AVG SMB Market Landscape Report 2011

Contents

Following the success of AVG's SMB market landscape study in 2010, GfK was commissioned to conduct a follow-up study in mid-2011 with the remit of understanding how the market has changed in the previous 12 months.

Six main themes resulted from the research:

01 **SMBs may be responding to renewed economic uncertainty, as they rein in IT spend in 2011**
Overall SMB IT spend has declined against 2010, as a likely result of organisational austerity measures. Alongside this, we have observed that attitudes towards IT spending (such as outsourcing and decision-making) have become more conservative.

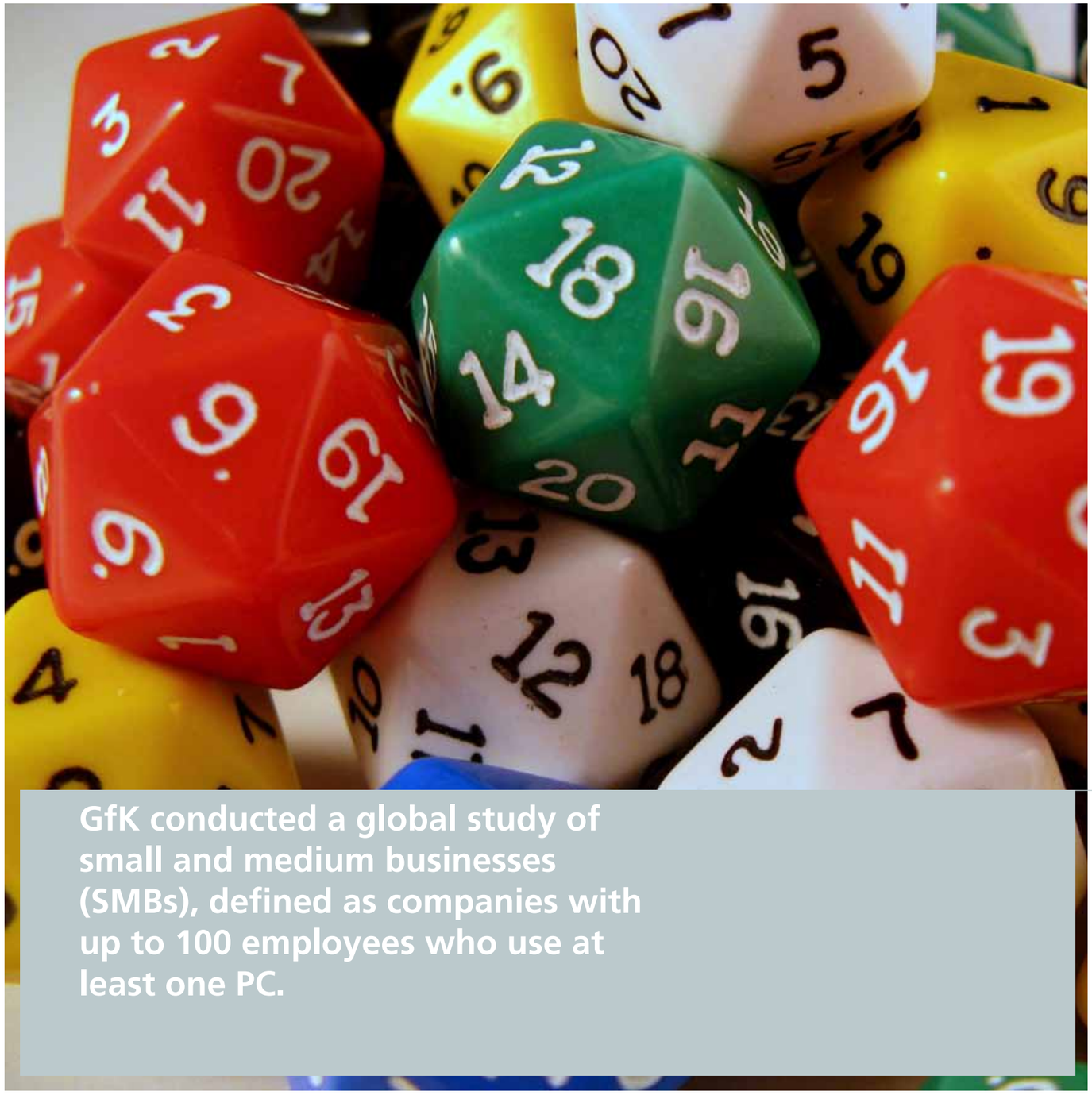
02 **SMBs are embracing technologies to increase levels of mobility, but few are aware of the potential dangers they present**
Alongside the use of a wider variety of hardware devices, SMBs are showing greater interest in solutions suitable for use by mobile workers. However, not all are aware of the IT security risks that accompany this technology.

03 **SMBs recognise the opportunities which social networking offers their companies to promote their business and engage with customers**
One-in-three SMBs has a social network page or profile on the three major social networks, and are most commonly using them to engage customers and to share company and product information.

04 **Traditional IT vulnerabilities still cause most concern; although SMBs are waking up slowly to emerging IT security threats**
The majority of SMBs remain focused on the more traditional threats to IT security, such as email and web viruses. However, they are becoming aware of new ways in which their organisational security can be compromised, including theft of information and social engineering.

05 **While greatest security concerns were around losing access to files and replacing hardware, the reality of IT security breaches shows the true cost to SMBs**
SMBs are often most concerned about the more short-term, logistical issues resulting from an IT security breach, including time and cost to replace damage. However, those who have experienced a breach are more likely to have seen the longer-term impacts such as a loss of sales and revenue opportunities.

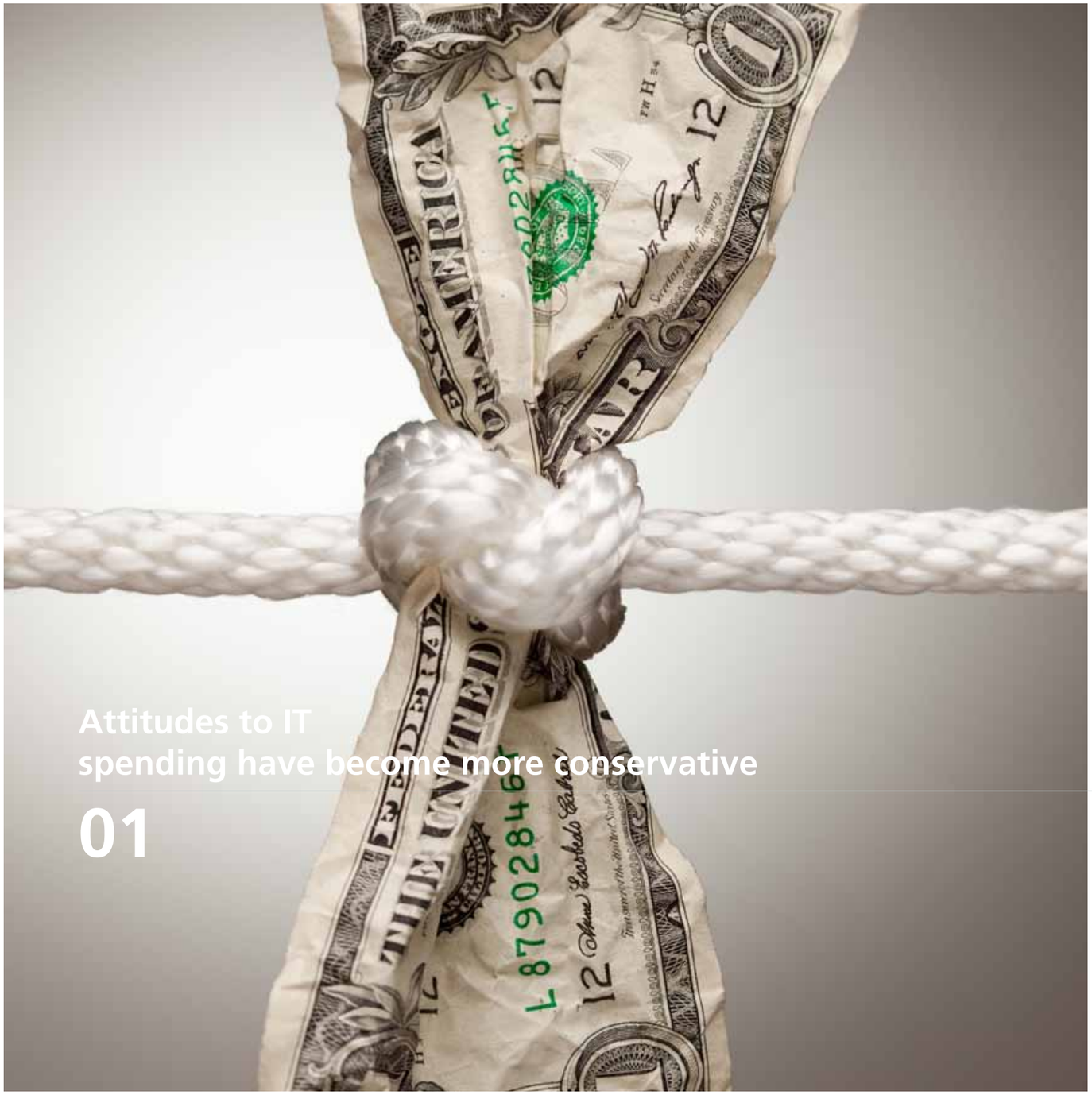
06 **Peace of mind, performance and reassurance continue to be top priorities for SMBs when considering security software**
Universally SMBs want security software to deliver the right level of protection and not impact on business performance. The vast majority of SMBs (97%) also want the reassurance of a trusted brand to deliver this.



GfK conducted a global study of small and medium businesses (SMBs), defined as companies with up to 100 employees who use at least one PC.

The quantitative survey was conducted online, with a remit of exploring the SMB IT security software market landscape. Along with revisiting the 2010 key metrics in order to understand how the market has changed in the past 12 months (size, spend, attitudes), there were also several new areas explored around the use of emerging technology and the implications for IT security. 1,000 interviews were conducted in the USA and UK during August 2011. Individual respondents were senior business decision makers responsible for IT purchasing decisions.

All data referenced in this paper is sourced from this study.



Attitudes to IT spending have become more conservative

01

SMBs may be responding to renewed economic uncertainty, as they rein in IT spend in 2011

While in the previous report in 2010 it was reported that SMBs were feeling more positive about both their outlook and that of the economy in general, it would appear that renewed uncertainty in 2011 has led to a reduction in IT spend.

SMBs in the USA are typically spending 15% less than in 2010, while their UK counterparts' outgoings have diminished by 17%. In spite of this, we do see some pockets where spend has risen against 2011. In the USA it is the 1-5 employee organisations whose investment in this area is up, while in the UK it is the medium portion (26-50) of the SMB market who appear to be spending more.

Figure 1.
Year-on-year change in IT spend by number of employees, USA

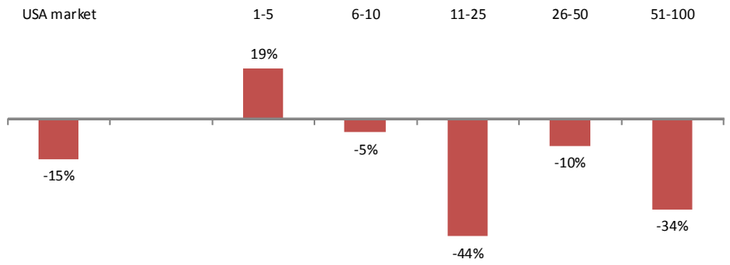
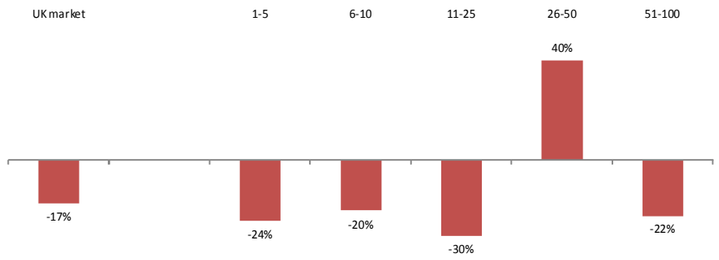


Figure 2.
Year-on-year change in IT spend by number of employees, UK



These organisations, who typically view IT as less essential to the success of their business, may be choosing to avoid investment in this area while the wider economic outlook and consumer spending remain unstable.

As a possible symptom of this, we are seeing some SMBs moving to managing IT in house, rather than incurring the extra expense associated with outsourcing. More than a half say that they would prefer to keep IT support and management in house, and that they feel confident to make IT decision without outside consultation.

Figure 3.
Agree with "I would prefer to keep IT support and management in-house", by number of employees

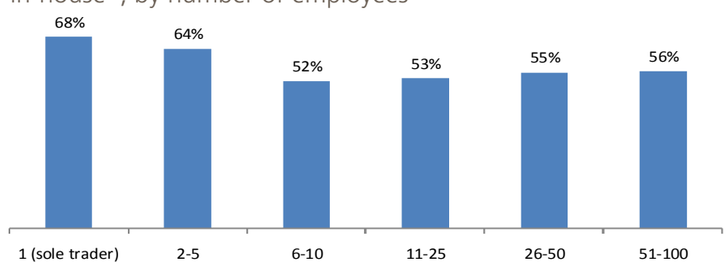
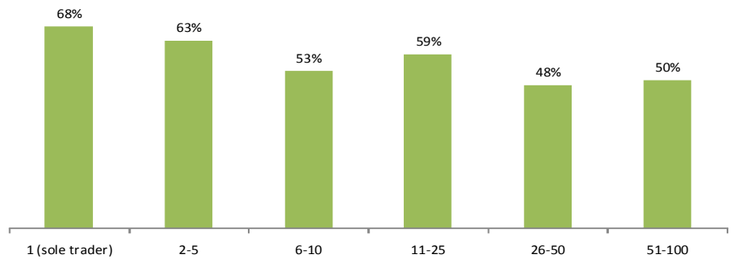
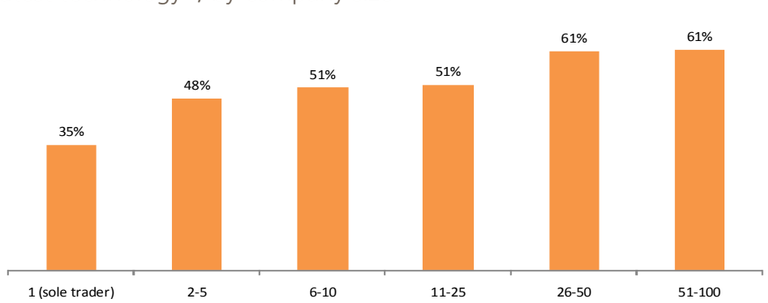


Figure 4.
Agree with "We have the confidence to make our IT decisions without outside consultation", by company size



In addition, it is the smaller organisations who feel less inclined to adopt the latest technology, which may be a method to manage their outgoings. In fact, we see that overall 22% of UK and USA SMBs spend more money on tea and coffee for staff than they do on IT.

Figure 5.
Figure v. Agree with "My business is always keen to adopt the latest technology", by company size



Mobility has become more relevant to SMBs

02

SMBs are embracing technologies to increase levels of mobility, but few are aware of the potential dangers they can present

With the rapidly-evolving mobile communications market offering many opportunities to the SMB segment, it is of no real surprise that these organisations are evaluating the options available to them. Half of SMBs in the UK and USA give employees remote access to their networks, with the typical remote worker spending one day a week working away from their office. Most popular locations for remote working are at home and on the move. When asked about the IT options which they were considering employing, many stated an interest in antivirus/internet security for smartphones and solutions for mobile workers.

Figure 6.
Remote network access among SMBs

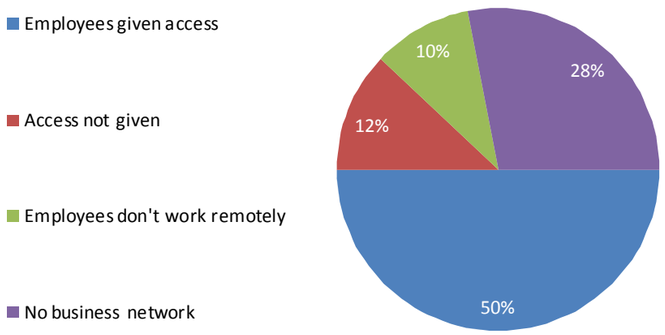
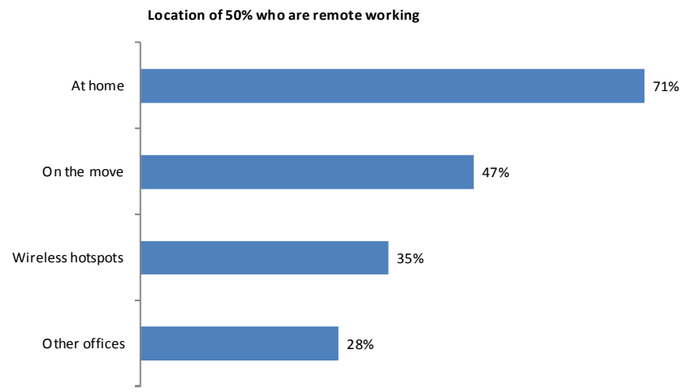
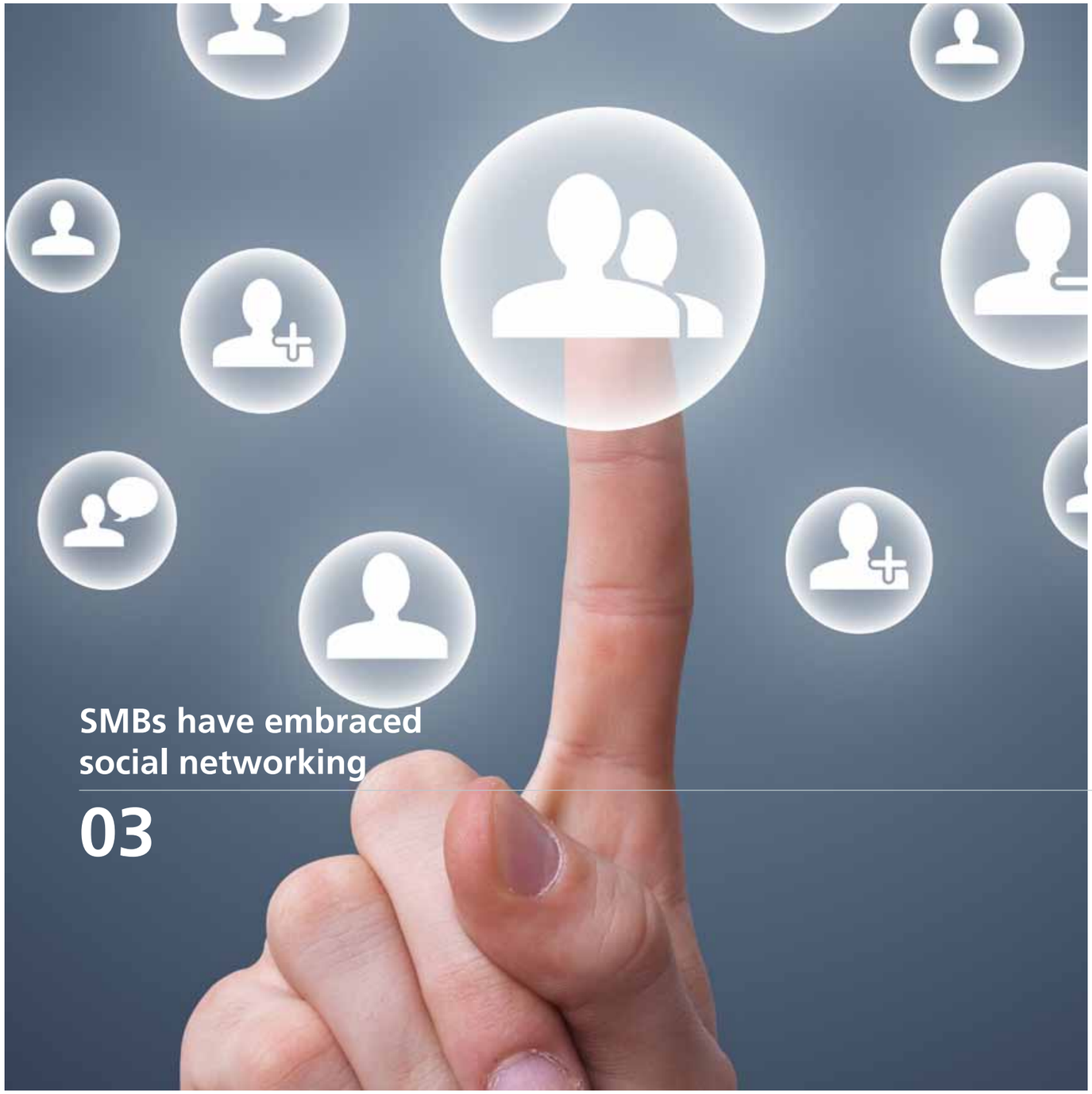


Figure 7.
Location of SMB remote workers



This technological development is best represented in the types of hardware which are currently being utilised by SMBs. One in ten SMBs are now using tablet devices, a threefold increase on 2010 – while a corresponding decline in laptop use may suggest that tablets are a seen as a more appropriate mobile computing solution, particularly among larger organisations. The fast-paced development of Android mobile technology over the past year appears to have filtered down to SMB level, where almost one in five companies is now using these devices. This uptake may have come at the expense of BlackBerry, whose penetration of UK and USA SMBs has fallen away since 2010, and now occupies the same level as Android.

However, the SMB market appears to lack awareness of the potential security issues which these developments present. Almost three quarters of SMBs do not agree that the use of mobile phones in business represents a threat to IT security.



SMBs have embraced social networking

03

SMBs recognise the opportunities which social networking offers their companies to promote their business and engage with customers

More than a third of SMBs currently have a profile or page on the three major social networks (Facebook, Twitter and LinkedIn). Facebook is the most popular, with 30% of SMBs claiming to have a page; while just under a fifth each claim to have a profile on LinkedIn and Twitter.

Figure 8.
% of SMBs who have a page/profile on social networks

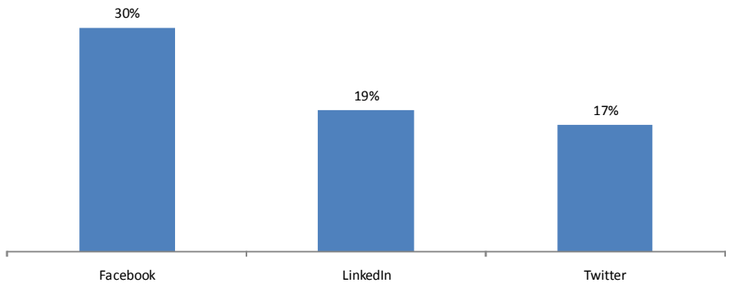
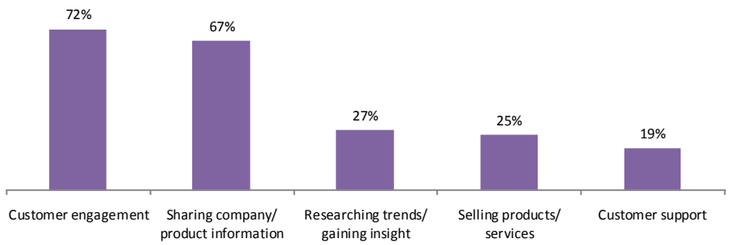


Figure 9.
How SMBs are using social networks



Almost 2-in-5 US SMBs claim to have a social networking page or profile, and they are most likely to be found in service and retail industries; and particularly among the smaller companies (2-10 seats). Also, those organisations with internal IT resources are more likely to be employing a social networking strategy.

SMBs are most frequently using social networks to engage with their customers, and to disseminate company and product information. However, more than a quarter of these organisations claim to be using their social networking connections to research trends and gain consumer insights.

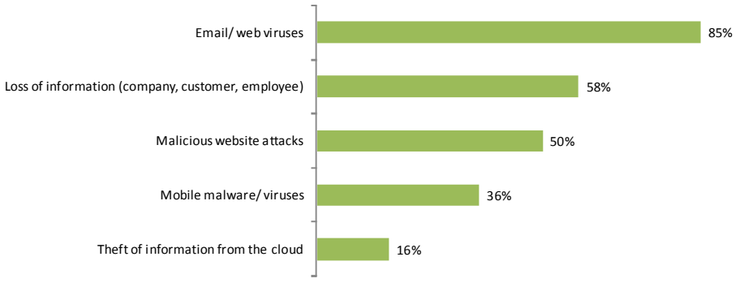
Awareness of emerging security threats among SMBs

04

Traditional IT vulnerabilities still cause most concern; although SMBs are waking up slowly to emerging IT security threats

It is likely that the proliferation of, and interest in new technology at SMB level is creating this awareness, as much of the threat can be linked to emerging technology trends. It is typically the larger end of the SMB market (51-100 employees) who are most aware of these new threats to IT security. Traditional virus sources still top IT decision-makers' security worries, with more than 4-in-5 stating that email- or web-borne viruses remain their key worry. However, it would appear that only a little over half of SMBs consider information security to be a major issue. 58% said that they were worried about loss of company or customer information, social engineering or employee identity theft. Only around a third of SMBs claim that they are worried about mobile malware and viruses, which would correspond with the increased use of smartphones and progression of technology in this area.

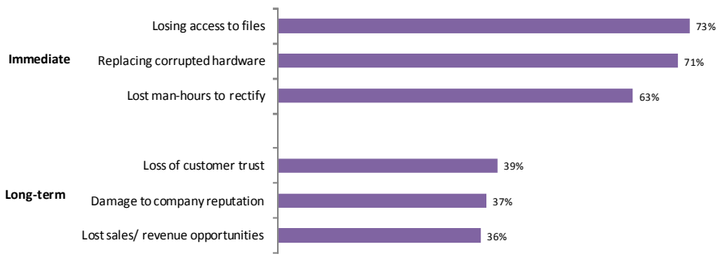
Figure 10.
SMBs' IT security concerns



In the 2010 edition of this report it was noted that large numbers of SMBs were considering moving their data into the cloud. However, we see that one-in-six of these SMBs now has concerns about the safety of their data which is stored here.

When looking at what impact SMBs feel an IT security breach would have on their organisation, it would appear to centre around the more immediate, logistical issues; including lost access to files and having to replace hardware. However, the lack of emphasis placed on the longer-term implications for their business would suggest that many SMBs may be unaware of the extent to which their organisation can be damaged by IT security vulnerabilities.

Figure 11.
SMBs' concerns relating to IT security threats



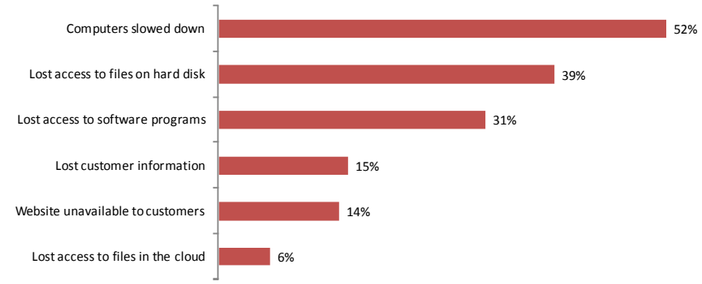
The true cost of IT security breaches to SMBs

05

While greatest security concerns were around losing access to files and replacing hardware, the reality of IT security breaches shows the true cost to SMBs

One-in-six SMBs has experienced an IT security breach. While this figure is marginally down against 2010, it still represents more than 1 million companies in the USA and UK who have suffered as the result of failing or insufficient IT security. More than half of those companies experiencing a breach claim to have suffered slowing down of computers, making it the most likely symptom. However, around a third of organisations claim to have lost access to either files or software programs following a security failure.

Figure 12.
Results of SMBs' IT security breaches

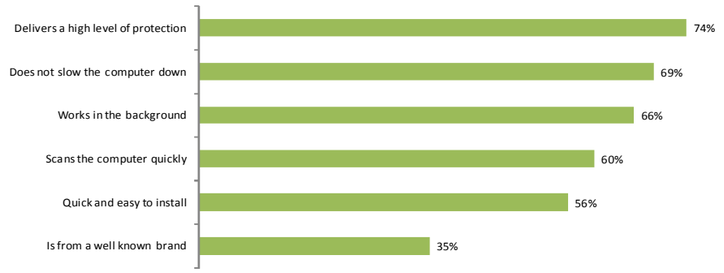


As a result of these security breaches, it is estimated that SMB market in the UK and USA:
- Lost 30million man-hours in labour rectifying the results of IT security breaches in the past year (22.1m hours in the USA, 7.9m hours in the UK). At an organisational level, this translates to more than three days' labour for each company who has experienced a breach.
- Lost out on $14.87m sales/revenue opportunities as a result of organisational IT security breaches. This breaks down as $11.30m in the USA and £2.19m in the UK.
- Spent $7.52million to replace damaged hardware (including corrupted computers etc.) as a result of IT security breaches. This breaks down as $5.60m in the USA and £1.18m in the UK

Peace of mind, performance and reassurance continue to be the top priorities for SMBs when considering IT security software

SMBs are remarkably consistent in terms of their requirements for security software. They want IT security software to:
- Deliver the right level of protection
- Not impact on business performance
- Work in the background

Figure 13.
SMB priorities for security software perofrmance (% essential/very important)



There is an expectation from almost all SMBs that a well known security software brand should be able to meet their requirements. Consequently brand reputation carries considerable weight when it comes to purchase decision making.

01 It would appear that renewed economic uncertainty in 2011 has led to a reduction in IT spend among SMBs. As a possible symptom of this, more SMBs are moving to manage IT in house rather than incurring the extra expense associated with outsourcing.

02 SMBs are embracing technologies to increase levels of mobility, best represented by the increase in tablet devices with a corresponding decline in laptop use, few are aware of the potential security risks that accompany this technology. Almost three quarters of SMBs do not agree that the use of mobile phones in business may represent a threat to IT security.

03 SMBs also recognise the opportunities which social networking offers their companies to promote their business and engage with customers. One-in-three SMBs has a social network page or profile on the three major social networks and are readily employing a social networking strategy.

04 While the majority of SMBs remain focused on the more traditional threats to IT security, such as email and web viruses, they are becoming aware of new ways in which their organisational security can be compromised, including theft of information and social engineering.

05 SMBs often only realise the true cost of IT security breaches after experiencing one. Those who have experienced a breach are more likely to have seen the longer-term impacts such as a loss of sales and revenue opportunities and the man hours lost from reacting to a breach.

06 SMBs desire a trusted IT security solutions brand. This needs to protect their business and run in the background and not slow business systems while preventing security breaches.

About

AVG

AVG is a global security software maker protecting 98 million active users in 170 countries from the ever-growing incidence of Web threats, viruses, spam, cyber-scams and hackers on the Internet. AVG has nearly two decades of experience in combating cybercrime and advanced laboratories for detecting, pre-empting and combating Web-borne threats from around the world. Its free, downloadable software allows novice users to have basic anti-virus protection and then easily upgrade to greater levels of safety and defense when they are ready. AVG has a strong reseller network consisting of resellers, partners and distributors globally including CNET, Ingram Micro, and Wal-Mart.

www.avg.com

GfK NOP

GfK NOP Ltd is part of the GfK Group and a leading market research agency in the UK and internationally. It is a renowned supplier of market information and insight, offering sector specialists and best-in-field research for qualitative, quantitative, ethnographic, omnibus and online research services.

Why choose AVG to protect your business: We are the champions of small business security

Our products are designed exclusively with the small and medium business in mind, ensuring they are high on protection, light on resources and easy to use

AVG has considerably higher levels of satisfaction amongst small businesses compared to other major brands

We're rated #1 for ease of use by Tolly*

We're rated 5* for value for money by SC Magazine

That's why 1 in 4 SMBs already trust AVG to protect their business**

Sources: *Tolly independent testing labs **AVG & GFK Small Business IT Security Survey August 2011

We Protect Us™

AVG is 98 million active users working together, sharing threat information to keep each other safe.

Together WE keep 240 new viruses off our PCs every minute

Together WE remove over 100 million threats every single day

Every six seconds someone new joins US

Every six seconds someone recommends US

Join our community today to learn how We Protect Us™