Achieving best practice in IT management for SMBs

Contacts:

Bob Tarzey
Quocirca Ltd.
+44 1753 855794
bob.tarzey@quocirca.com

As businesses grow they carry with them many practices established in their early days. Good practices stand them in good stead as they become larger businesses. This applies to all aspects of running a business, but especially to IT management. Good practice in IT management allows businesses to make effective use of IT while minimizing costs and reducing business risk.

- **SMBs make extensive use of IT from the day they are conceived**
  PC penetration is high. The overwhelming majority use internal networks and servers. All are now connected to the internet. Many are starting to use advanced storage options.
- **Their IT infrastructure is complicated by use of diverse operating systems**
  On the desktop Microsoft Windows is used by 93.5% of SMBs, but many have not upgraded to Windows XP and are using a mix of old and new to avoid the inconvenience and expense of upgrades. On their servers SMBs are also using a mix of old and new versions of Microsoft operating systems along side UNIX, Linux and other operating systems
- **SMBs are still managing most of their applications in house and there is no headlong rush for hosted solutions**
  Email is quite commonly outsourced and business applications increasingly so. But the majority have no stated plan to move to external management by a third party preferring to keep things in house.
- **There is an awareness of the threats to information systems and the data they contain**
  After the failure of internet connections the most common problems faced by SMBs are attack by viruses and malfunction of PCs. This makes the PC the most vulnerable part of the IT infrastructure and the problem is increasing as employees become more mobile. Despite this, PCs are not as well protected as servers.
- **SMBs need to keep their IT management under review and be responsive to new threats**
  Once good practice is in place it needs to be kept under review to make sure it remains effective and that new threats like spyware and phishing are protected against.
- **Patching of operating systems is not as effective as it should be**
  The belief that there is little benefit in paying for upgrades is understandable, but it should not preclude good patch management. Small SMBs need to take advantage of Microsoft's automated online patch management procedures. As businesses grow and their IT environments become more complex, central management of both servers and PCs becomes more important and in house automated software can be used to achieve the same goal.
- **The main reason that good practice is hard to achieve is due to lack of expertise and resources**
  Most small SMBs do not have an IT expert in-house. Even in large SMBs, where they often do it is not always their full time job. This means that to achieve good practice SMBs require easy to use automated tools.
- **Those responsible for IT in SMBs should be free to focus on the business, whether or not it is their full time job**
  Automating the drudge of backup, patch management and keeping security up to date frees the individual responsible for IT to focus on adding value to the business. This is not only a motivation for them, but increases the overall confidence the business has in IT and makes sure it is able to react more easily to rapidly changing business needs and regulatory requirements.

RESEARCH NOTE:

This report is based upon data collected from the interviews of 241 senior managers of SMBs (including managing directors, finance directors and IT managers) across the US.

The research was sponsored by **Computer Associates** and we thank them for their support.

We also thank all the participants who give their time and without whom such reports would not be possible.

Contents

Introduction 3
A note on terminology 3
SMBs and their use of IT 3
Exposure to risk 5
Achieving best practice 6
Appendix A – How good are your practices? 8
Appendix B - Interviewee Sample Distribution 9
About Computer Associates 10
About Quocirca 11

Introduction

A company's culture transcends its people. A simple practice like ordering pizzas on a Friday afternoon is likely to survive over a number of years, even if all the original people who first thought it would be a good incentive not to leave early at the end of the week have moved on.

As companies grow good and bad practice can become embedded in the way they operate. Of course, certain things have to change, a company that starts in the spare bedroom may, if successful end up working across multiple premises with many employees at each. But it will carry with it on that journey some of the practices from those early days.

This applies to all aspects of the way a company is run: the way it reports its accounts, the way it treats its employees, the way it markets itself and sells its products and the extent to which it makes good use of information technology (IT).

It is this last point that is the subject of this report. The report looks to at how small and mid-sized businesses (SMBs) use IT and how this evolves as they grow. It also examines the origins of bad practice in the use of IT and the threat this poses if it remains unchecked.

For SMB managers who read this report, it offers peer review and a check point for looking at their own IT practices. They will also be better armed as they enter in to discussions with IT suppliers.

The report is based on primary research in to SMB IT practices conducted by Quocirca in April 2005 (see box on front page for details). For the convenience of reporting the results SMBs are classed in to four categories:

- Soho (small office, home office) – 10 or less employees
- Small SMB – 11 to 49 employees
- Mid SMB – 50 to 300 employees
- Large SMB – 301 to 1000 employees

When the term SMB is used on its own it refers to the whole sample.

A note on terminology

Throughout the report the terms "business" and "SMB" are used and not the alternatives "enterprise" and "SME". One of the questions posed to the respondents was what terms they felt applied to themselves. Around 40% of large SMBs considered themselves to be enterprises, but hardly any of the smaller three groups did. All 4 groups were quite comfortable with terms like small businesses and mid-sized businesses.

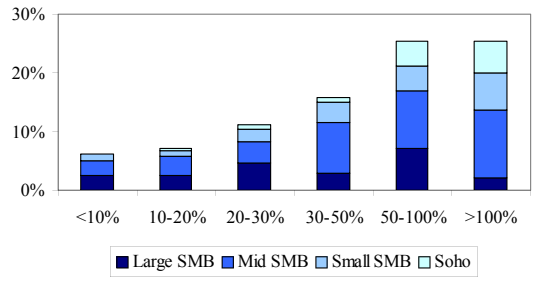
One exception was for the smallest of businesses who where offered the term "micro-business", but few thought this applied to them. So the report uses the term Soho for convenience, as it is widely used in the industry, although Quocirca is under no illusion that start-ups wander around referring to themselves as "Sohos".

SMBs and their use of IT

SMBs make extensive use of IT; this is true from day one. One of the best measures of this is PC penetration rates (fig 1). Over 50% of SMBs have 50% or more of their employees using PCs and there is little difference between the small and the big guys, although a lot of Soho businesses have more than one PC per employee, perhaps suggesting redundant kit and inefficient use of resources.

Figure 1

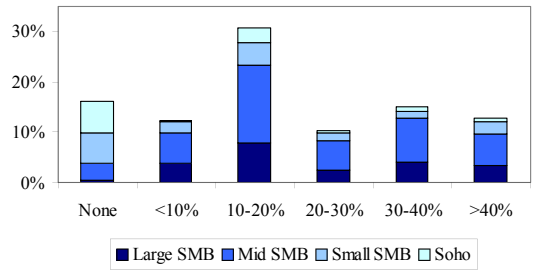
PC Penetration (% of overall sample)



All SMBs are now connected to the internet mainly by broadband (75%), but 9% still choose or have to rely on dial up. The remainder, mainly the larger ones, use ISDN or leased lines. SMB's employees are increasingly mobile, around 20% of employees having access to laptop PCs (fig 2).

Figure 2

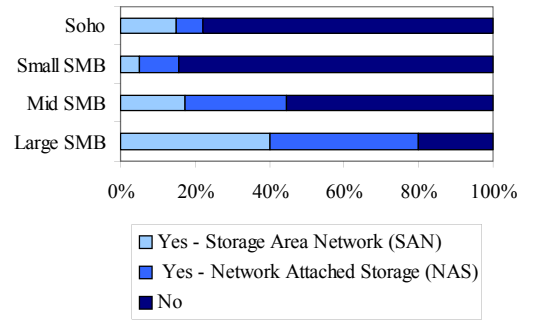
Laptop PC penetration (% of overall sample)



As businesses grow and, in many cases, spread to multiple locations, they start to embrace more complex technologies like internal networks and shared servers. Use of these technologies is high; 75% of Soho businesses had an internal network and 57% had shared servers; among larger SMBs there were few not using these technologies. Advanced network storage options are less widely used by small and Soho SMBs but commonly used by large SMBs (fig 3).

Figure 3

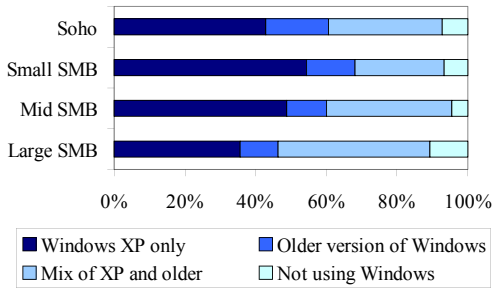
Do you have any additional disk storage that is shared by these servers or accessed directly by your desktop and laptop computers? (% of category)



Perhaps the greatest IT complexity that SMBs have to deal with is in the heterogeneous operating environments they end up with. This is not always through choice. Even on the desktop where 93.4% of respondents use Microsoft Windows, less than half of these had updated all their PCs to the latest version of Microsoft's operating system, Windows XP, which was released over 3 years ago (fig 4). 37% of them are using a mixture of XP and older versions.

Figure 4

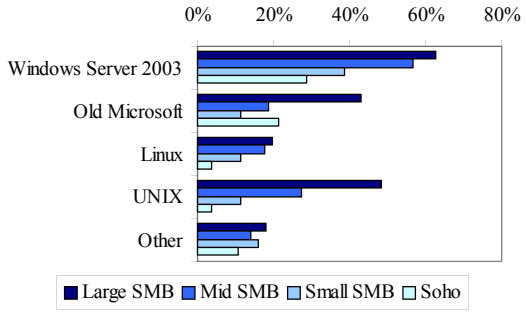
Microsoft Windows versions run on PCs (proportion of category)



When it comes to servers the situation is even more heterogeneous (fig 5). Again Microsoft's operating system dominates, with a similar mixture of old and new (Microsoft's latest server operating system, Windows Server 2003 was released, as the name suggests, 2 years ago). But the use of non-Microsoft operating systems, in particular UNIX and Linux, is far more popular for servers than for individual PCs.

Figure 5

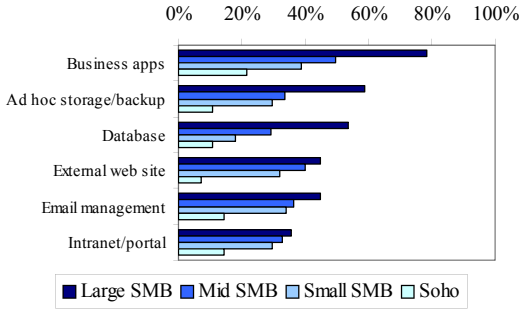
Operating systems run on servers (% of category using OS)



As businesses grow, they add servers to their internal network to support a variety of shared applications and provide common repositories for data and other information (fig 6).

Figure 6

What functions do you use the servers for? (% of category saying yes)



Almost any of these can be outsourced these days, but while the majority are still kept in house, the market is gradually changing in favour of the outsourcers. The number of SMBs outsourcing email management is heading for 50% and business applications are not far behind (figs 7 and 8).

Figure 7

Use of outsourced email management (% of category)

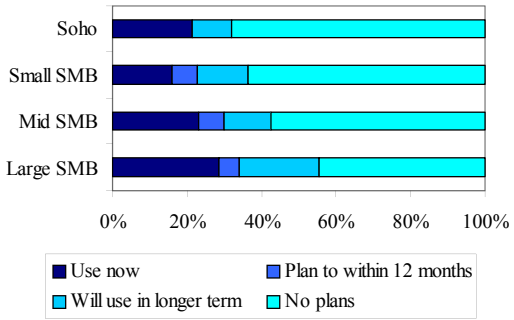
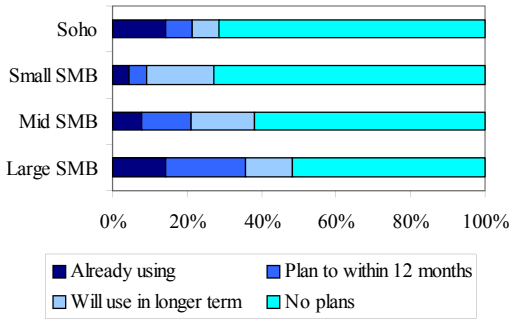


Figure 8

Use of hosted applications, e.g. customer relationship management/CRM (% of category)



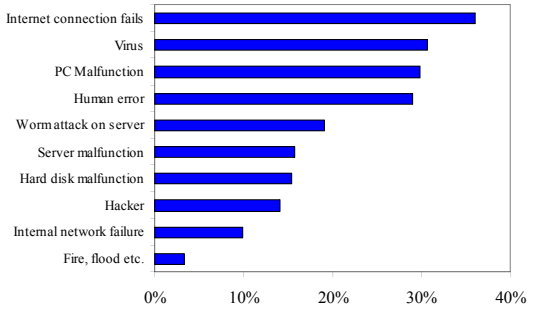
SMBs are advanced in their use of IT, it empowers their businesses. Their computers are largely connected internally and to the rest of the world via the internet. Their operating environments are heterogeneous; both in the software they use and the way applications are maintained and delivered. With their businesses reliant on IT, how exposed are they to IT failure that has the potential to bring their operations grinding to a halt and how easily can they recover from disaster?

Exposure to risk

The most common IT failure reported by SMBs was a failure of their internet connection (fig 9). When it is up and running it leaves them exposed to the second most reported cause of IT failure, computer viruses, most commonly carried by email.

Figure 9

Has your company's ability to function been affected by an IT failure of some sort? (% of overall sample saying yes)



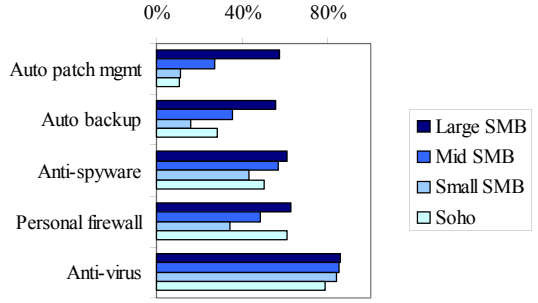
But almost as high is PC malfunction. The inability of an individual to function does not necessarily bring the business to its knees, but can be a serious cause of lost time, both for the individual concerned and the person who ends up fixing the problem. It is not only time that gets lost but also data. This is not just inconvenient, with increasing regulation of businesses of all sizes it is a risk that has to be avoided.

PC malfunction is most likely to be caused by a software failure, which may in turn, be caused by a virus. Viruses themselves most often target known vulnerabilities in out of date software. All these things can be protected against.

PC malfunction is one thing, complete loss is another. As employees are increasingly mobile the threat of theft is even higher. And, bearing in mind that the fourth most common cause of IT failure is human error, let's not forget that this includes employees simply losing mobile devices. PC malfunctions can often be fixed and data recovered; stolen or lost PCs are usually gone for ever, and the files and data on them have too, if they were not backed up to a server or other separate storage device .

Figure 10

What software does your company have installed as standard on your desktop and laptop computers? (% of category)



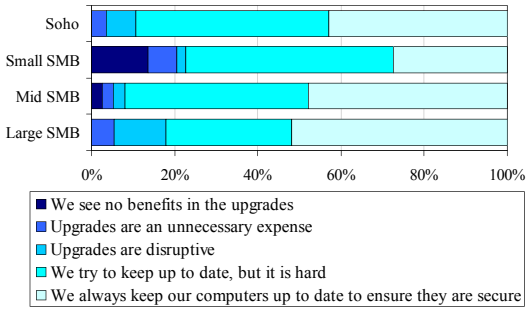
SMBs are not ignorant of all this, around 80% have anti-virus control as standard (fig 10). But as new threats emerge some are slow to react. Less than 50% have protected themselves from spyware, which is usually down loaded unnoticed while browsing the web. The threat of spyware is more insidious than viruses. A well written virus shows off by spreading as widely and quickly as possible, causing as much havoc as it can in a short space of time. Spyware however likes to remain invisible for as long as possible, stealing information and slowing down PCs in the process.

In an ideal world all computers would be up to date with the latest software, but many find this as a chore (fig 11). If Microsoft had its way all businesses would run the latest version of Windows on both their desktops and servers, but many of those SMBs who only use Microsoft's operating systems do not achieve this.

Installing, the latest versions of any operating system is not always practical. It is not just that upgrades are an expense in themselves, but the hardware they run on often needs to be upgraded too. This explains why so many PCs have not been upgraded to Windows XP; many SMBs have other things to spend their money on.

Figure 11

When considering software upgrades which of the following statements applies to your company? (proportion of category)



Patches to operating systems are, however, usually free. These are the small upgrades to software that fix known vulnerabilities that the writers of viruses, worms, trojans etc attack. While few Soho and small businesses have software in place to help with this it is likely that many are using Microsoft's automatic update facility available over the internet. This is a significant benefit for smaller businesses that tend to use other Microsoft software packages as well as its Windows operating system.

As businesses grow they tend to use more specialist and customized applications. These need to be tested against new patch levels before the patches are released and IT managers like to control the entire process centrally. However, 40% of large SMBs are not using automated software to do this (fig 10).

What ever the cause of IT failure, be it on the desktop or server, there should be no excuse for data loss because everyone backs up their computers – don't they? This is true of the majority who have formal routines for backing up their computers (figs 12 and 13).

Figure 12

Do you have a formal routine for backing up data on your server computers? (proportion of category)

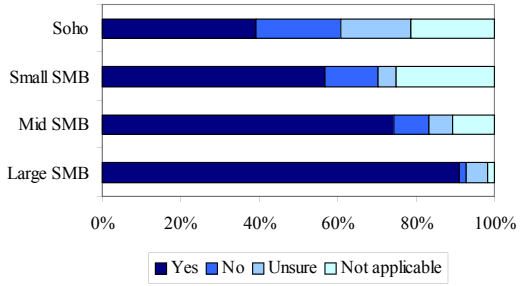
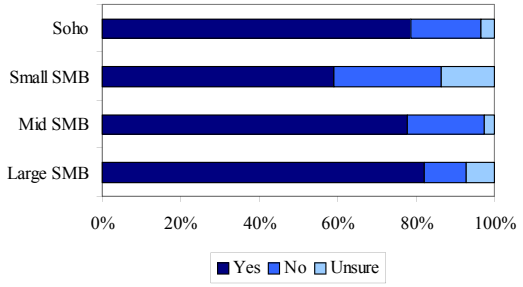


Figure 13

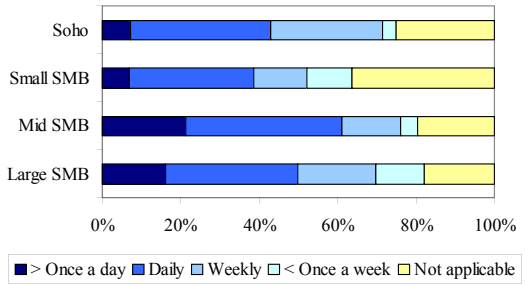
Do you have a formal routine for backing up data on your desktop and laptop computers? (proportion of category)



But, a worrying number do not and only 25% are using automated software to do so (fig 10). And, when it comes to PCs almost 50% are not doing this on a daily basis (fig 14) – go to work on Monday, have laptop stolen on Friday – a week's work completely lost.

Figure 14

If yes, how often do you back up your desk top and note book PCs? (proportion of category)



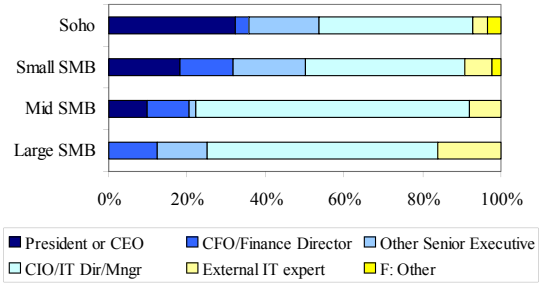
Achieving best practice

SMBs understand the causes and risks of IT failure and the consequences it has for their businesses. Superficially many seem to be doing the right things, but look behind the scenes and there are holes. The main reason for this is a lack of resources and time.

For around half of Soho and small businesses a non-expert manages IT. This falls to around 25% for mid and large SMBs (fig 15).

Figure 15

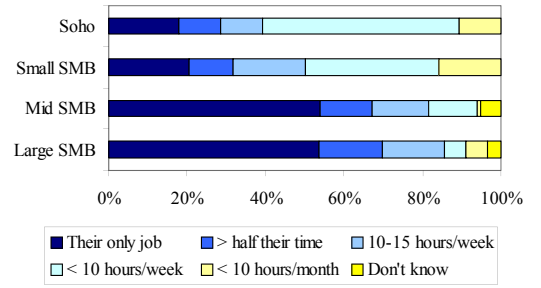
Who manages the computers and associated infrastructure in your company? (proportion of category)



But even for those with an expert they are not always doing it full time (fig 16).

Figure 16

How much of their time would you estimate is spent managing IT? (proportion of category)



Given SMB IT resource limitations, it is far more important to automate basic processes so as to free up time to work with other managers on strategic IT issues and increasing the value of IT to the business as a whole.

For those SMBs that grow to become larger businesses good IT practice will play a major part, especially as the business expands across multiple sites; far better to establish good practice when the business is still small, than to try and correct it when it has grown and inefficiencies have become embedded.

In addition to this the role of IT is becoming more critical, not just because businesses are reliant on it, but because business regulators expect data retention at levels which only well managed IT can deliver.

Best practice is not actually that hard. Despite the heterogeneous operating environments, diverse delivery of applications and the 100% on line use of IT, SMBs can protect themselves quite easily. Many already do and there are easy steps that can be taken for those with holes in their procedures to catch up. Certain IT vendors make it their business to provide the tools to do all this regardless of these

challenges. The hardware and software to do all this is, relatively speaking, cheaper than it has ever been.

Making sure that processes are standardised and automated and supplied by an expert ensures not just protection against today's threats but also those that will emerge in the future. A once off audit and renewal is good starting point, but regular update and review is also necessary.

Appendix 1 provides a checklist. For IT experts this is intended to serve as a reminder to seek any gaps in the way their IT infrastructure is protected. For the non-expert it acts as checklist when consulting advisors and suppliers.

If those who are responsible for IT in SMBs achieve all this and ensure that their use of IT is safe and secure, they will not just be making a major contribution their company's growth but they will avoid having regular IT crises, have peace of mind and, if it is part of their company's culture, enjoy their Friday afternoon pizza after another week of positive contribution to the businesses.

Appendix A – How good are your practices?

For IT experts this is intended to serve as a reminder to seek any gaps in the way your IT infrastructure is protected. For the non-expert it acts as checklist when consulting advisors and suppliers

- A large amount of any businesses' data, including documents, spreadsheets and email, end up stored on the local drives of employees' PCs. Make sure you have a regular routine in place for backing this data up to a central location. There are products that can fully automate this and will run on current and past versions of Microsoft Windows and other desktop operating systems
- This needs to include laptop PCs, either as soon as they re-attach to the internal network or remotely over the internet. Remote backups are not impractical, good backup software will just look for recent changes. Backing up to a local disk does not always protect against theft (unless the user is diligent in keeping storage disks and PC separate).
- The reason for doing this is because of the high failure rate of PCs. All too often this will not be due to a hardware failure but an operational failure caused by mal-ware or other misuse. Help minimise this by ensuring that all PCs are protected by anti-virus software. This needs to be kept up to date automatically, which requires an annual subscription. Most anti-virus products will run on current and past versions of Microsoft Windows and other desktop operating systems
- Many anti-virus vendors now also have an anti-spyware offering that checks PCs for software that has been inadvertently downloaded while browsing the web. Spyware is an invasion of privacy but more importantly it can degrade performance of already overworked PCs.
- Once PCs have been backed up to a central location, this data too needs to be backed up, along with any other data stored at that location. For many SMBs this will be a server set aside for ad-hoc storage and backup. If you have no need for a server, use a separate network attached storage device. Such devices can be purchased for little cost these days and have huge capacity.
- Ensure you also take copies of these central backups off site, for protection against fire etc.
- Server failure can also be caused by viruses and other mal-ware, so make sure they are also protected by anti-virus software. Most anti-virus products run on the different operating systems used by SMBs.
- When considering new applications, consider hosted solutions as an alternative to running them in house. A third party will have the expertise to provide secure communications across the internet and will take care of the backup of data under their management.
- If you already outsource email management, check your supplier's ability to filter spam, viruses and phishing emails (those pretending to be from banks etc.). If you manage email in house ensure you have this capability.
- Wherever your internet connection enters the organisation make sure it is protected by a firewall that includes intrusion prevention software. Intrusions such as worms target operating systems and common applications like databases.
- Upgrades are disruptive and for many it is too impractical and expensive to install each and every one. But patches, which fix known problems, serve an important role. Installing patches is not half as disruptive as a major IT failure. Virus writers and worm writers usually target software vulnerabilities once they have been identified by the vendor. The highest risk period is between the vendor announcing the problem and the patch being installed. Patches are provided for free (unlike many upgrades) and their installation can often be automated.

Computer Associates®

quocirca

Appendix B - Interviewee Sample Distribution

The primary research data presented in this report is from 241 interviews with SMBs across the USA. The profile of the business sizes of the interviewees is shown in figure 17 and their geographic spread in figure 18.

Figure 17

Breakdown of respondents by category (number of respondents)

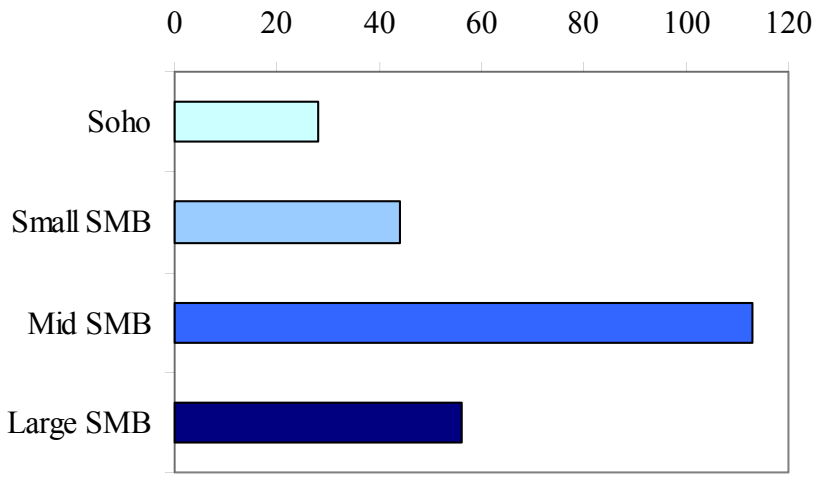
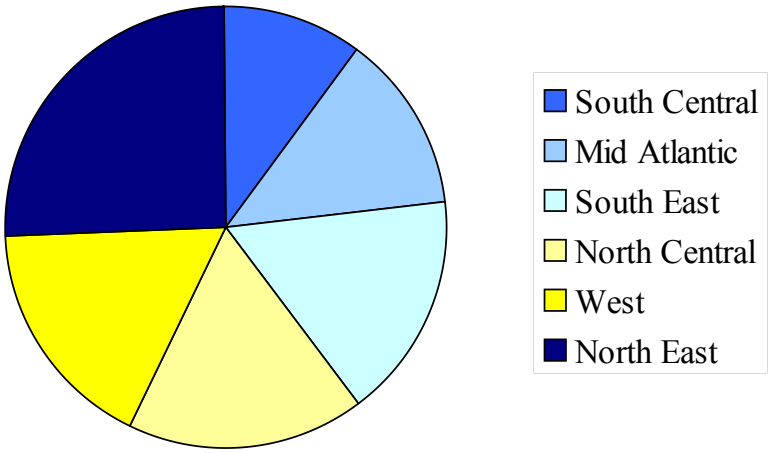


Figure 18

Breakdown of respondents by US region (number of respondents)



About Computer Associates

Computer Associates International, Inc. (NYSE:CA), the world's largest management software company, delivers software and services across operations, security, storage and life cycle and service management to optimize the performance, reliability and efficiency of enterprise IT environments. Founded in 1976, CA is headquartered in Islandia, N.Y., and operates in more than 100 countries. For more information, please visit http://ca.com.

About Quocirca

Quocirca is a perceptional research and analysis company with a focus on the global markets for information technology and communications (ITC). Its analyst team is made up of real-world practitioners with first hand experience of ITC delivery who continuously research and track the industry in the following key areas:

- Business Process Evolution and Enablement
- Enterprise Applications and Integration
- Communications, Collaboration and Mobility
- Infrastructure and IT Systems Management
- Utility Computing and Delivery of IT as a Service
- IT Delivery Channels and Practices
- IT Investment Activity, Behaviour and Planning

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help its customers improve their success rate.

Quocirca has a pro-active perceptional research programme, regularly polling users, purchasers and resellers of ITC products and services on the issues of the day. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, CA, Dell, Vodafone, Orange, EMC and Cisco. Sponsorship of specific studies by such organisations allows much of Quocirca's research to be placed into the public domain. Quocirca's independent culture and the real-world experience of Quocirca's analysts, however, ensures that our research and analysis is always objective, accurate, actionable and challenging.

Many Quocirca reports are freely available and may be requested via registration at www.quocirca.com. To sign up to receive new reports as and when they are published, please register at www.quocirca.com/report_signup.htm.

Contact:

Quocirca Ltd
Mountbatten House
Fairacres
Windsor
Berkshire
SL4 4LE
United Kingdom

Tel +44 1753 754 838
Email info@quocirca.com

quocirca