WHITEPAPER

Remote Access

The Future Of The Workforce

Author SecureData

March 2013

Part 1. Executive Summary

CONTENTS

2012 saw the first 4G mobile network launched in the UK followed by an influx of 4G-enabled devices onto the market, including the eagerly anticipated iPhone 5. However, 2013 will be the year 4G really starts to make its mark. The winners of the spectrum auctions were announced in February and most mobile operators are launching their 4G networks in the coming months, which will lead to faster connection speeds and higher availability of mobile internet.

By the end of the year we can expect to see a vast number of consumers using 4G to access the internet as a result of this. But how will this improved access impact businesses and remote working? Will better speed and availability lead to a greater demand from employees looking to access the organisation's networks remotely and, if so, are IT departments and businesses prepared for this and the extra security risks it could bring?

SecureData has conducted a study of IT managers to get their opinions on the situation; we believe the following are the most salient findings:

- All employees are now able to work remotely at some point during an average working month; a year ago this was not the case.
- Over half of organisations believe that the introduction of advanced technologies such as 4G will impact the number of employees accessing their networks remotely due to higher availability and faster internet connections.
- Over 80% of organisations expect to see an increase in employees requesting BYOD (Bring Your Own Device) schemes to take advantage of the faster connections and higher availability offered by advanced technologies such as 4G.
- Over 80% of organisations expect there to be an increase in security risks to their business with the higher availability and faster connections to the internet with advanced technologies such as 4G.
- 33% of organisations have budget assigned specifically for security issues associated to remote access.

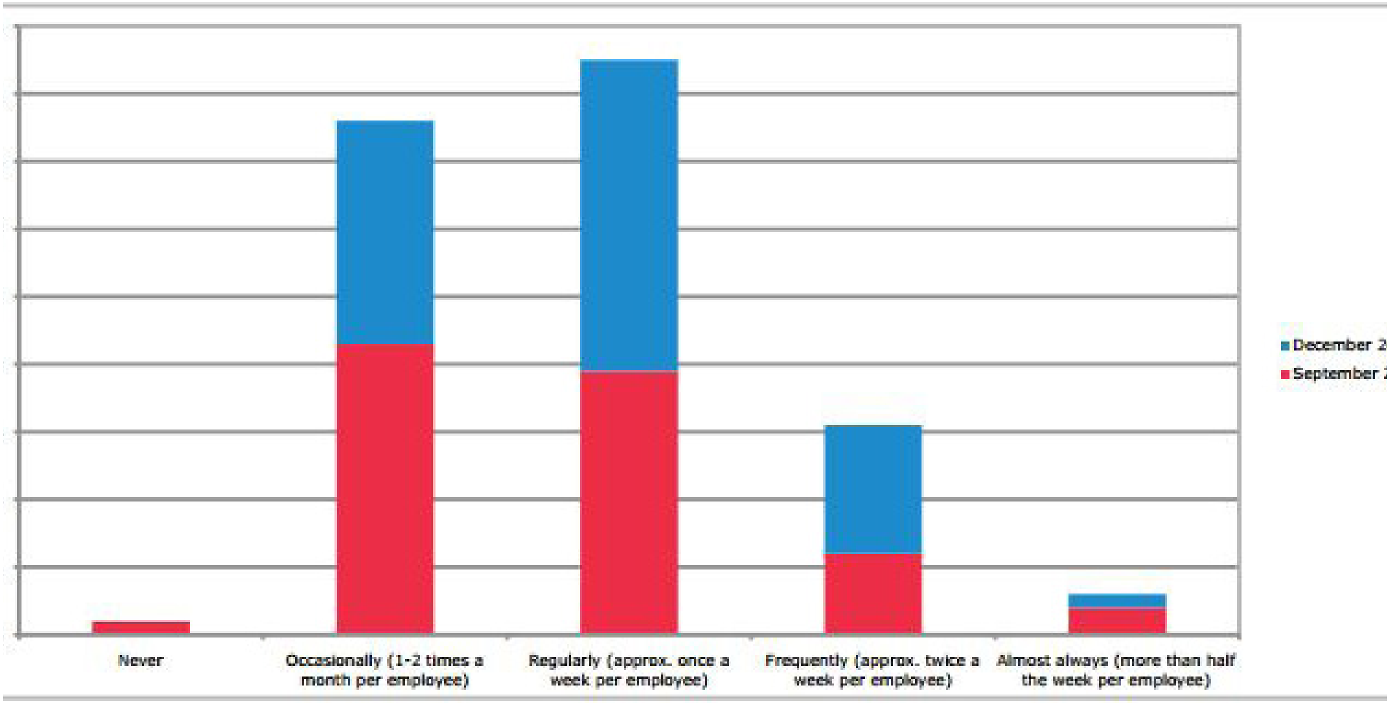
There are more employees than ever accessing their organisation's network remotely on a regular basis. Organisations are also beginning to recognise that with the advancement of technologies, such as the rollout of 4G, and the improvement in internet connectivity, even more employees will look to access their networks remotely. Alongside this, organisations recognise that these changes will create more security risks. However, most are unprepared, as the majority of organisations do not have a BYOD policy in place permitting employees to use personally owned mobile devices (laptops, tablets and smartphones) to access the organisation's network or a remote access policy in place. Furthermore, a large percentage has no specific budget assigned to deal with the ongoing security risks associated with remote access. Most of those that do, only have budget available to deal with reactive issues.

Alan Carter,
Solutions Consultant,
SecureData

The study's findings highlight that UK businesses are aware, but still not prepared for the ever increasing number of employees looking to access networks remotely. Those waiting to see the impact 4G will have before implementing any kind of policy will leave the organisation vulnerable to more security risks. By not creating the appropriate policy and framework for employees to use personal devices, businesses are creating a bigger risk as employees will find their own ways of transferring corporate data to devices, methods which are often very risky. This may be done to allow employees to work from their own devices, and whilst not malicious, it could leave the organisation open to security breaches which could include the loss of highly sensitive data. It is vital that remote access is fully supported on an ongoing basis. If this is something a business may struggle to do internally, then it needs to look at outsourcing or managed service opportunities around implementing a policy and its ongoing management. Smartphones and tablet devices are not going away and neither is the risk to corporate data held on these devices.

Part 2. Anaysis of key findings

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



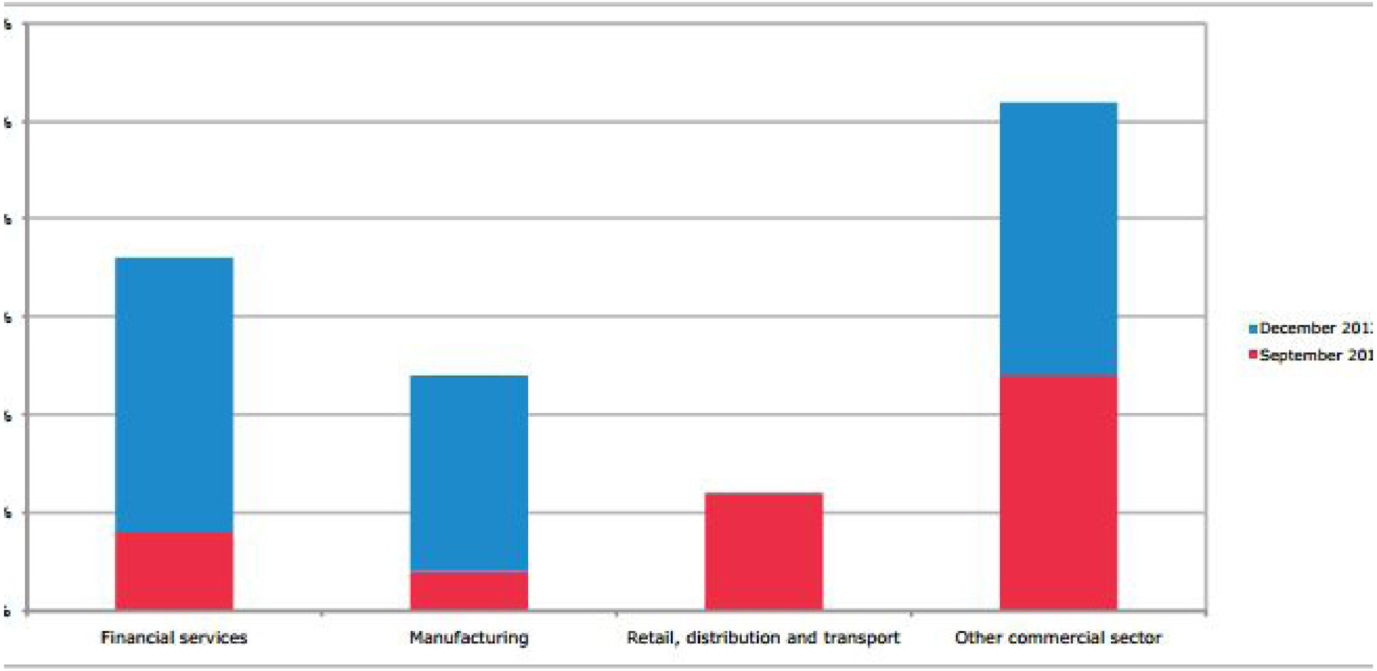
KEY FINDINGS

• For the first time, all respondents are allowed to work remotely from home at some point during their average working month.
• 79% of respondents are allowed to work remotely from home one to four times a month.
• Similarly to the previous year (see appendix), 56% of respondents in the financial services sector work from home regularly (approximately once a week). However, there has been a major increase in employees working from home more frequently in this sector (approximately twice a week), rising from 8% to 28% over the last year.

ANALYSIS

These results highlight the ever-increasing trend in flexible working across a variety of industry sectors. With 100% of all respondents now allowed to work remotely from home it shows that businesses are embracing flexible working practices on an even greater scale. However, with increasing numbers of employees working from home this means more and more confidential data is being shared across networks and devices and this is particularly prudent in the financial services sector where numbers working from home are higher and there is often a greater volume of confidential data. There are a number of security issues that need to be addressed by businesses in order to offer employees the benefits that can be found with remote working, while ensuring peace of mind that business data is protected at all times.

2. Does your organisation currently have a policy in place for employees to work remotely via their own mobile device such as a smartphone and / or a tablet.



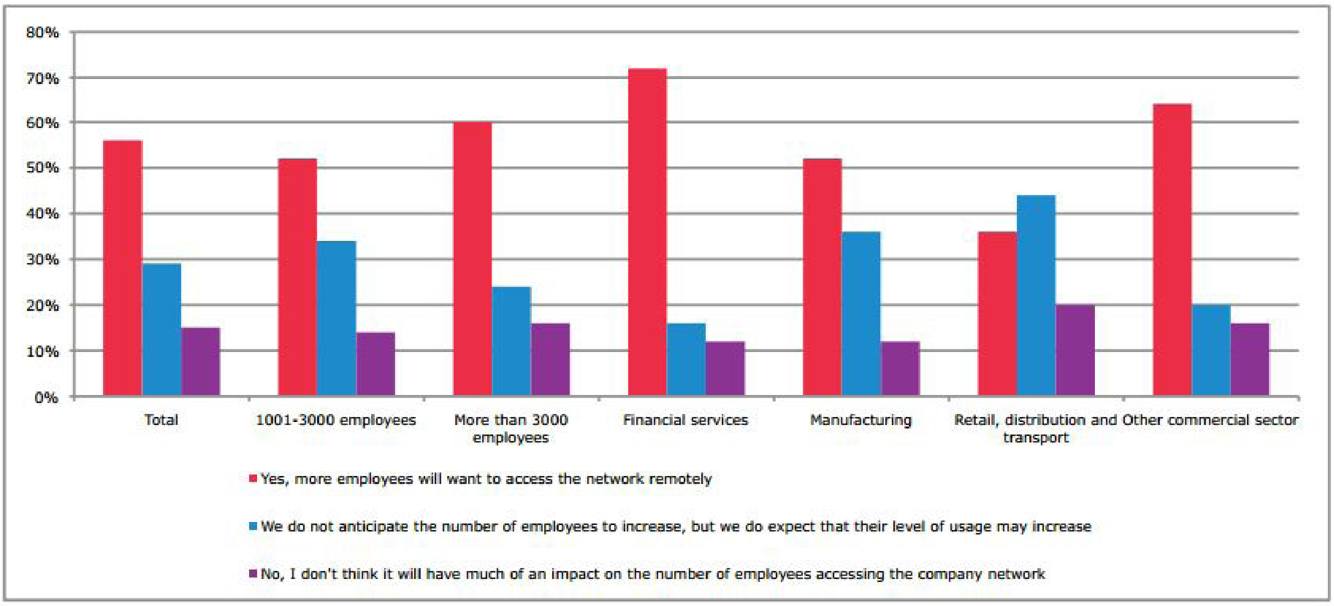
KEY STATISTICS

- 39% of respondents have a policy in place for employees to work remotely via their own personal mobile device.
- 14% of respondents do not see having a BYOD policy in place as a priority at all.
- There has been an increase over the last 12 months in organisations putting BYOD policies in place to support employees working remotely from home or on the move (see appendix). The highest rises were seen in larger businesses (of more than 3,000 employees) up from 6% to 40%

ANALYSIS

There has been an increase over the last 12 months in the number of organisations putting BYOD policies in place, particularly in large businesses, showing that its importance is being recognised by some. However, given that 100% of employees are now able to work from home (as per Q1) and only 39% of organisations actually have a BYOD policy already in place and 14% don’t even see putting a policy in place as a priority, it suggests that many organisations are still lagging behind or are not recognising the importance of getting policies in place now.

3. Do you think higher availability and faster connections to the internet with technology advancements such as 4G will have a direct impact on the number of employees accessing your organisation's network remotely?



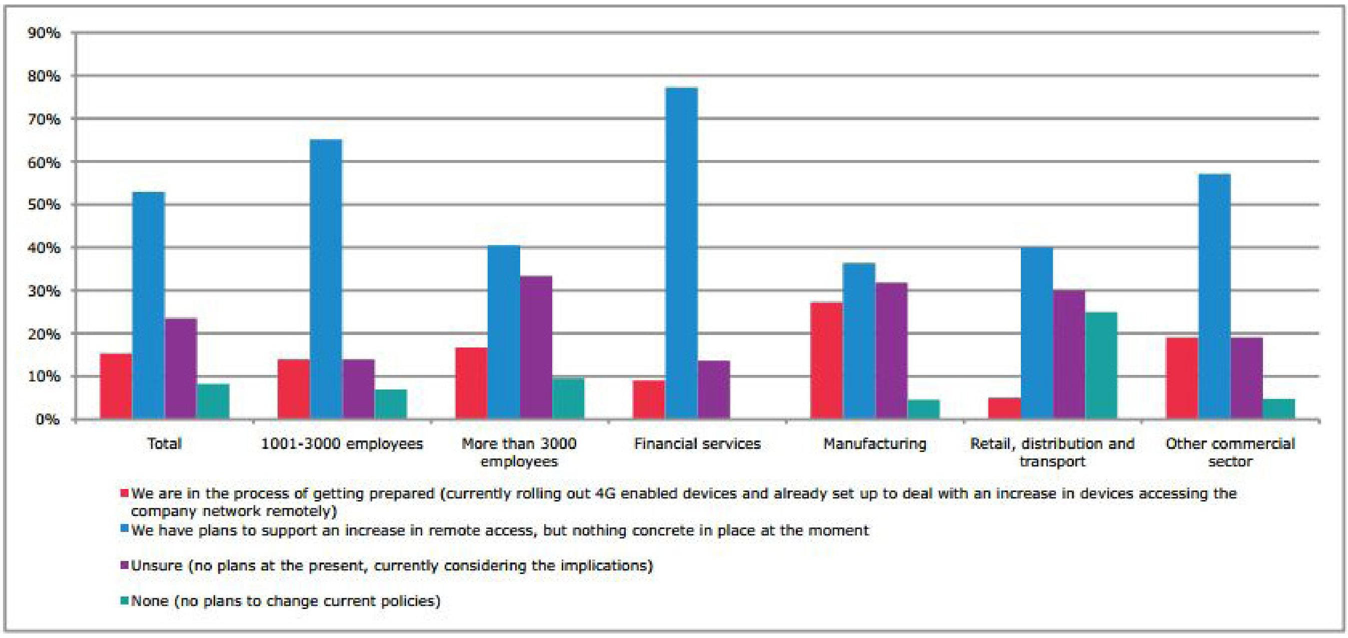
KEY STATISTICS

- 56% of respondents believe that higher availability and faster connections to the internet with technology advancements such as 4G will impact the number of employees accessing their networks remotely.
- According to the respondents, the greatest impact is expected to be seen within the financial services sector with 72% anticipating an increase in demand on the network.
- Demand is also expected to be greater in larger organisations with 3,000 employees or more. In total, 60% of large organisations envisage an increase in demand.

ANALYSIS

Over half of organisations expect to see an impact on the number of employees accessing their networks remotely as a result of higher availability and faster connections to the internet with technology advancements such as 4G. This is even higher in the financial services sector and with organisations of more than 3,000 employees. However as we have seen in Q2, 61% do not have a BYOD policy in place to deal with this. This reveals that businesses are not prepared for an influx in demand on the network through personal mobile devices. This may be due to 4G still being relatively new in the UK. As the full UK rollout is not due until later in 2013, organisations may be waiting to see its full impact before setting a policy in place. However, it is vital that policies are put in place as soon as possible, to ensure organisations are protected.

4. Are you already prepared for a potential increase in employee usage or the number of employees accessing your organisation’s network remotely due to technology advancements such as 4G?



KEY STATISTICS

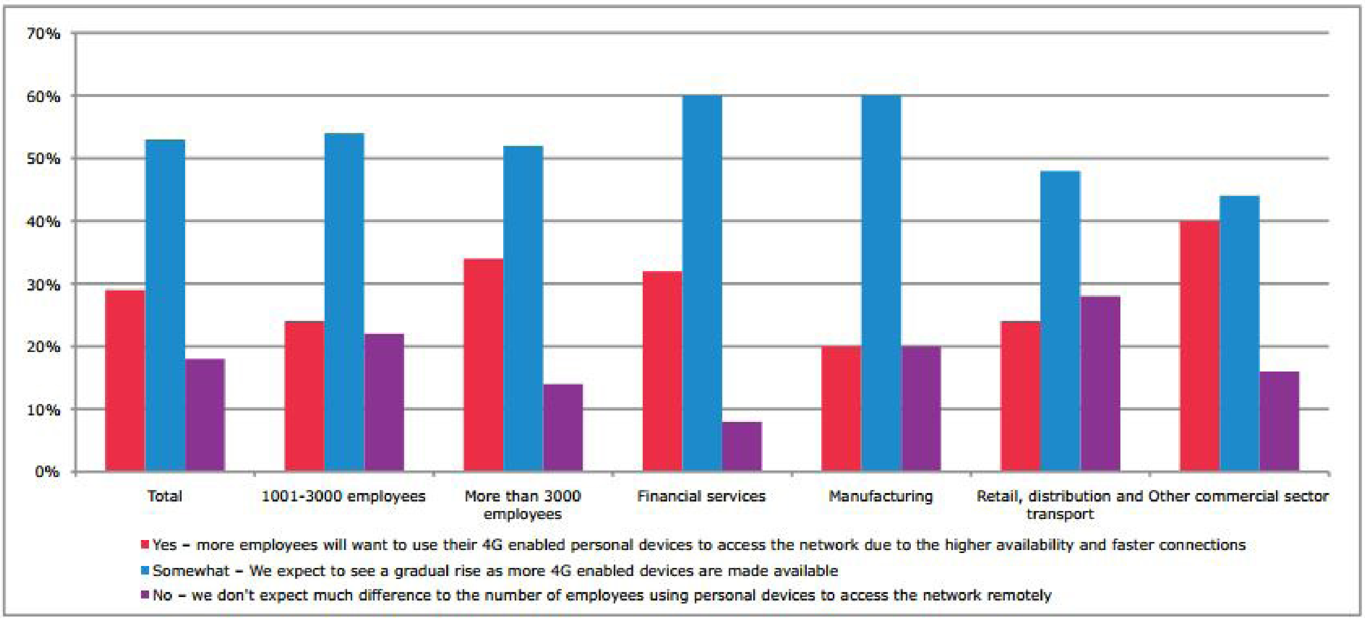
- 15% of respondents are in the process of getting prepared for a potential increase in employees accessing the organisation’s network remotely - by rolling out 4G enabled devices and being set up to deal with an increase in devices accessing the network remotely.
- 53% of respondents have plans to support an increase in demand for remote access working, but nothing concrete in place yet.
- 77% of financial services organisations also have plans in place to support the increase in demand but only 9% are already in the throes of preparation.
- Over a quarter of organisations in the manufacturing sector are also in the process of preparing for a potential increase in employee usage or in the number of employees accessing their organisation’s network remotely due to technology advancements such as the 4G rollout – including rolling out 4G enabled devices to employees.

ANALYSIS

Although 56% of organisations expect to see an increase in demand with the introduction of advanced technologies such as 4G (Q3) only 15% are actually in the process of preparing for the influx. Without policies already in place and without staff buy-in and understanding it can leave organisations vulnerable to attacks and at risk of losing confidential data. It is vital that employees are educated on the policy in order to avoid any confusion and accidents leading to security breaches.

Furthermore, the surge in employees accessing the network brings another concern for businesses. Organisations must increase their system’s capacity now to ensure that the network is capable of supporting the anticipated extra users.

5. Do you foresee an increase in employees requesting BYOD schemes in the workplace to take advantage of the higher availability and faster connections to the internet with advanced technologies such as 4G?



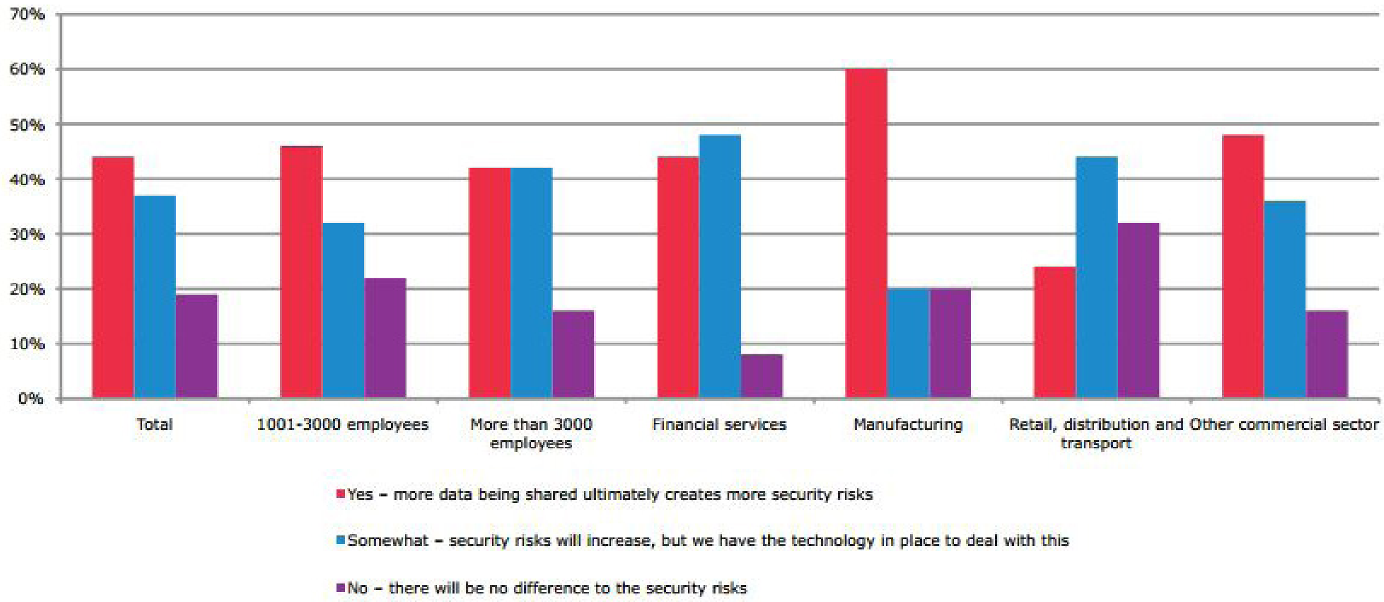
KEY STATISTICS

• Over 80% of respondents expect to see an increase in employees requesting BYOD schemes to take advantage of the faster connections offered by advanced technologies such as 4G. 53% believe this will be a gradual rise.
• 92% of respondents in the financial services sector expect to see an increase in employees requesting BYOD schemes with the introduction of advanced technologies such as 4G.
• 86% of respondents in organisations of over 3,000 employees expect to see an increase in employees requesting these schemes.

ANALYSIS

Organisations (in particular in the financial services sector and those with more than 3,000 employees) are recognising that with better facilities and technologies more employees will be looking for BYOD and flexible working schemes. They are also recognising that with new technologies employees will be looking to use their own devices that are 4G-enabled to make the most of the faster connections and availability. Organisations need to have a policy in place to make sure that any data accessed from the network on personal devices is only seen and retrieved by the employee. For example, ensuring a child using the family iPad cannot access business emails or documents.

6. Do you think higher availability and faster connections to the internet with advanced technologies such as 4G will bring increased security risks for your organisation?



KEY STATISTICS

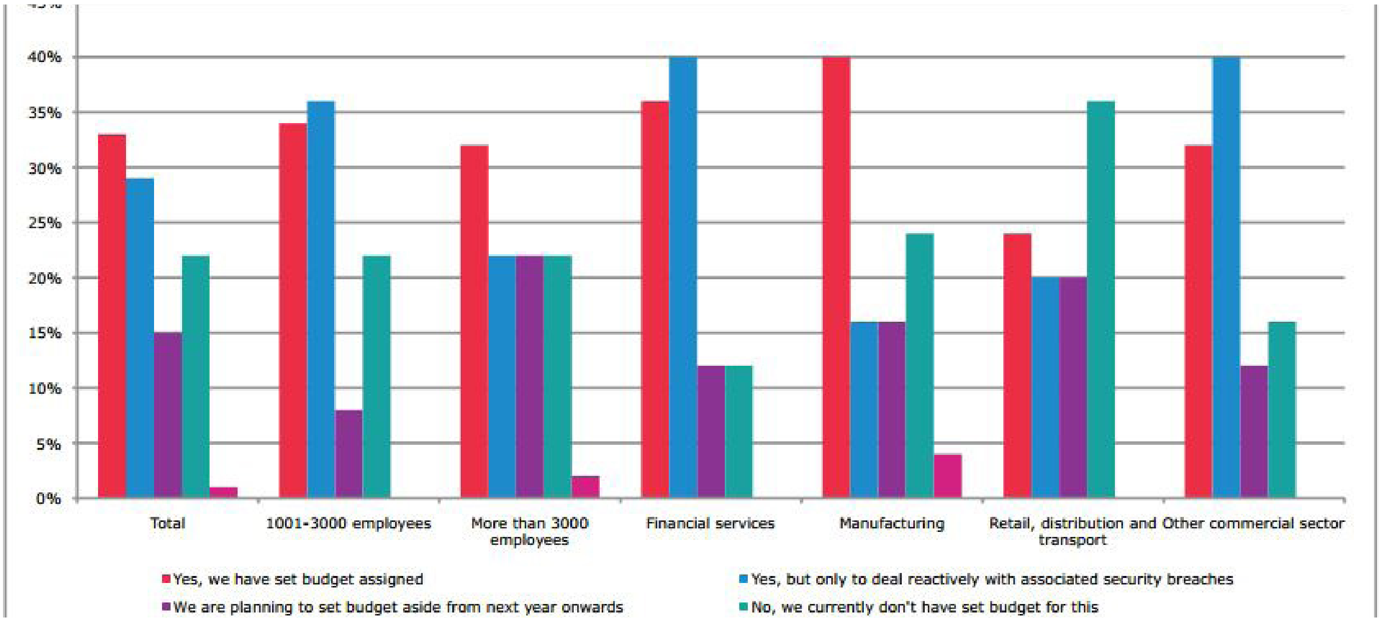
• Over 80 per cent of organisations expect there to be an increase in security risks with higher availability and faster connections to the internet with the introduction of advanced technologies such as 4G.

• Manufacturing was the industry most concerned with the increased threat of security risks with 60% of repondents expecting an increase in data being shared across the network leading to more security risks.

ANALYSIS

The vast majority of organisations expect to see an increase in security risks as a result of advanced technologies such as 4G. However, as we saw in previous questions, 85% of organisations have no set plans in place to support this increase. It is clear that organisations can see there are risks associated with BYOD and remote access, particularly given the rollout of 4G, however they are not acting upon it.

7. Does your organisation currently have budget assigned specifically for security around employees accessing the network remotley?



KEY STATISTICS

- In total, 33% of respondents have budget assigned for security issues associated with employees accessing the network remotely and 29% of organisations only have budget assigned for reactive issues.
- 40% of respondents in the financial services sector have budget purely assigned for reactive security issues.
- Manufacturing is the most prepared industry sector with 40% of organisations having budgets already assigned for the security risks associated with remote access.

ANALYSIS

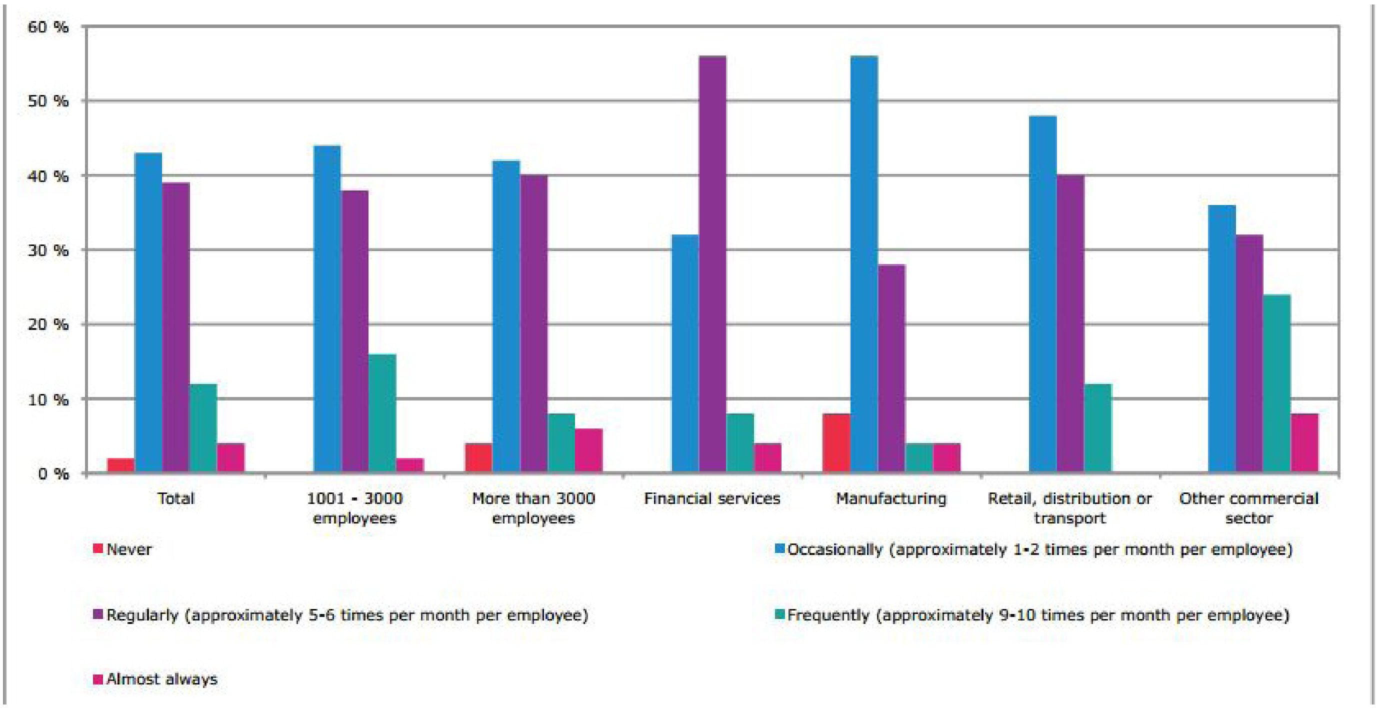
Only a third of organisations have budget assigned for ongoing security risks associated with remote access, even though the majority of respondents recognise that there will be an increase in risks (Q6). This could leave many businesses out of pocket as they try to combat the risks. Furthermore, just under a third have budget assigned for purely reactive issues, thus leaving organisations at risk on a daily basis without a fully managed system in place. It is essential for organisations to be prepared and able to tackle security issues head on and not just mobilising when an issue has already occurred.

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:

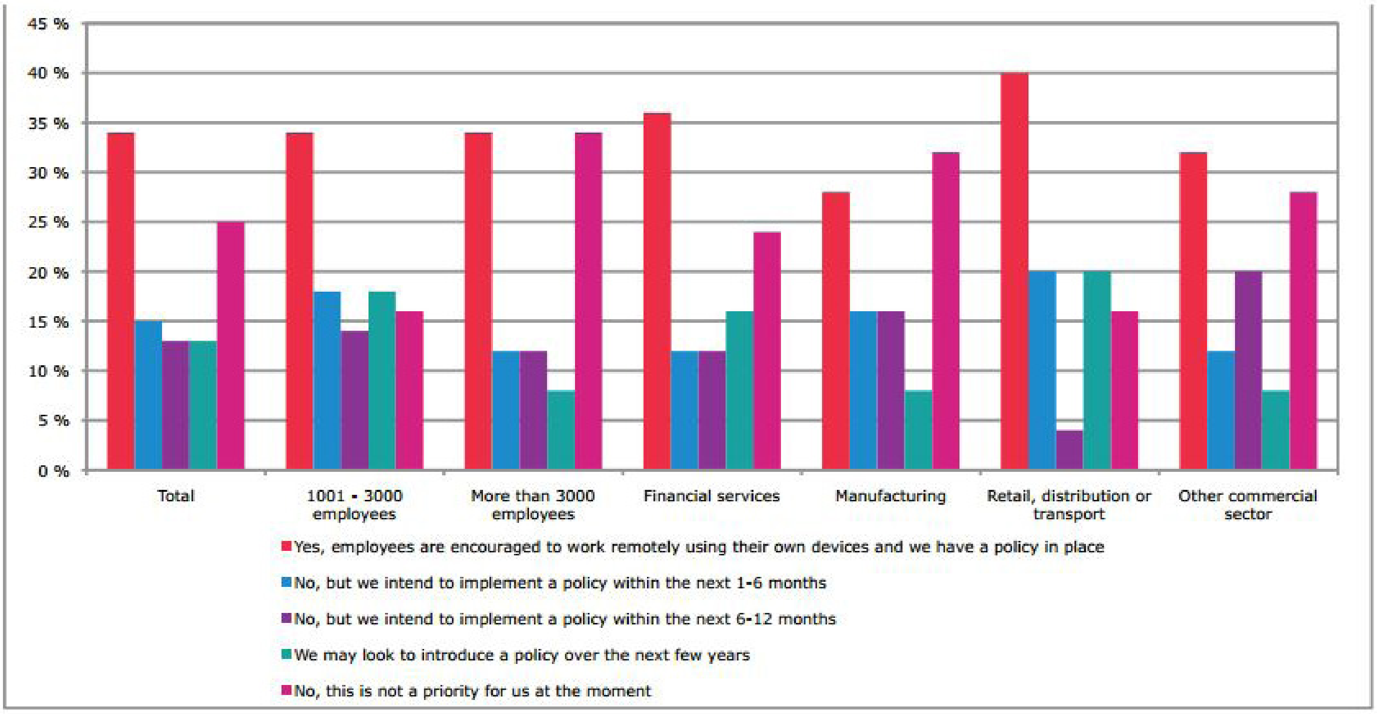
- Does your organisation allow employees to work from home?
- Does your organisation currently have a policy in place for employees to work remotely via their own personal mobile devices such as smartphones and iPads?
- Do you think higher availability and faster connections to the internet with technology advancements such as 4G will have a direct impact on the number of employees accessing your organisation's network remotely?
- Are you already prepared for a potential increase in employee usage or the number of employees accessing your organisation's network remotely due to technology advancements such as 4G?
- Do you foresee an increase in employees requesting BYOD schemes in the workplace to take advantage of the higher availability and faster connections to the internet with advanced technologies such as 4G?
- Do you think higher availability and faster connections to the internet with advanced technologies such as 4G will bring increased security risks for your organisation?
- Does your organisation currently have budget assigned specifically for security around employees accessing the network remotely?

2011 research graphs referenced in Questions 1 and 2

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



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?



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?
- Do you think higher availability and faster connections to the internet with technology advancements such as 4G will have a direct impact on the number of employees accessing your organisation's network remotely?
- Are you already prepared for a potential increase in employee usage or the number of employees accessing your organisation's network remotely due to technology advancements such as 4G?
- Do you foresee an increase in employees requesting BYOD schemes in the workplace to take advantage of the higher availability and faster connections to the internet with advanced technologies such as 4G?
- Do you think higher availability and faster connections to the internet with advanced technologies such as 4G will bring increased security risks for your organisation?
- Does your organisation currently have budget assigned specifically for security around employees accessing the network remotely?

2011 research graphs referenced in Questions 1 and 2

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