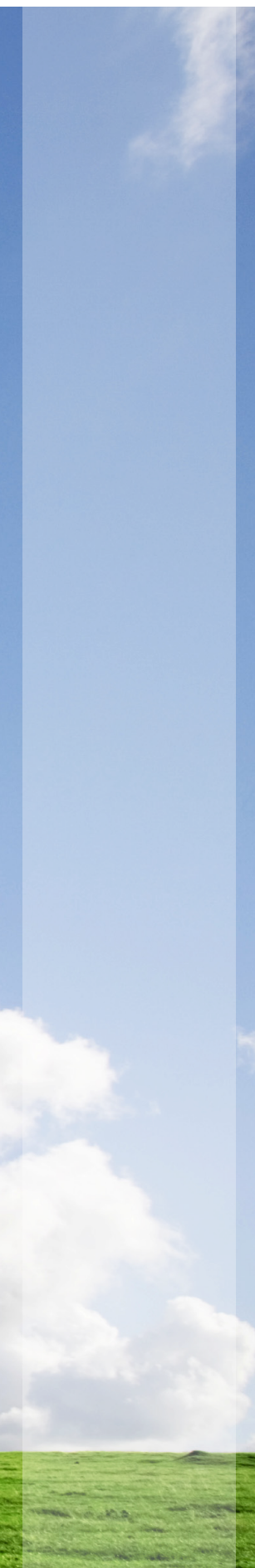


My dog ate my iPad – security risks of the consumerised workplace

Commissioned by SecureData

Conducted by Vanson Bourne

Publication date: November 2011



My dog ate my iPad – security risks of the consumerised workplace

Part 1. Executive summary

The 'consumerisation of IT' is not a new term. Security managers have been warned about the preparation needed to manage the increased security risks from the growing number of consumer technologies entering the workplace since the phrase was first popularised a decade ago.

Since then, we have seen mobile devices swarm the market, in the form of incredibly sophisticated smartphones and tablet devices that have captured the imagination of the nation. Flexible working has become a reality for many and a growing number of companies are allowing employees to bring their personal devices to use in the workplace in BYOD (Bring Your Own Device) schemes. But have the security risks been managed and met to the same degree, or is there still further work to be done to ensure the safety of workplace data?

SecureData has conducted a study to review the situation; we believe the following are the most salient findings:

- Flexible working is a huge trend across a number of industries, with it being most popular in the financial services sector.
- A large proportion of employees use their own personal mobile devices such as smartphones or tablets to work remotely or whilst on the move.
- A large proportion of businesses don't have a policy in place for employees to work remotely via their own personal mobile devices. Moreover, a quarter of businesses will not be implementing a policy as they don't see it as a priority.
- The biggest consideration when implementing such a policy is the security risk it presents.
- A surprisingly high number of people are allowing children or other household members to use their work device. Those that don't, see security as the biggest reason why not to.

In summary, employees are working from home in large numbers. They are using their personal mobile devices to work remotely or whilst on the move, but there's still a large proportion of companies that don't have a policy in place to deal with this securely. Despite security being the most important consideration identified by the study, some businesses are even choosing not to put developing a proper policy to deal with this on their agenda.

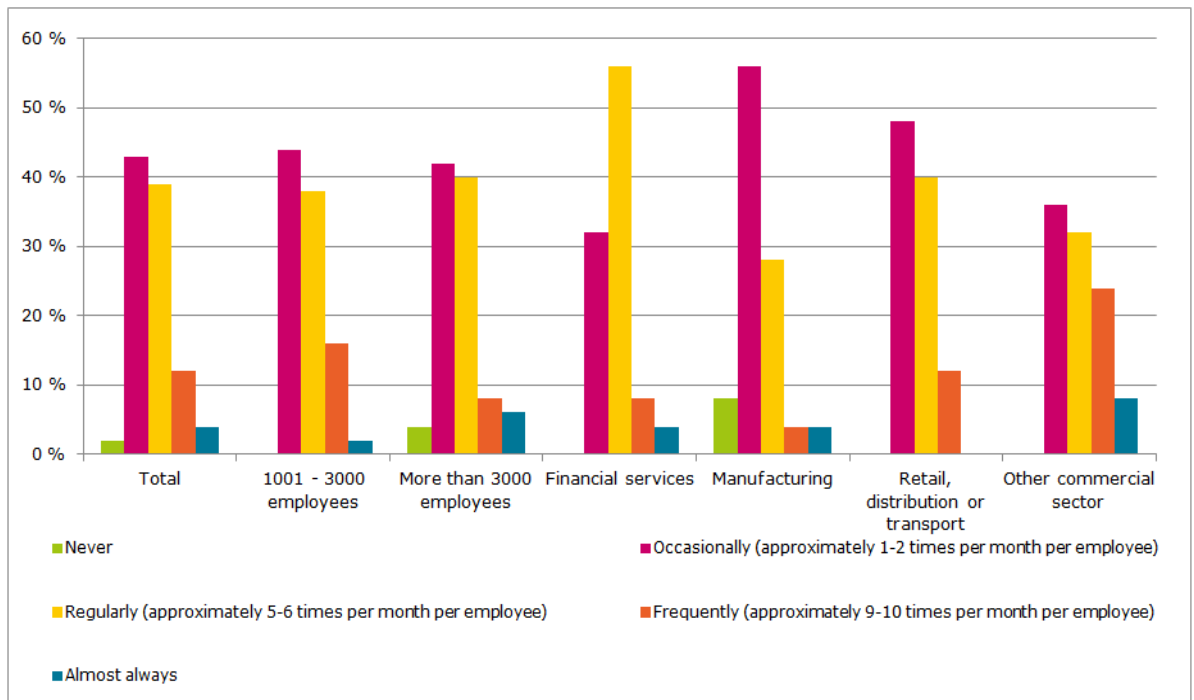
The study findings present a huge opportunity for businesses. Employees already have the latest mobile device, which many are using to access their work information anyway. Businesses need to work with employees to resolve this. Smartphones and tablet devices are not going away and neither is the risk of corporate data held on these devices. By not providing the appropriate policy and framework for people to use personal devices, companies are creating a bigger risk as people will find their own ways of transferring work to devices, methods which are often very risky. There will only be further integration between the technology in our personal and professional lives. Schemes such as BYOD are ideal; cost savings with company-owned equipment can be made and they satisfy employee's desire for flexibility. It enables rich mobile working but can also ensure compliance and the safety of business data by having a managed policy in place.



Etienne Greef, Professional Services Director, SecureData

Part 2. Analysis of key findings

1. Does your organisation allow employees to work from home?



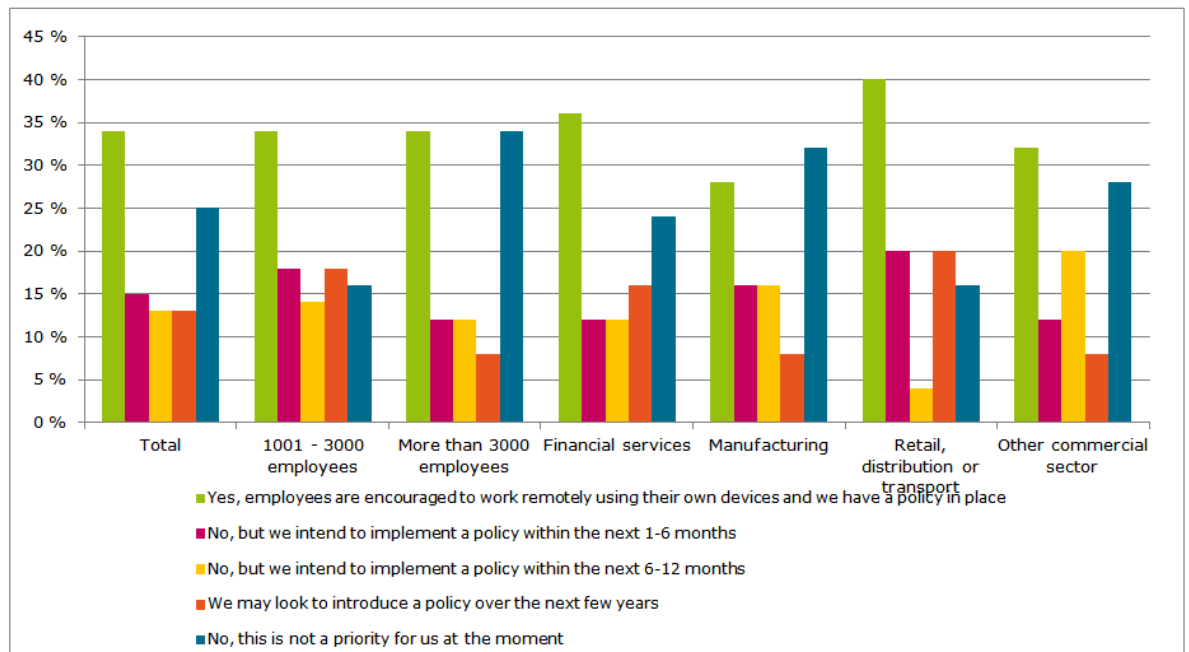
Key stats:

- Only 2 percent of all respondents are not allowed to work from home, which leaves a huge majority of 98 percent being allowed to work from home (more than once a month).
- In the financial services sector, 56 percent of employees surveyed regularly work from home (approximately five to six times a month / over once a week) and all (100 percent) are allowed to work from home at least once a month.

Analysis:

- These findings reveal a very large trend in flexible working practices. With 98 percent of employees across all industry sectors surveyed allowed to work from home, this highlights that businesses are willing to let employees work in the environment that best suits their needs. But working from home, or even whilst on the move, can bring with it a number of issues that businesses must address:
 - Rich mobile working: Employees need to be able to connect to the network in a secure manner and access the information they need to make faster and better decisions on the move
 - Company information must be safe and secure at all times
 - Compliance to regulatory standards is vital to the successful modern workplace
 - Ultimately, employees should be able to work from home like they do in the office
- This is even more pertinent in the financial services sector where regular home working takes place and there is a greater volume of sensitive information.

2. Does your organisation currently have a policy in place for employees to work remotely via their own personal mobile devices such as smartphones and iPads?



Key stats:

- The survey revealed that 25 percent of organisations do not have a policy in place for employees to work remotely via their own personal mobile devices (such as a smartphone or a tablet device) and don't think it is a priority at the moment.
- A further 41 percent don't currently have a policy in place for employees to work remotely via their own personal devices, but have said that it is on their agenda to implement.

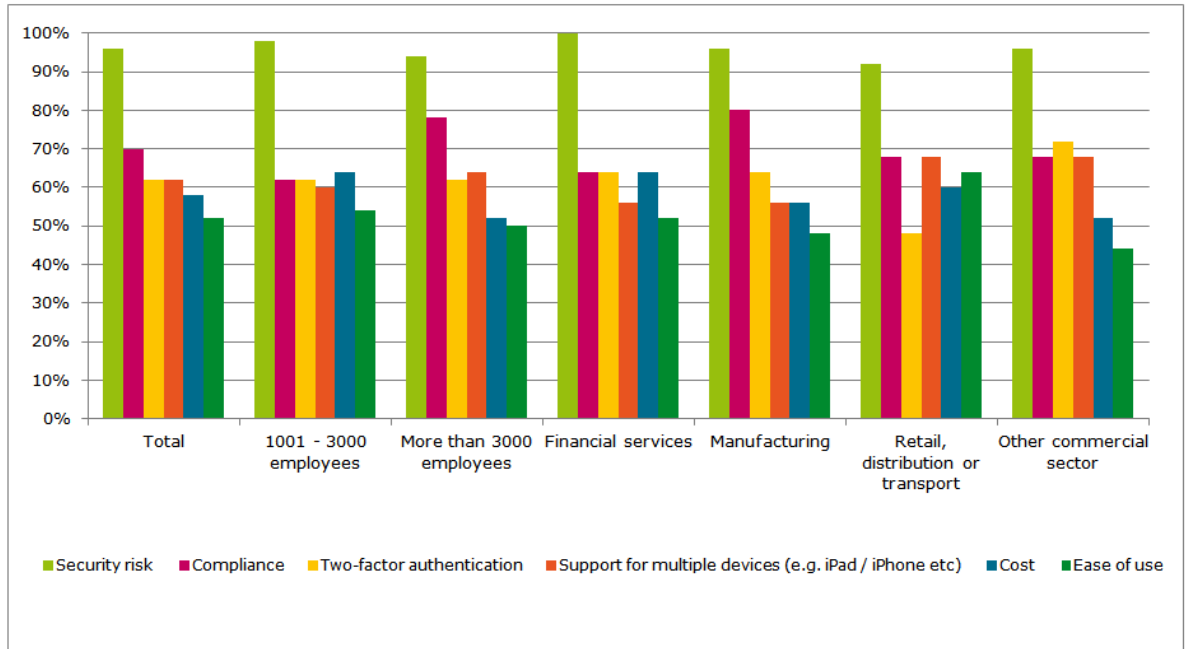
Analysis:

- In total, 66 percent of respondents' organisations don't currently have a policy in place for employees to work remotely via their own personal mobile devices. This means that a large proportion of companies are not ready to support the growing number of consumer devices that might potentially be entering the workplace. This could leave them open to security breaches, including the loss of highly sensitive company data, if the technologies aren't being managed. If this is something they may struggle to do internally, businesses need to look at outsourcing or managed service opportunities around implementing a policy and the on-going management of it. The added benefits of managed services would also mean that the network can be protected globally twenty four hours a day, seven days a week, three hundred and sixty five days a year, taking the hassle away from the business, allowing it to concentrate on its core focus.

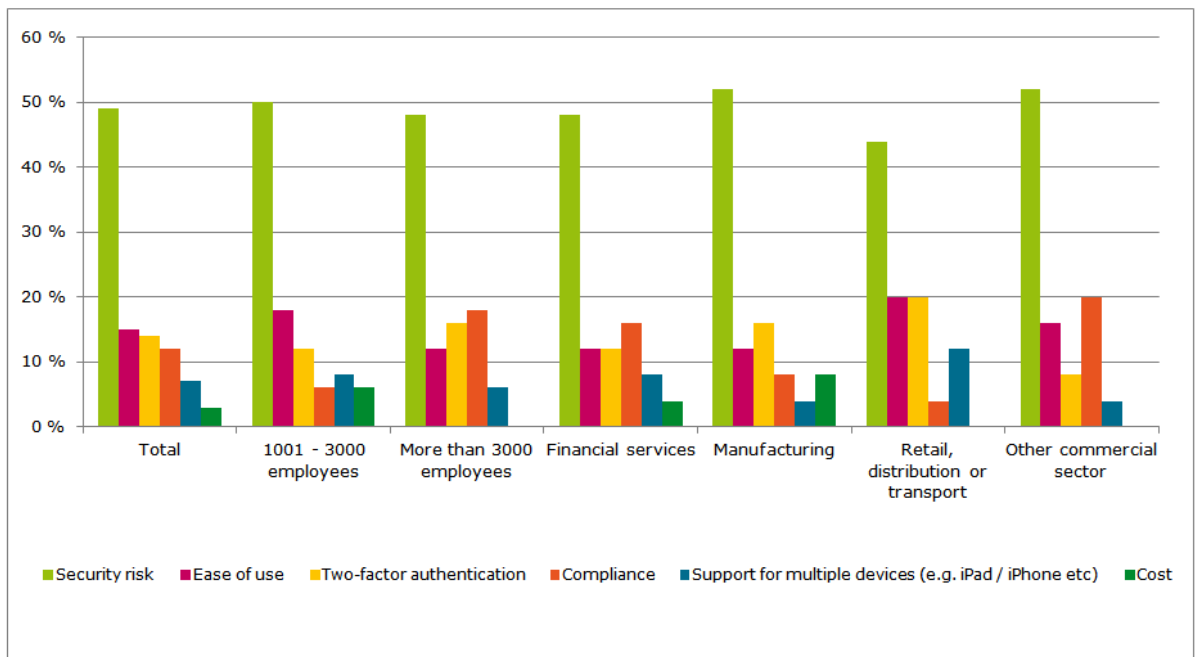
3.

(a) In order of the most significant first, please select and rank from the list below what you think are the top four most important considerations when implementing such a policy:

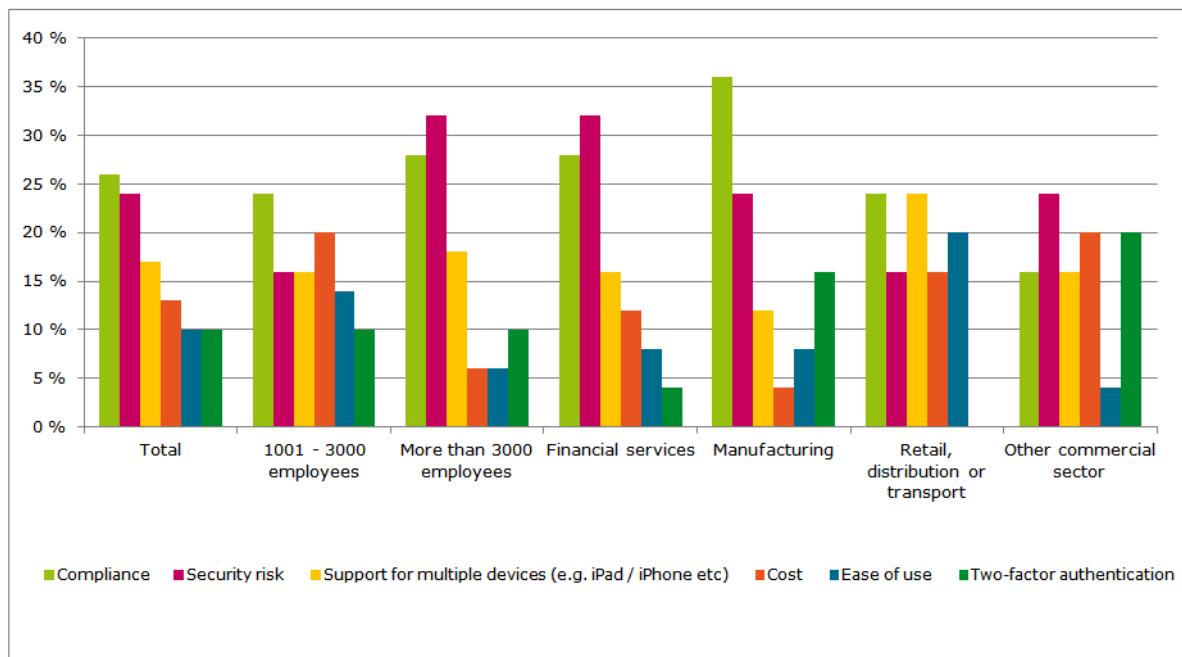
NB: This represents the total number of respondents who ranked the following options anywhere between 1 and 4



(b) In order of the most significant first, please select and rank from the list below what you think are the top four most important considerations when implementing such a policy: Responses ranked 1.



(c) In order of the most significant first, please select and rank from the list below what you think are the top four most important considerations when implementing such a policy: Responses ranked 2.



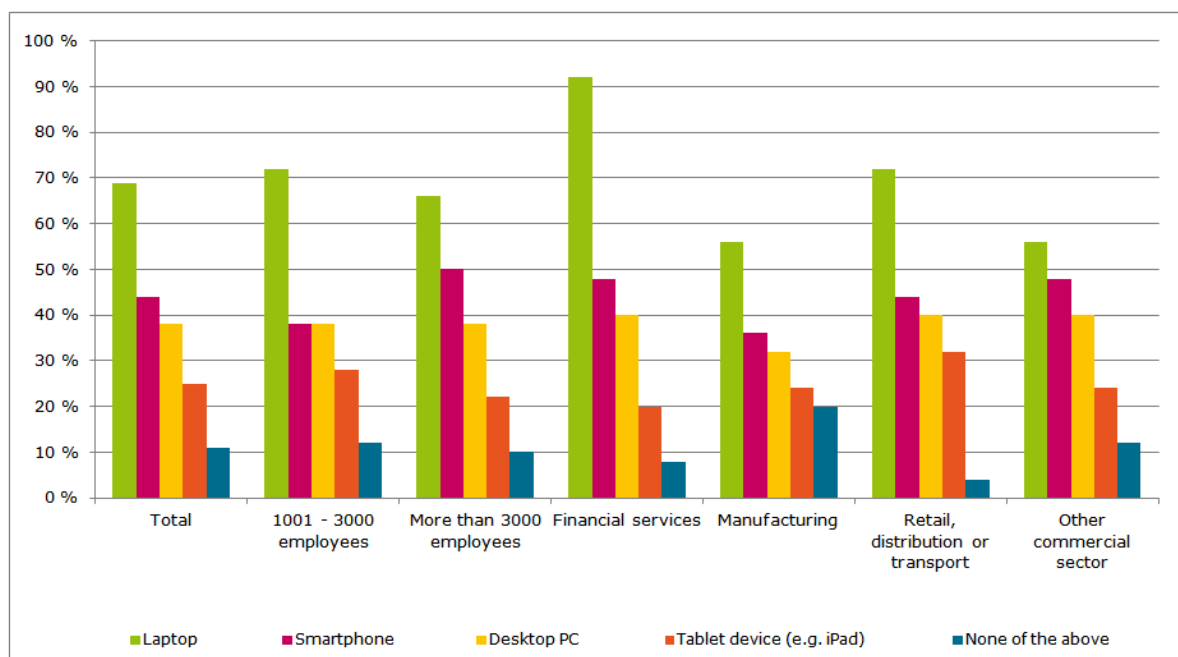
Key stats:

- A massive 96 percent of those surveyed selected security risk as one of the top four most important considerations (graph a) when implementing a policy for employees to work remotely via their own personal mobile device.
- A total of 49 percent selected security risk as the top concern overall (graph b).
- After security, compliance is the second most important consideration, with 70 percent of respondents ranking it in their top four concerns (graph a) and 26 percent ranking it the second most important consideration (graph c).

Analysis:

- Whilst there are a number of important considerations, including ease of use, two-factor authentication, support for multiple devices (e.g. iPad/ iPhone) and cost, security risk is unanimously the largest. This shows that security is top of mind, yet still there is hesitancy by many to put a policy in place. Businesses need to address this and not shy away from it.
- Networks and infrastructure do require highly skilled personnel to put policies in place and manage them effectively. If this is not possible within an organisation whether for financial reason or other, to get round this, businesses can look to outsource or deploy managed services in the place of IT specialists, which can help with long term stability and ease of use.

4. Which personal device(s) do you use to work remotely at home or whilst on the move? (Not supplied by your company)



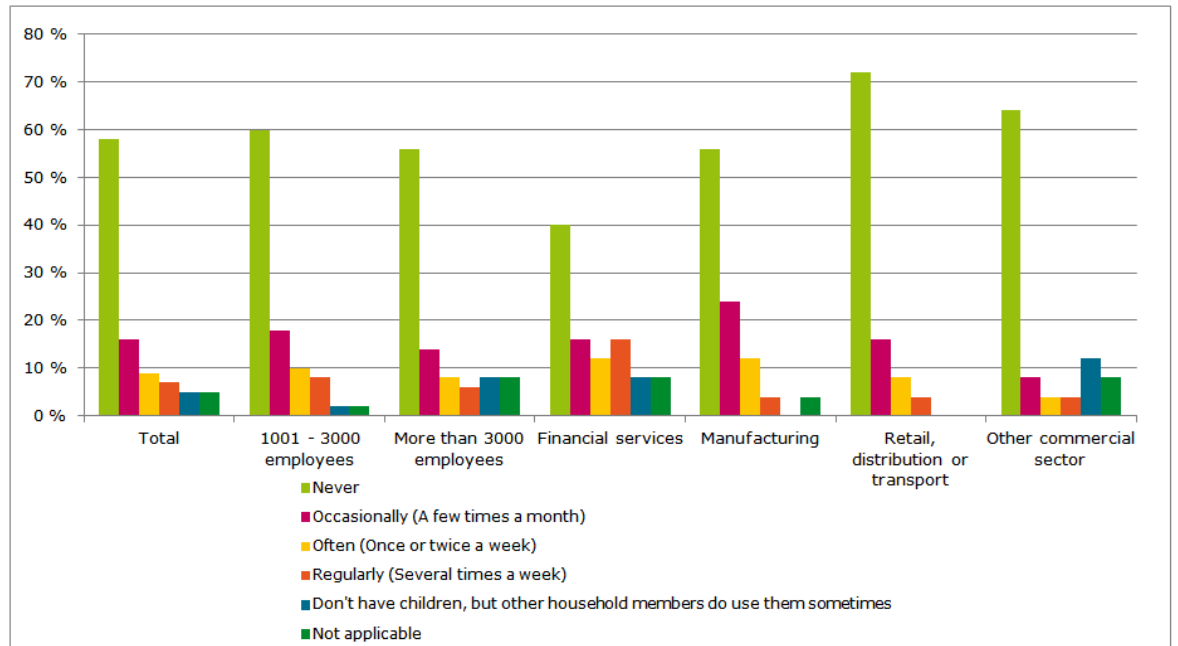
Key stats:

- In total, 69 percent of those surveyed use smartphones and tablet devices not supplied by the company to work remotely at home or whilst on the move (44 percent smartphones and 25 percent tablet devices).
- A huge 92 percent of employees in the financial sector use their own laptops to work remotely at home or whilst on the move.

Analysis:

- There is a large proportion of people already using their own devices to work remotely at home or whilst on the move. So businesses really need to take heed of this to ensure that the devices are connected securely with the office network and that they are in control of it.
- The financial services sector is still heavily reliant on laptops, as well as other devices which may tie into the fact that they work from home more regularly and have greater volume of sensitive information at risk.
- Tablet devices have only really been around on a mass scale for a few years. But already a quarter of tablet device users are using them for work purposes.

5. Do you let your children (or other members of your household) use your work device e.g. laptop, smartphone, tablet device such as an iPad?



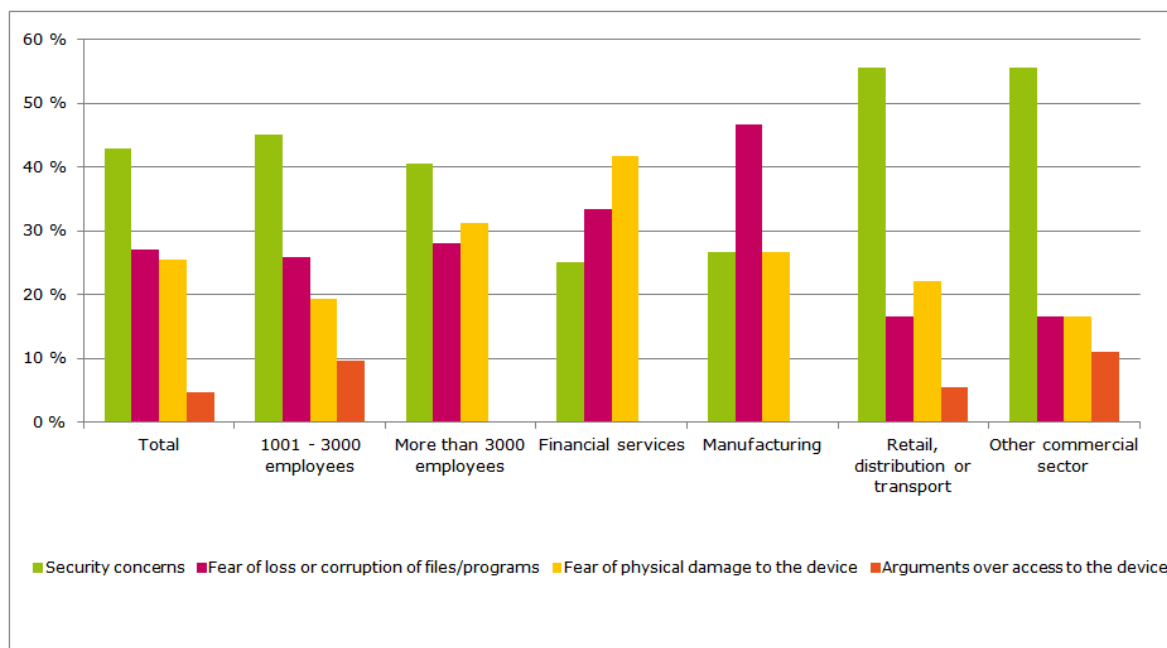
Key stat:

- In total, 37 percent of respondents allow their children (or other members of their household) to use their work device e.g. laptop, smartphone and tablet device.

Analysis:

- This is a surprisingly high proportion of people allowing their children or other household members to use their work devices, especially considering how big a consideration security risk played in question three (96 percent). This again presents an opportunity for companies to ensure that devices which will cross over from personal to professional life are managed safely and securely by the business.

6. Which of the following is or would be the main reason for you NOT letting children or other household members use your work device?



Base: Only asked of respondents who do not have children or do not let their children use their work devices

Key stat:

- In total 43 percent of respondents state that security concerns would be the main reason for them not allowing children or other household members using their work devices.

Analysis:

- This result reiterates the security concern surrounding the use of work devices outside of the office. Having a policy in place will help employees to understand how the devices can be used, what is safe and what isn't.

Part 3. Appendix

SecureData commissioned a Vanson Bourne Omnibus survey of 100 IT managers in large UK enterprises (more than 1,000 employees) across the financial services, manufacturing, retail, distribution/transport and commercial sectors. The following questions were asked:

- Does your organisation allow employees to work from home?
- Does your organisation currently have a policy in place for employees to work remotely via their own personal mobile devices such as smartphones and iPads?
- What do you think are the most important considerations when implementing such a policy?
- Which personal device(s) do you use to work remotely at home or whilst on the move (Not supplied by your company)?
- Do you let your children use your work device e.g. laptop, smartphone, tablet device such as an iPad?
- Which of the following is or would be the main reason for you NOT letting children or other household members use your work device?

To find out further information about SecureData or the survey, please contact Jessica Hayward:

Jessica Hayward

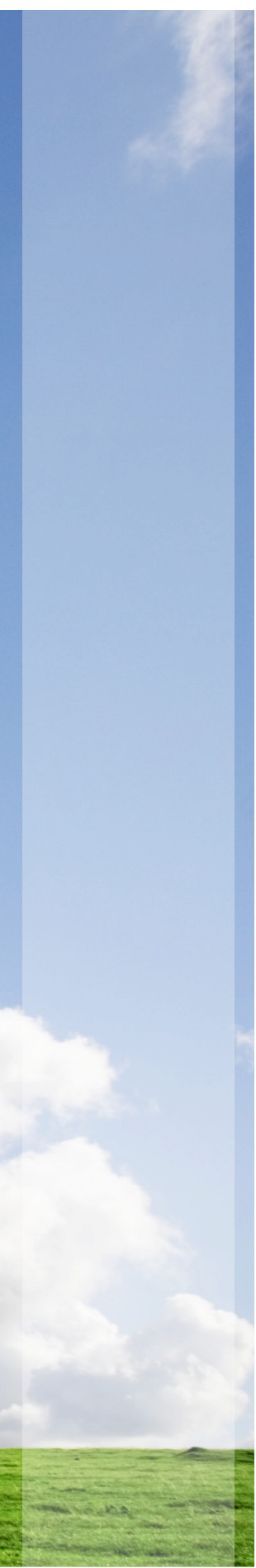
Marketing Manager

SecureData

D: 01622 723444

marketing@secdata.com

www.secdata.com



To contact us

Tel: 01622 723456

Email: marketing@secdata.com

Web: www.secdata.com

SecureData, SecureData House, Hermitage Court, Hermitage Lane, Maidstone ME16 9NT

T: 01622 723400 F: 01622 728580 www.secdata.com

SecureData, Unit 1, Horizon Business Park, 1 Brooklands Road, Weybridge, Surrey KT13 0TJ

T: 01622 723400 F: 01622 728580 www.secdata.com

November 2011