to deal with security challenges.

The relationship between mobility and security

When we ask about the extent to which security challenges impact the ability of a company to adopt flexible working practices – a topic that is of increasing importance to many businesses - some very interesting variations arise (Figure 2).



More mobile companies handle security better to enable flexible working, while those with limited mobile see security as a major issue

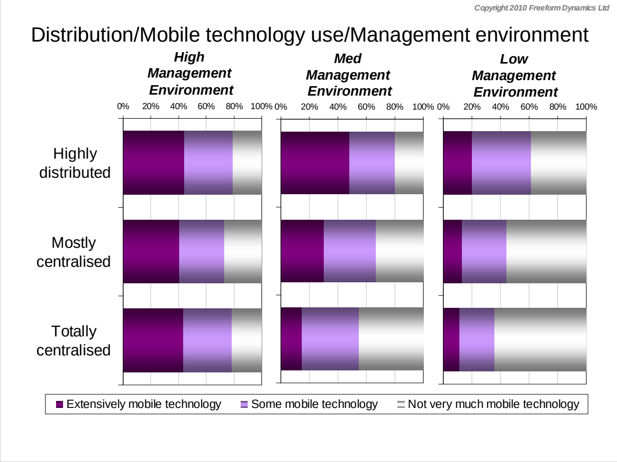
Figure 2

So, companies that use mobile technology more extensively, on the whole, have dealt effectively with the security challenges around flexible working. This is self-fulfilling, to a degree: if they couldn't address these challenges, there would be little point in an extensive mobile deployment.

But what of the other two groups of companies that have considerably less mobile technology in place? Around half are struggling with the issue of being able to adopt more flexible working, which in a world that increasingly demands mobility, is less than ideal. So, what are the characteristics of these companies that have 'sussed' the security challenge issue, and are there some pointers that other organisations can take away?

The role of the management environment

When we look across the different company splits we have defined, and examine the type of management environment[1] they operate in, some possible answers start to emerge. (Figure 3).



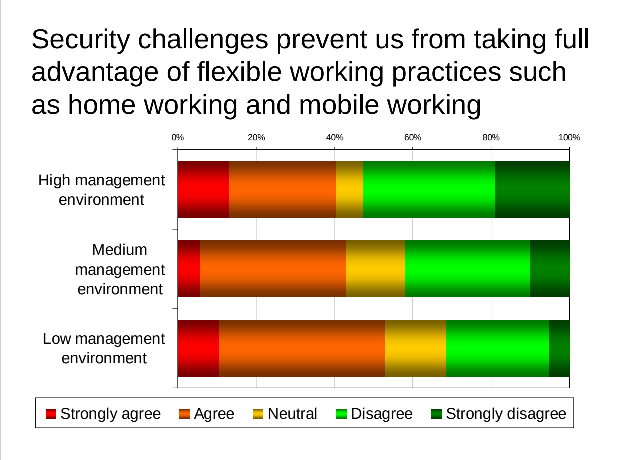
There is a direct correlation between the extent to which a company uses mobile and the extent of its management capability

Figure 3

[1] Management environment takes into account a range of management-related issues such as management awareness around information access and security, and information management and protection, as well as things such as general workforce data security and protection awareness, consideration of business risks, existence of and compliance with policies in relation to electronic security and access, and data management and protection, defined business-continuity procedures, staff training on information security and protection, and consideration around security and protection during recruitment. Companies that demonstrate a high capability across these areas have been classified as displaying high management environment, while conversely, companies with medium and low capability have been classified as medium and low management environments, respectively.

Companies that operate in a higher-capability management environment will tend to have deployed mobile technology more extensively. It is interesting to note that this correlation between management capability and mobile deployment plays out equally across highly distributed and more centralised companies alike. But for companies in lower-capability management environments, more highly distributed companies still lead with respect to mobile use.

So this tells us that companies that are better at managing are better at getting mobile up and running in their business. Moreover, if we refer back to our initial analysis around security challenges, and look at it from the perspective of management capability, the impact of this on a company's ability to deal with security challenges is clear. (Figure 4)

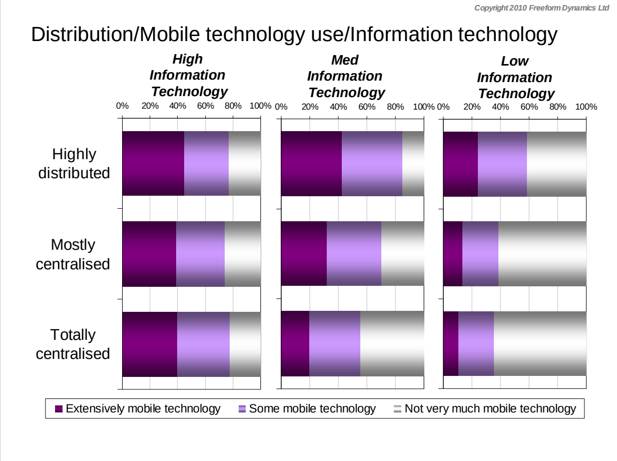

Security challenges prevent us from taking full advantage of flexible working practices such as home working and mobile working

Companies with higher management capability see themselves as better able to deal with security challenges around flexible working

Figure 4

Higher mobile-use companies are also more IT capable

As with the management environment, it is those companies which operate in a higher-capability IT environment[2] that will tend to have deployed mobile more extensively, as shown in Figure 5.


Copyright 2010 Freeform Dynamics Ltd
Distribution/Mobile technology use/Information technology

Companies that have deployed mobile more extensively are more likely to operator in a higher capability IT environment

Figure 5

[2] Information technology capability takes into account a number of different measures, including degree of service provisioning, identity and access management facilities, degree of protection against external security threats, capability around IT arrangements for routine backups of systems etc., management of information retention, deletion and archival, ability to monitor the health and security of IT systems, capability around keeping IT systems up to date with latest fixes and security patches. Companies that demonstrate a high capability across these areas have been classified as being a high IT environment, while conversely, companies with medium and low capability have been classified as medium and low IT environments, respectively.

Already a clear pattern is emerging between ability to overcome security challenges associated with flexible working, the extent of mobile use in a company and, more importantly, its management and IT capability. In a nutshell, the likelihood of security challenges occurring lessens for companies that possess certain characteristics, notably:

- They are more distributed
- They have better management in place
- They are more advanced in terms of their approach to IT
- They deploy mobile technology more extensively

These characteristics are interrelated, to some degree. So, for example, a more distributed company will use mobile more, as will a company that has a progressive approach to, say, IT or management. A more distributed company may need to be more IT-advanced simply because it is more distributed, and a sound approach to IT to deal with getting services and goods across and around different sites is critical for survival.

This is all interesting stuff, but what can we glean from it – in particular, what are the lessons other types of organisations can learn?

Security challenges exist for all, but can be overcome

Let’s be clear: security challenges exist, in a not-insignificant way, in all the groups of companies we have looked at, whether they are highly distributed or highly centralised, whether they use mobile technology a lot or not, whether they operate a high capability management environment or a low one, or whether they have a high capability IT environment or not.

However, whatever the relationship, the fact that this sub-group of companies that ‘do things better’ exists is important because it demonstrates that any challenges around security, perceived or otherwise, are surmountable.

To see what can be done when it comes to dealing with these challenges, we can drill into the specifics of what make up IT and management capability. From a management perspective, the key is having senior management in place, who are tuned into issues around security, and have effective strategies for dealing with them, such as:

- Ensuring policies are up to date in relation to electronic security and access
- Take more account of compliance with data management and protection policy
- Raise the importance of issues around information security during recruitment
- Place more emphasis on training staff on security issues.

More competent companies in these areas are also much more IT-savvy, paying attention to issues such as:

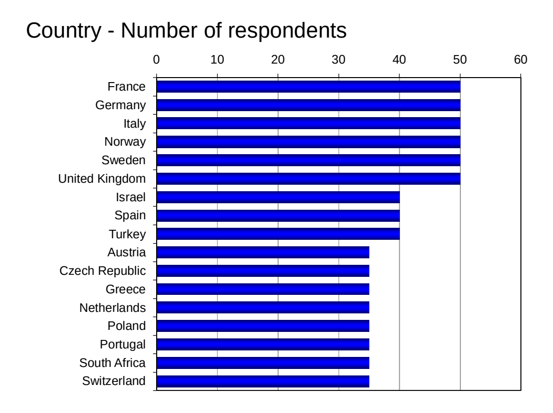
- Putting in place proper procedures for identity and access management
- Ensure that systems are protected against external security threats
- Have a thorough approach with respect to information management
- Keeping IT systems up to date.

For organisations looking at increasing their level of distribution or mobility, the advice is clear: that sooner or later, if you want to join organisations that have succeeded in these areas, you will need to address the security challenges they have overcome. It is not by accident that such organisations have improved both their management and IT capabilities, so for those companies that fall into the bracket of ‘not there yet’ with security challenges, the issues cannot be ignored for very long, as changing business practices simply won’t permit it. Resolving security challenges in the mobile environment isn’t an insolvable or insurmountable problem, but may require more rigour around approaches to IT and management practices in general, and this may be no bad thing for the organisation as a whole.

Appendix A

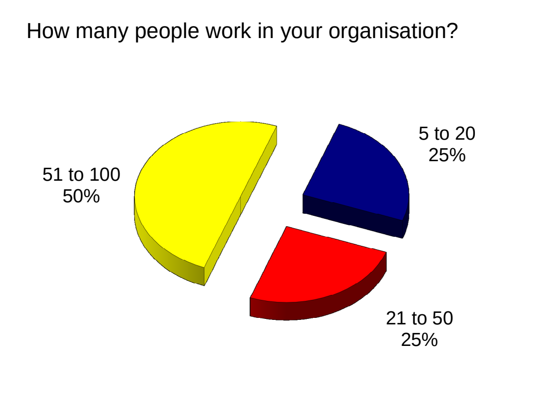
Research Sample

The study from which these inside tracks have been produced was designed and executed by Freeform Dynamics in Q1 2010 via a telephone survey of 700 small businesses in Europe.



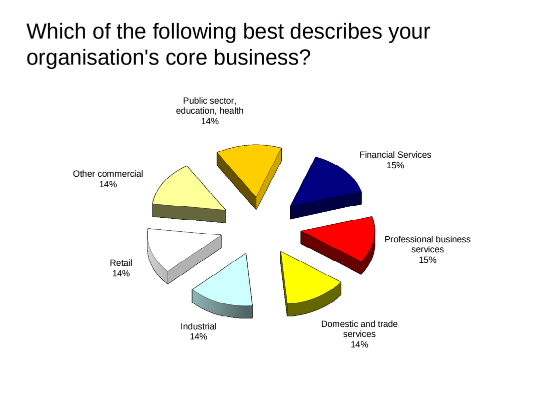
The research sample explored the experiences and capabilities of 700 small businesses across 17 countries in EMEA

Figure A1



The sample was targeted at the 'small' end of the SMB sector

Figure A2



A balanced sample was taken from a range of industries

Figure A3

About Freeform Dynamics

Freeform Dynamics is a research and analysis firm. We track and report on the business impact of developments in the IT and communications sectors.

As part of this, we use an innovative research methodology to gather feedback directly from those involved in IT strategy, planning, procurement and implementation. Our output is therefore grounded in real-world practicality for use by mainstream business and IT professionals.

For further information or to subscribe to the Freeform Dynamics free research service, please visit www.freeformdynamics.com or contact us via info@freeformdynamics.com.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at www.symantec.com.

Terms of Use

This document is provided for your general information and use only. Neither Freeform Dynamics Ltd nor any third parties provide any warranty or guarantee as to the suitability of the information provided within it for any particular purpose.