

Contacts:

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

Protecting the IT and data assets of small and mid-sized businesses

Small and mid-sized businesses (SMBs) are as reliant on IT as large enterprises, but have to manage their IT infrastructure with fewer people, who will often lack specialist skills. They need products that are easy to implement and manage but they can not be expected to invest time and money in extensive maintenance. SMBs' systems and processes will soon become outdated unless there is a high degree of automation.

This report looks at the state of health of the use of IT by SMBs and considers how they can better protect their IT and data assets. SMB managers who read this report should be better armed to engage in discussions with their IT suppliers.

- **SMBs are as reliant on IT as enterprises and their use of IT is sophisticated**

PC penetration is high. 70% of small businesses and 90% of mid-sized businesses are using servers and internal networks and only 3.5% are still not connected to the internet. Around 40% of mid-sized businesses are using advanced storage options.

- **But they have limited resources to deploy and manage their IT infrastructure**

This leads to shortfalls in the way they protect their IT and data assets. One in three mid-sized businesses does not have an IT manager and the same is true of 90% of small businesses. Even when an IT manager is in place, it is often only part time.

- **This lack of resources means once systems are in place they do not receive regular scrutiny**

50% of SMBs have not reviewed the security of their internet connection or checked their ability to recover from backup in the last 12 months. On desktop and laptop PCs, deployment of security software is inconsistent and backup procedures are patchy. They are more diligent about backing up servers.

- **Because of this PCs are a high risk area for SMBs**

The most common IT malfunction experienced by SMBs is failure of PCs and the most common security threat they face is from viruses, most likely to arrive at an unprotected PC by email. Whilst Microsoft Windows is used across the board, it tends to be older releases and updating to the latest version is not practical for many.

- **SMBs are aware of the value of their data and the need to be able to retrieve it for future reference**

90% have had to retrieve historic data at some point to satisfy auditors or some other regulatory requirement and 75% admitted to having had a problem recovering the required data on some occasions.

- **If SMBs' IT systems are not protected, system failure is likely to be painful**

Whatever causes system failure, be it a security problem or some other malfunction or disaster, a poorly protected IT infrastructure is going to be harder to recover and in some cases recovery may not be possible. Either way it will be costly for the SMB, both through loss of productivity and data assets.

- **Mitigating the threats is not hard and the right products need little management once in place**

There are a number of steps SMBs can take to mitigate these threats including the outsourcing of certain point solutions, automating desktop backup and installing security products that maintain themselves. This can all be done without needing to change the underlying infrastructure that has already been invested in – see the check list at the end of this report.

RESEARCH NOTE:

This report is based upon data collected from the interviews of 200 senior managers of SMBs (including managing directors, finance directors and IT managers) from a number of European countries. Other sources of data are highlighted where they are used.

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

Contents

Introduction	3
A note on terminology	3
SMB resources and risk	3
The SMB technology-scape	5
Mitigating risk	6
Appendix A – How well protected are your IT data and assets?	7
Appendix B - Interviewee Sample Distribution	8
About Computer Associates.....	9
About Quocirca	10

Introduction

If you manage a small or medium sized business (SMB) the headlong rush the information technology (IT) industry has been making to persuade you to spend more on their products may have passed you by. If it has, this is probably due to the fact that despite their best efforts, technology vendors find it hard to engage with small businesses and, even when they do, misunderstand their requirements.

This is not a co-ordinated effort by vendors; most have turned to SMBs individually as a response to revenue from the enterprise sector drying up in the early years of this decade. Of course, many vendors have always served small businesses well, but many others now fancy their chances of doing so in the future.

Either way, vendors have to overcome the challenge of communicating their message to SMBs without creating unnecessary concern.

This report highlights the issues managers of SMBs should consider when reviewing their use of IT and offers them a health check relative to their peers. It also aims to help SMB buyers see through some of the fear, uncertainty and doubt that vendors and their agents are prone to create and identify the threats that need to be mitigated and those that do not.

SMB managers who read this report should be better armed to engage in discussions with their IT suppliers.

We are not going to spend any time in this report defining what an SMB is; there are plenty of definitions and they all vary. The report makes use of findings from interviews with 200 SMB managers from a range of EU countries and industries. All these businesses had 300 employees or less – i.e. they were from the lower end of the SMB sector.

One finding was that the size of a business has a far greater impact on the way it uses IT than its geographic location. The recommendations in this report therefore apply to any SMB of a relevant size in any developed country.

In order to highlight the importance of business size, when referring to the opinions of the respondents to the interviews, we have divided them into two groups:

- Small businesses with less than 50 employees which constituted 40% of the sample
- Mid-sized business with between 50 and 300 employees constituted 60% of the sample

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

A note on terminology

We have used the terms “business” and “SMB” throughout this report to stay on the same wavelength as the target audience. When we asked respondents what terms they felt applied to themselves, less than 5% considered “enterprise” to be relevant.

SMB resources and risk

Strapped for resources and cash poor is the stereotypical image of the SMB. Looking at the state of some enterprises, this seems a little unfair. SMBs’ spending power and human resources will vary widely. But whatever their IT requirements, SMBs do not have large dedicated teams of IT experts to implement and manage the technology required.

Whilst about 65% of mid-sized businesses do have a dedicated IT manager, for half of them it is not their full time job. For small businesses the number with a dedicated IT manager falls to just 10% and it is rarely their dedicated task (figures 1 and 2).

Figure 1
Who manages the computers and associated infrastructure in your company?

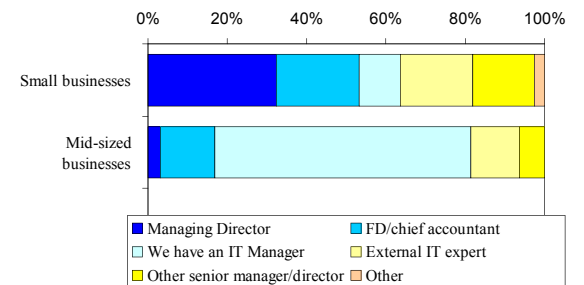
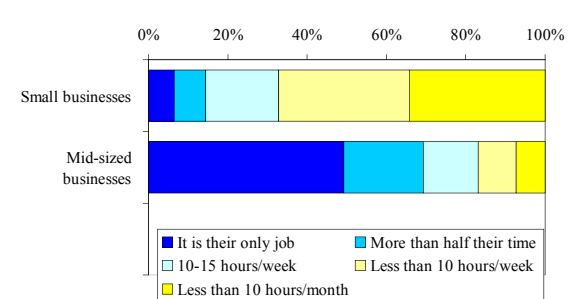


Figure 2
How much of their time would you estimate is spent managing IT?



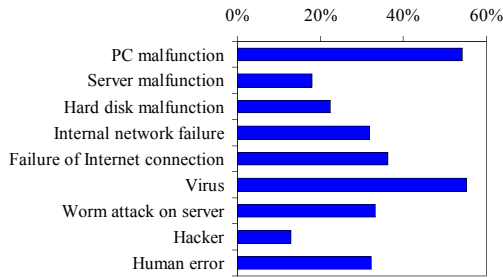
The message is obvious – IT needs to be simple to implement and manage and once the infrastructure is in place it will not receive regular scrutiny so management processes need to be as automated as possible.

This is fact not supposition – here are some examples. In our survey, in the last year over 50% of SMBs had not checked their ability to recover from a backup and over 50% had not reviewed the security of their internet connection to the outside world (10% admitted to it not being secured at all).

With limited resources this lack of review is not surprising. It is easy to offer advice of the type “make sure you review your IT security and recovery procedures on a regular basis”. But, with the best will in the world, it will not happen. Because of this many SMBs will be over exposed to threats of IT failure (figure 3) and the consequent costs of prolonged recovery and potential data loss.

Figure 3

How often has your company's ability to function been affected by an IT failure of some sort? (tick all that apply)



When we look at the causes of some of these problems, it is clear that there is some outright bad practice. A small percentage admitted to not regularly backing up their servers and the message to them is plain – “get your act together”. But blatant bad practice was rare and for the majority of SMBs, things do not happen because they are just too hard to do.

Backup up is a good example of this. Whilst most SMBs were diligently backing up their servers (figure 4), only 45% say that they are doing so for their personal computers and less than 10% were doing so on a daily basis (figures 5 and 6).

Figure 4

Do you have a formal routine for backing up data on your server computers?

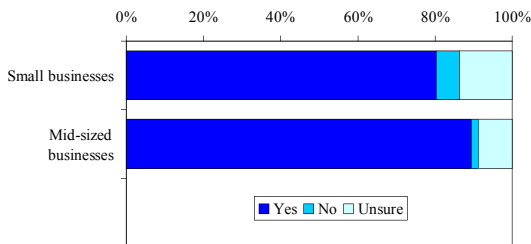


Figure 5

Do you have formal routine for backing up data on your desktop and laptop computers?

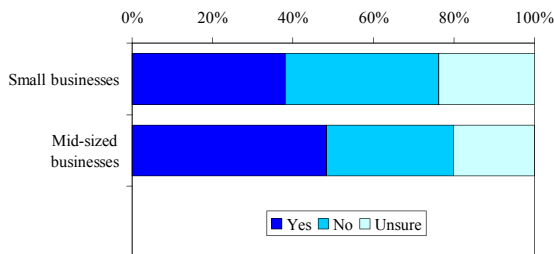
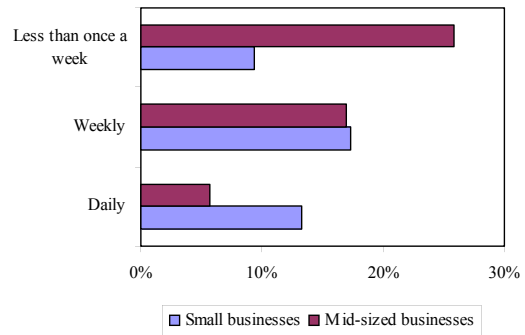


Figure 6

If yes, how often do you backup your desktop and notebook PCs?

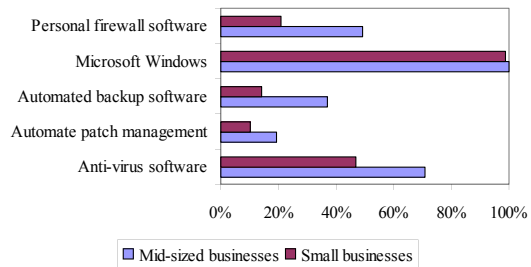


This means that a large amount of their data is at risk – 60% admitted that their ability to function had been affected by the failure of a PC at some time; this was far greater than server failure which stood at around 20%.

One reason for PC failure is poor protection from viruses. 29% of mid-sized businesses and 53% of small businesses did not have standard policies around the use of anti-virus software on their PCs (figure 7).

Figure 7

What software is installed as standard on your desktop and laptop computers?



SMBs do understand the value of their data and the need for making it available to external agencies. 65% have had to retrieve data for auditors at some point, almost 50% have had to do so to satisfy national regulations and over 30% to satisfy the EU. In all, 90% remembered having to retrieve something at some time. 25% claimed they had never had a problem finding such data, the rest had. In fairness for many this was a rare occasion, but it is these rare occurrences that catch the best of us out. The growing emphasis on corporate governance and disclosure in general is likely to increase such demands over time.

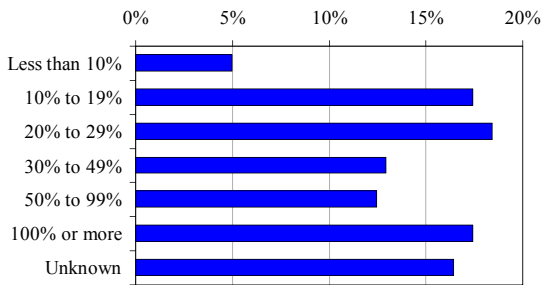
There is more to this than the worry about being able to retrieve data. The failure of part or the whole of any company's IT infrastructure can bring a business to its knees whilst as full a recovery as possible takes place. The longer this recovery takes the more money the business will lose. The chances of system failure can be reduced through good security and the chances of data loss reduced to a minimum by regular backup of both servers and PCs.

But if such good practice is hard for SMBs due to lack of resources and/or experience, what can be done to help? To answer this question needs an understanding of the SMB's IT environment.

The SMB technology-scape

SMBs are not technophobes. PC penetration rates (number of PCs per employee) are similar to those of enterprises (figure 8).

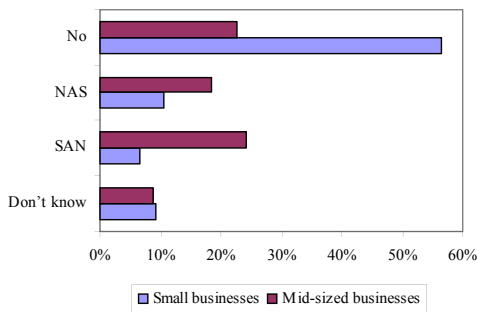
Figure 8
PC penetration (what % of your employees use a PC?)



Over 90% of mid-sized businesses and 70% of small businesses have an internal network. Similar numbers have servers attached to these networks and around half have had multiple servers. Only 3.5% said they were not connected to the internet at all.

40% of mid-sized businesses are using advanced storage capabilities like network attached storage (NAS) or storage area networks (SAN) (figure 9).

Figure 9
Do you have any additional disk storage that is shared by these servers or accessed directly by your desktop and laptop computers?



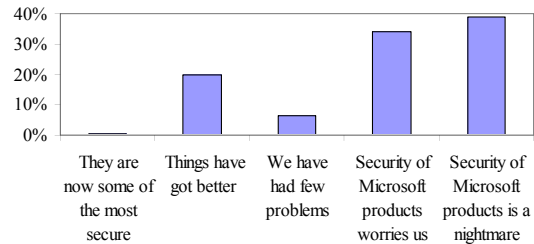
This was less amongst small businesses, the majority of which had no additional storage capability other than that on their servers (if they had one).

So why, with fairly advanced use of technology, are risks being taken with security and poor protection of certain data assets? One obvious answer is that technology, namely the internet, has introduced risk that did not exist a decade ago. But there are two other major reasons – cost and complexity.

Technology vendors have taken huge strides in helping businesses manage this risk. For example Microsoft's latest operating system (Windows XP with Service Pack 2) has greatly enhanced security features. This is true of all Microsoft products as it drives out its trustworthy computing initiative.

The problem is that the majority of businesses are not using the latest versions of Microsoft products. This is reflected in the perceptions around the security of Microsoft products articulated by respondents to a recent online survey conducted by Quocirca (figure 10).

Figure 10
Microsoft has been talking a lot in 2004 about security and what they call "trustworthy computing": How would you rate Microsoft in this area?

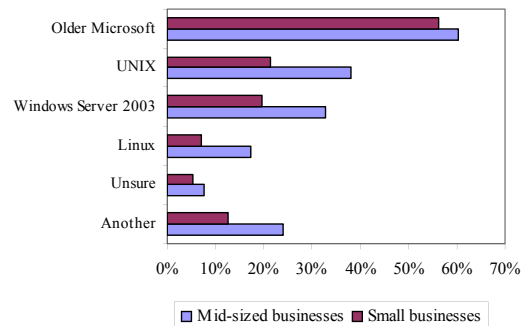


Data from separate online Quocirca survey, based on the responses of 5,772 users of IT

But simply telling businesses to upgrade is not realistic. It is not just the cost of the software, newer products require more resources and to run the latest versions often requires new or upgraded hardware. The total cost puts many businesses off making upgrades as the visible benefits to the business are limited.

The widespread use of older Microsoft software is evident when we look at the operating systems used on servers. Of those using Microsoft operating systems on their servers, only one third were using the latest product – Windows Server 2003 (figure 11).

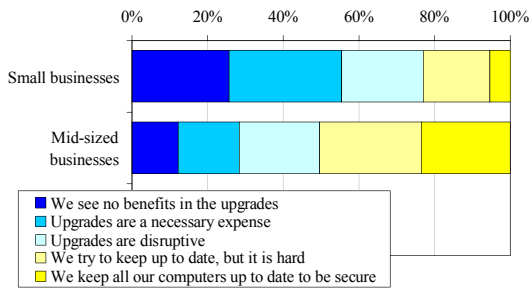
Figure 11
What operating systems do your servers run? (tick each that apply)



It is not just cost that puts SMBs off upgrading, upgrades are problematic for other reasons. They are disruptive and core applications may not run on the most recent operating system version and even if they do, upgrading the applications themselves is a further expense, which may be seen as of limited value to the business (figure 12).

Figure 12

When you consider upgrading software on your computers which of the following statements applies to your company?



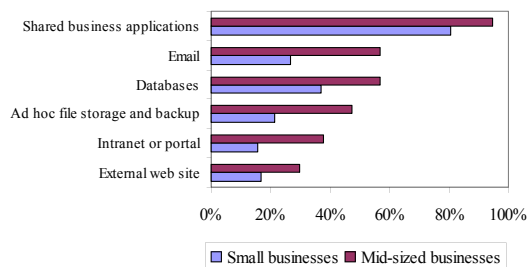
Anyway, when it comes to servers many choose to use non-Microsoft products. UNIX is more widely used than Windows Server 2003 and Linux is used by about 18% of small businesses. The figures suggest that as SMBs replace old servers they are choosing Windows over Linux by a factor of two. Interestingly, because about 50% of SMBs have only one server, for those that select Linux it is likely to be more strategic, unlike in larger enterprises where Linux is often used tactically.

Whether SMBs are selecting Linux for cost reasons or not is a moot point, but either way, it leads to complexity. 35% of respondents were using multiple operating systems. This included various mixes of Windows, UNIX and Linux, as well as other unspecified operating systems (likely to have included IBM's OS400).

One reason for this is that it will often be the selection of an application that drives choice rather than the operating system. If a core application is only available on a certain operating system then it will be added to the IT infrastructure's increasing complexity. 90% of SMBs who had a server were using it to run such applications (figure 13).

Figure 13

What functions do you use the servers for?

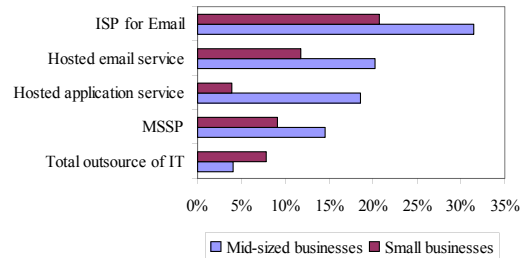


A small percentage of the total said they were also using a hosted application service, i.e. they were entrusting someone outside of their company to run an application for them and accessing it over the internet. Outsourcing certain point solutions is not a bad idea for many SMBs, especially those who lack in-house skills.

Providing transactions against hosted applications are conducted over a secure connection, the hosted service provider is likely to have a far better managed infrastructure than most SMBs. Indeed for one particular application – email – outsourcing is now as common for SMBs as keeping it in house (figure 14).

Figure 14

Do you use any of the following outsourced services?



Mitigating risk

Perhaps the easiest way to mitigate risk is to pass the problem to someone else, which is why hosted services are becoming more popular with SMBs. For example, a major benefit of outsourcing email management is that a good third party should deliver a clean stream of email, free of viruses, spam, phishing-emails etc. Whilst they cannot guarantee 100% protection from such threats, it is a good starting point.

But threats come to businesses in other ways. Nearly 40% reported that their servers had been the target of worm attacks and 20% of mid-sized businesses reported uninvited human intruders. Spyware is the big new evil and can arrive uninvited, initiated by surfing the web. Other risks will emerge in the future.

Good IT security can prevent many of these threats having an impact. But security failures will occur as risks evolve and this, along with plain old hardware failure, human error and other disasters, will lead to occasional system failure and the associated potential for loss of data and productivity is inevitable.

Protection against all this has to be initiated in house. Providers of hosted services can only secure the data they are responsible for. It is possible to contract managed security service providers (MSSPs) to help manage much of this but this is, in effect, buying in expertise and resources.

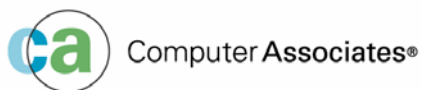
For a quick review and health check turn the page and run through our checklist to ensure you have covered all the bases. For IT experts this is intended to serve as a reminder, for the non-expert it acts as a discussion document when consulting suppliers, resellers etc.

For SMBs, protection of their IT infrastructure and data assets is not hard and need not be that expensive. To not do so is likely to be very inconvenient and costly.

Appendix A – How well protected are your IT data and assets?

This check list serves as a reminder for those experienced in the management of IT and as a discussion document for the less experienced that are running an IT health check with a third party

- 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.
- This needs to include laptop PCs, either as soon as they re-attach to the network or remotely over the internet. Remote backups are not impractical, good backup software will just look for recent changes.
- 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.
- Many anti-virus vendors now also have an anti-spyware offering that checks PCs for software that has been inadvertently downloaded whilst 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 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 control.
- 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.

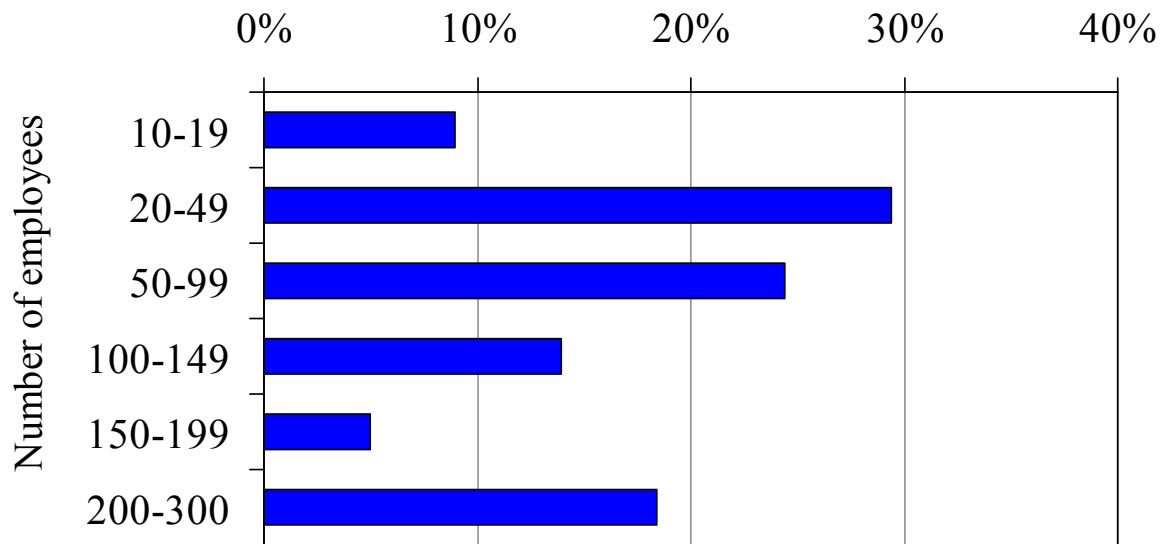


Appendix B - Interviewee Sample Distribution

The primary research data presented in this report is from 200 interviews with SMBs across Europe, apart from the data in figure 10 which is taken from a Quocirca survey involving 5,772 end users of IT. The profile of the business sizes of the interviewees is shown in figure 15.

Figure 15

How many people work at your company?



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 research and analysis company with a focus on the European market 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 primary 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 Morgan Stanley, Oracle, Microsoft, IBM, CA 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

The logo for Quocirca, featuring the word "quocirca" in a lowercase, sans-serif font. The letters "qu" are blue, "o" is red, "c" is blue, "i" is red, "r" is blue, "c" is red, and "a" is blue.