"Highest Performance
Lowest Price"

Microsoft
GOLD CERTIFIED
Partner

GFI WHITE PAPER

THE GFI SOFTWARE SME SECURITY REPORT

March 2009

Contents

Executive Summary

As the economy slides deeper into recession, IT budgets are holding up well, with analysts Forrester predicting IT spend will increase by 2.5% in 2009. But just how effectively will those budgets be spent? How well do organizations of every size understand the best areas to prioritise spend to mitigate against the effects of a challenging marketplace?

With the near ubiquitous reliance on IT across every organization, it is essential to get this investment right – but are the UK's SMEs as well-placed to maximise IT as their blue chip counterparts? Or are they clinging to outdated strategies that are no longer appropriate in the current climate?

Certainly this research undertaken on behalf of GFI reveals a disturbing lack of insight into the changing – and escalating – nature of the security threat created by the recession.

The survey revealed that some 46% of SMEs are experiencing declining sales and a further 37% report flat growth. As a result, 44% of SMEs plan to cut their IT budgets in 2009, and only 19% plan any increase.

Yet these organizations will continue to focus their IT investment on infrastructure – laptops, PCs, servers – in sharp contrast with the overall market trends. In contrast, IT security was identified as a priority area for less than a quarter (23%) of SMEs – the 6th highest priority.

And while 31% would ring-fence their IT security budget even if forced to cut IT budgets overall, 37% see security as an area of minimal investment or one that could be cut if necessary.

Indeed, despite the higher rates of redundancies and staff dissatisfaction that has been proven to increase employee-led information theft, IT decision-makers of UK SMEs continue to drastically underestimate the security levels required to protect sensitive corporate data.

Indeed, over three quarters (78%) think external IT security threats are more concerning than internal ones. As a result, these organizations are most concerned about threats from virus attacks (88%), accidental data corruption (87%) and spam (77%).

In contrast, only 50% are concerned about threats from data theft by employees, 55% concerned about viruses being introduced via USB sticks and 59% concerned about staff losing USB sticks holding sensitive data.

A majority (72%) do, however, feel that in a prolonged recession the threat level is likely to increase or at least alter the character of the threats faced.

This lack of insight into the emerging internal threat has left these organizations woefully lacking in key areas of security. While nearly 100% use basic IT security measures such as anti-virus software and user password protection, most are more vulnerable in terms of portable storage device network access management (just 45%), network event logger (55%) and web filtering (61%).

Attitudes to securing and monitoring sensitive information are also inadequate, with only 41% of SMEs actively seeking to identify what sensitive data they are potentially holding. And while almost two thirds (64%) screen laptops for viruses before allowing them to link to the network, only 47% can track what information or software is being uploaded or downloaded.

Far worse is the attitude to the plethora of mobile devices now commonly used, from USB sticks to CDs and iPods. Only 45% screen USB sticks for viruses before allowing network access and only 28% are able to track what has been uploaded or downloaded. Only 40% screen CDs/DVDs for viruses before allowing network access and only 19% are able to track what has been uploaded or downloaded.

On top of this lack of relevant technology, the majority of SMEs are failing to protect themselves by drawing up written IT security policies that are signed by employees. An extraordinary 60% of organizations have either no policy at all to regulate access to the network by portable devices or only informal guidelines.

The result is that employees are free to edit, copy, delete or distribute sensitive data unseen by the organization.

This survey reveals a disturbing lack of insight into current IT needs amongst UK SMEs. Continuing to spend heavily on hardware and failing to recognise the growing threat of internal information theft posed by increasingly nervous and disgruntled employees – however loyal they may have been in the past – is adding significant, yet unnecessary, business risk.

The Results at a Glance

Recession bites…

□ 46% of SMEs are experiencing declining sales and a further 37% report flat growth

□ 44% of SMEs plan to cut their IT budgets in 2009 vs. only 19% who plan to increase

□ IT security was identified as a priority area for investment by 23% – which means it is the 6th highest priority

□ 31% would ring-fence their IT security budget even if forced to cut IT budgets overall. But 37% see IT security as an area for minimal investment or which can be easily cut if need be.

IT Security Priorities…

□ SMEs are most concerned about threats from…
> Virus attacks (88% are concerned about this)
> Accidental data corruption (87%)
> Spam (77%)

□ SMEs are least concerned about threats from…
> Data theft by employees (only 50% think this is a risk)
> Viruses being introduced via USBs (55%)
> Staff losing USBs with sensitive data on them (59%)

□ Most people (78%) think external IT security threats are more concerning than internal ones

□ 72% do feel, however, that a prolonged recession is likely to either increase or at least alter the character of the IT security threats they face.

IT Security Measures taken…

□ Nearly 100% use basic IT security measures such as anti-virus software and user password protection

□ But SMEs are more vulnerable in terms of:
> Portable storage device network access management (just 45%)
> Network event logger (55%)
> Web filtering (61%)

□ SMEs usually fail to protect themselves by drawing up written IT security policies that their staff are required to sign. Only 25% have policies that regulate their networks by portable devices.

□ Only 41% of SMEs actively seek to identify what sensitive data they are potentially holding**.**

Portable devices – the weak link in IT security…

□ 64% screen laptops for viruses before allowing them to link to the network and 47% are able to track what laptops are uploading/downloading

□ Only 45% screen USBs for viruses before allowing network access and only 28% are able to track what has been uploaded/downloaded from them

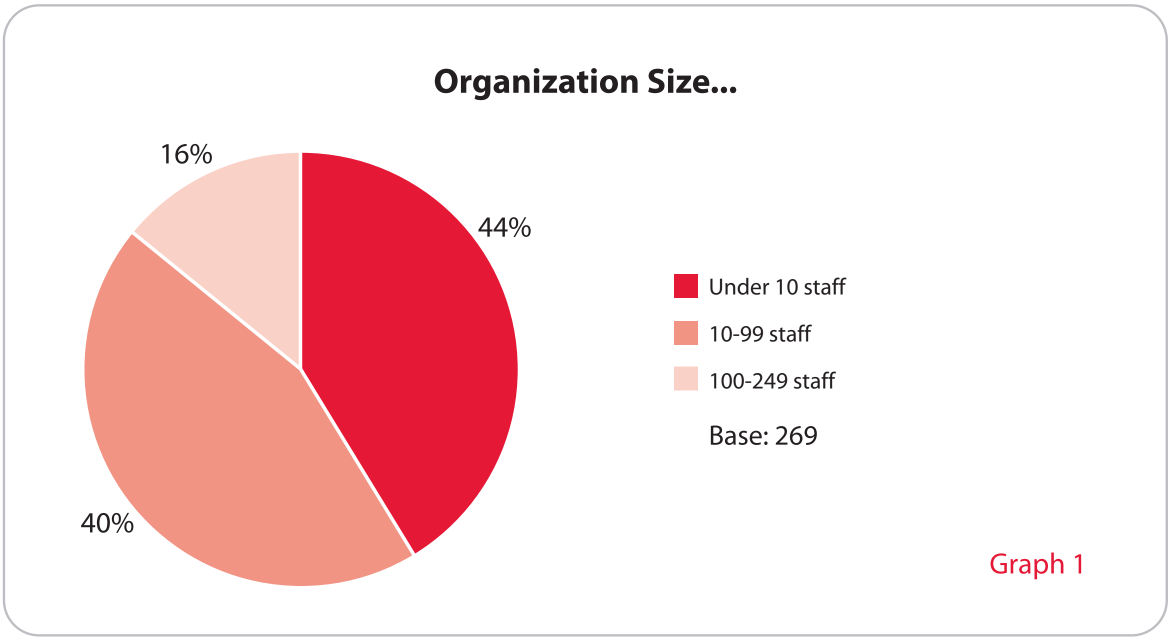
□ Only 40% screen CDs/DVDs for viruses before allowing network access and only 19% are able to track what has been uploaded/downloaded from them

□ Only 35% screen PDAs for viruses before allowing network access and only 18% are able to track what has been uploaded/downloaded from them.

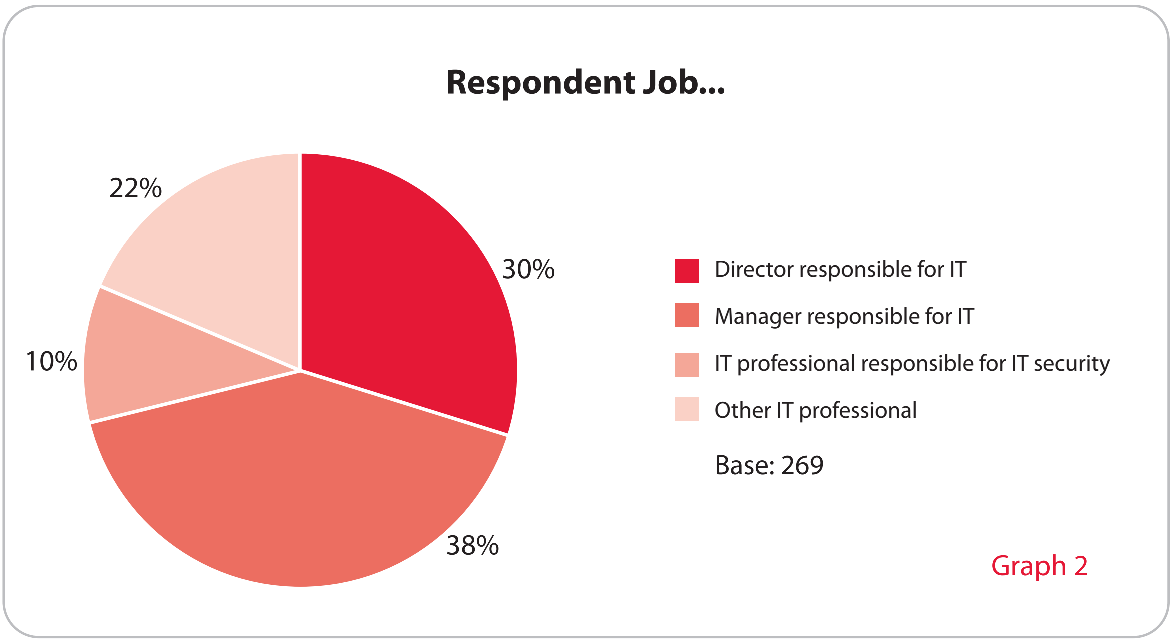
The Research

Organizations are struggling to juggle expenditure during the recession and it has never been more important to prioritise spend based on real business needs. But in a fast-changing business climate, just how aware are the UK's SMEs of the implications of redundancy and declining morale on the IT security of the business? And just what technologies and processes are they putting in place to safeguard critical business data – from customer information to staff HR records?

To assess the 'readiness' of the SME market, during February 2009, Redshift Research undertook 269 interviews with IT Directors, managers and security professionals on behalf of GFI. The survey focused exclusively on organizations with fewer than 250 employees, with 45% having less than 10 employees, 40% between 10 and 99 and 16% having between 100 and 249 staff (Graph 1).



Graph 1

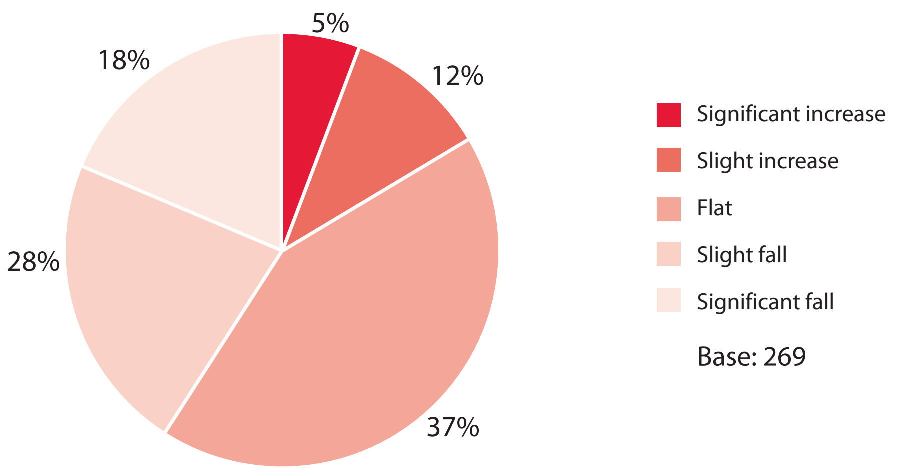


Graph 2

The companies surveyed spanned the full gamut of vertical markets, from general business services (23%), through retail (13%) and property & construction (12%) to media & leisure (4%).

These organizations are certainly feeling the effects of the recession. Almost a half (46%) are experiencing declining sales, while 37% report declining growth. And, as a result, it is not surprising that 44% of SMEs plan to cut IT budgets in 2009, while only 19% plan any increase (Graph 4).

Q4 What trend have you seen over the past six months in company sales/new business...



Base: 269

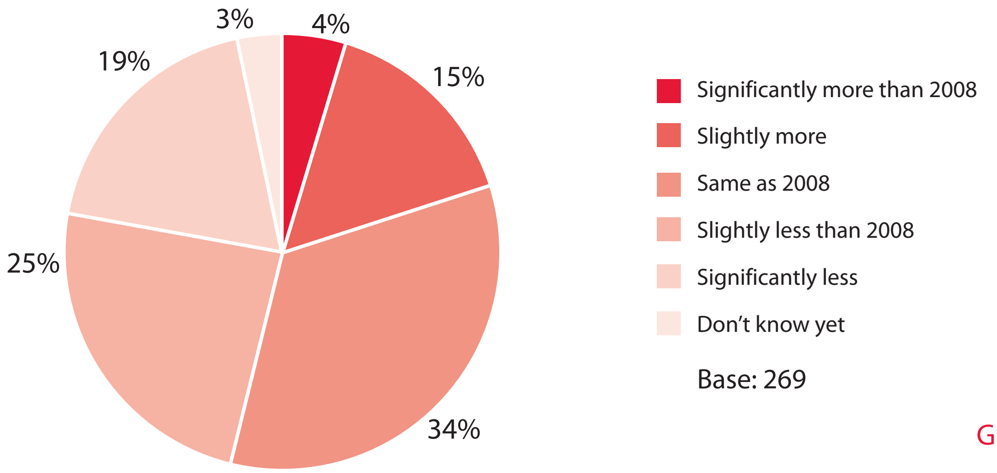
Graph 3

However, given this trend towards budget reduction, the areas of planned spend are somewhat surprising. Some 42% of companies cite new laptops as an area of major IT investment in 2009. This infrastructure-based trend is supported by new desktop PCs (39%), new office peripherals (29%), new servers/server upgrades (26%) and new office software (24%).

It is hard to see how investment in expensive hardware can deliver any quantifiable competitive advantage during a recession – and indeed this trend goes against expectation of pundits such as Gartner who predict a massive decline in sales of PCs. Gartner is projecting that worldwide PC shipments will decline by 11.9 per cent in 2009 - what the company has characterised as the "sharpest unit decline in history," while global semi-conductor revenue is set to fall by 24% this year.

In contrast, only 23% of these UK SMEs plan to prioritise security spend in 2009. Furthermore, when asked if a period of prolonged recession was to lead to a situation where IT budgets needed to be cut during the course of 2009, how likely would it be that the company would look to cut spending on IT rather than other areas, over a quarter (26%) responded that spend on IT security is minimal anyway, so there is no real scope for further cuts.

Q5 How do you think your overall IT budget for 2009 is likely to compare with 2008? Do you think the 2009 budget is likely to be...



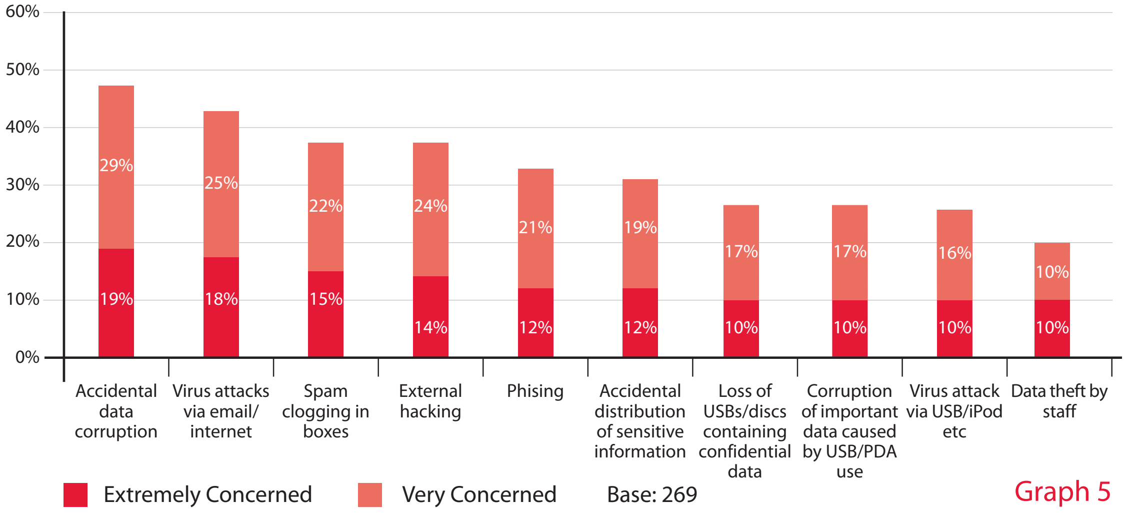
Graph 4

A further 11% stated the organization would be more likely to cut spend on IT security than on other IT products. Only 14% of these organizations believe it is vital to maintain a high level of investment in IT security as a key priority.

Understanding Risk

The reason for this lack of commitment to increasing security spend becomes apparent when assessing the SME market's understanding of current and emerging threats. Almost a half (48%) are either *concerned* or *very concerned* about accidental data corruption in the coming year; 43% are *concerned* or *very concerned* about virus attacks via email and 37% are *concerned* or *very concerned* about spam clogging email in boxes (Graph 5). External hacking (38%) and phishing (33%) are also key issues.

Q8 Thinking about the IT security risks that your business is likely to face during the coming year, which of the following types of threats are you most concerned about?



Graph 5

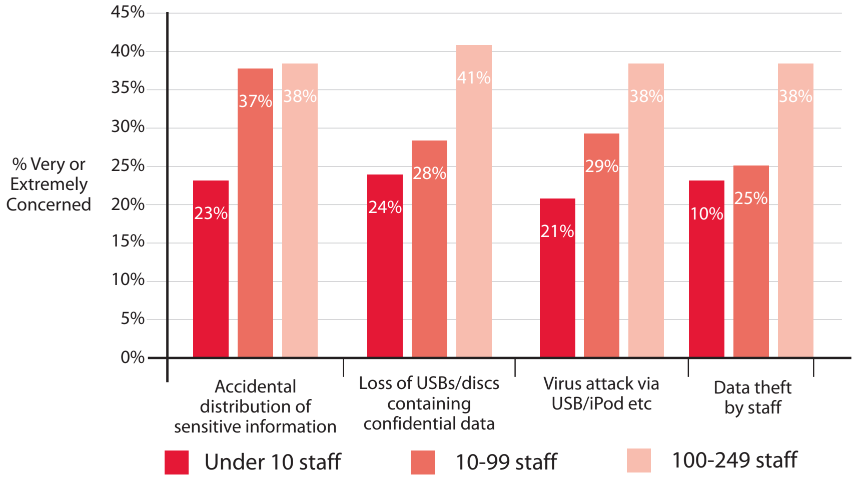
However, only 20% of organizations are either *concerned* or *very concerned* about data theft by staff. Yet recent surveys point clearly to the fact that this is a fast escalating risk, brought about by recession-led job insecurity.

Indeed, a recent survey of US workers by Ponemon Institute revealed that six out of every 10 employees stole company data when they left their job last year, using the information to get a new job, start their own business or for revenge. These figures are supported by another study conducted by McAfee which estimated total global economic losses due to data theft and security breaches by organized crime, hackers and inside jobs reached $1 trillion last year.

And this situation is not limited to the US marketplace. In the UK, the number of court cases brought to stop former employees using confidential data in their new jobs climbed sevenfold between 2006 and 2008, according to law firm Reynolds Porter Chamberlain (RPC). And this situation is expected to get worse as rising job insecurity is encouraging more employees to use confidential information obtained from their current employer when they begin working for a competitor.

Despite this clear trend, the GFI survey indicates that UK SMEs are overwhelmingly more concerned about external threats (78%), than internal (22%). Without a doubt, Management of smaller companies feel a closer bond to employees, tend to know them well and have a greater level of trust. Indeed, when these results are analysed further it becomes clear that the smaller the organization the greater the focus on external threats – as staff numbers grow, so does the perception of internal risk (Graph 6).

Q8 Thinking about the IT security risks that your business is likely to face during the coming year, which of the following types of threats are you most concerned about? ...concerns for some threats are influenced by company size...



Base: 120 (under 10 staff); 106 (10-99 staff); 42 (100-249 staff)

Graph 6

While only 10% of organizations with fewer than 10 people are concerned about data theft by staff, this rises to 38% of organizations with 100-249 employees.

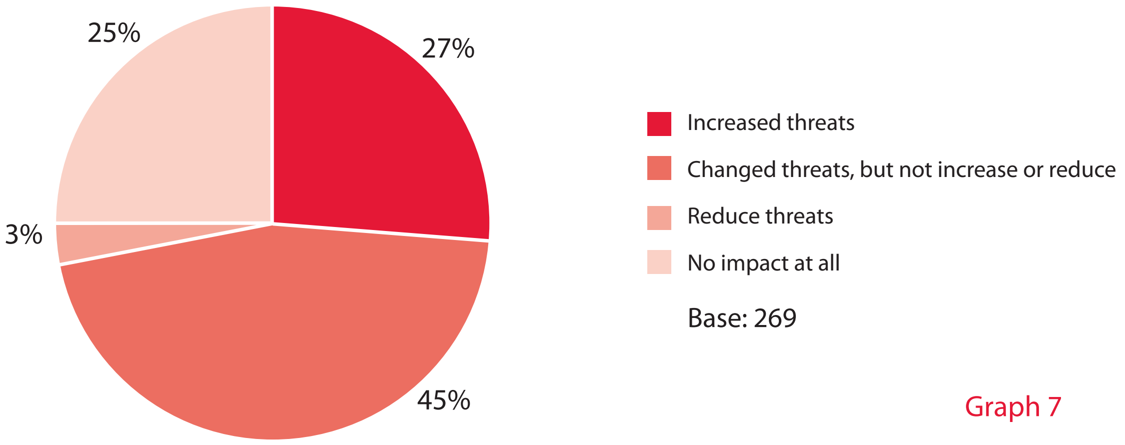
The results show similar, although slightly less marked, divergence for loss of USB sticks/discs containing sensitive data (41% larger organizations concerned against only 24% of smaller) and virus attack via USB/iPod (38% of larger, and 21% of smaller).

The differences are less notable when it comes to concerns about accidental distribution of sensitive information – rated a concern by 23% of organizations with fewer than 10 employees, 37% by those with 10–99 employees and 38% by the larger companies up to 249 employees.

Overall, 90% of organizations with less than 10 employees are more concerned with external than internal threats. This shifts to 74% of organizations with 10-99 employees and 57% of organizations with 100-249 employees, demonstrating the realisation of escalating threat as larger employee numbers reduce close staff/management bonds.

However, there is an awareness that security threats are changing as a result of the economic climate (Graph 7). Over one quarter (27%) believe that if the recession continues for a long time it is likely to increase the level of security threats faced; 45% believe the threat level will not change but the nature of the threats may change. However, 25% of organizations believe that the recession will have no real impact in terms of security threats at all, while 3% actually believe it will reduce the level of threat.

Q10 If the recession continues for a long period of time, what impact do you think this is likely to have in terms of changing the nature of the security threat you might face?



Graph 7

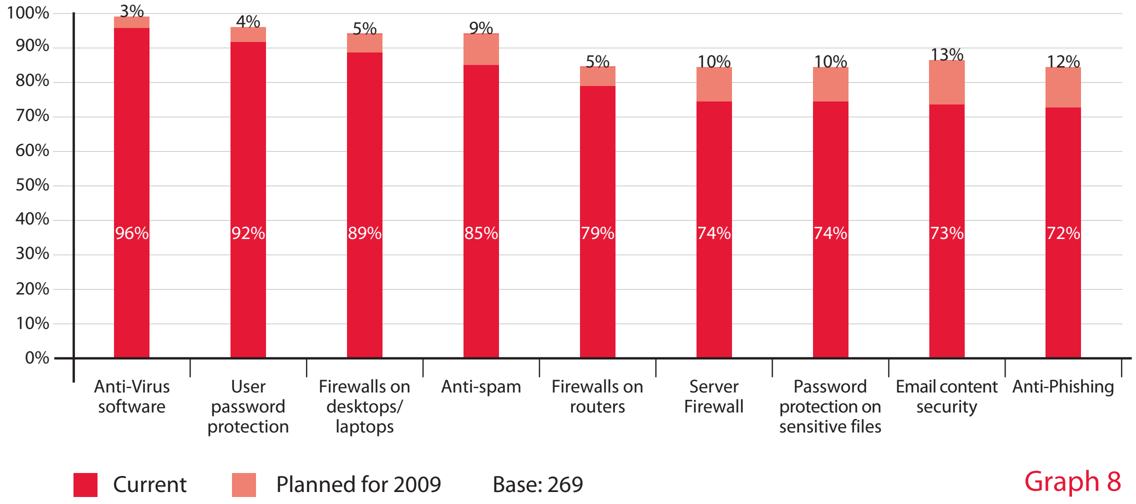
These results indicate that the UK's SMEs are failing to wake up to the new threats posed by a recessionary marketplace that is undermining employee confidence and morale. Corporate data is the lifeblood of any organization and even in the smallest organizations where trust is typically good, the looming threat of job loss will encourage any employee to look for economic leverage. Organizations simply cannot afford to continue to provide unhampered access to that information.

Securing the Organization

Given the widespread focus on external threats, it is little surprise that the survey reveals that UK SMEs are adhering to extremely traditional forms of security technology to mitigate risks. The vast majority of organizations already have the basic components of a secure infrastructure, namely anti-virus software (96%), user password protection (92%), firewalls on desktops/laptops (89%) and anti-spam (85%).

These organizations have also invested in firewall on routers (79%), server firewall (74%), password protection on sensitive files (74%), email content security (73%) and anti-phishing technology (72%) (Graph 8).

Q11 Which of the following IT security software application do you have in place that help you guard against these security threats currently and which are you planning to acquire? ... Widely used measures...

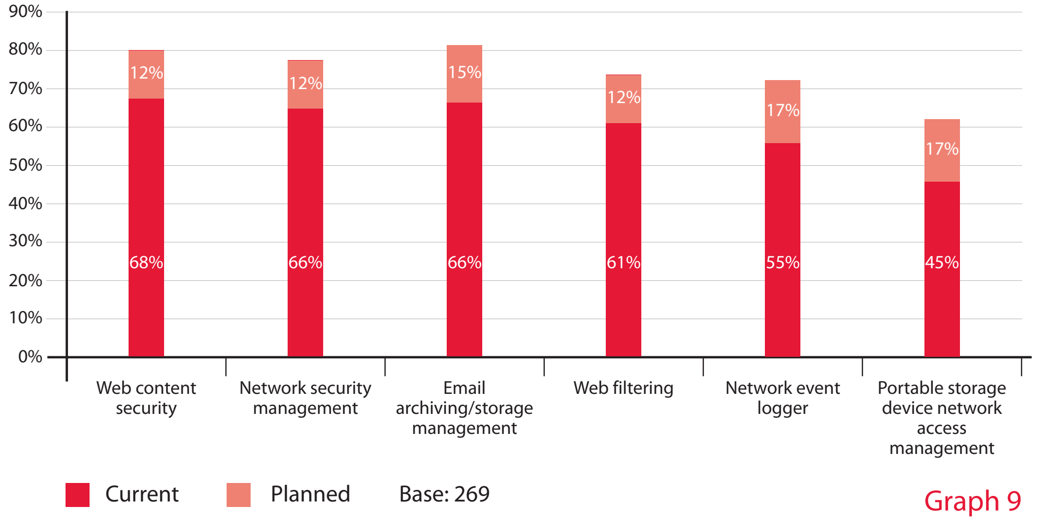


Graph 8

However, the results also reinforce the message that these organizations are failing to address the internal threat. Less than a half (45%) have invested in portable storage device network access management technology – and 37% have no plans to do so. Only 55% have a network event logger, and 28% do not plan to buy one in the coming year (Graph 9).

Once again there is also a marked difference in attitudes between the very small organizations and those with up to 249 employees. Only 36% of companies with less than 10 employees have portable storage device network access management, as opposed to 62% of the larger companies. Similarly 38% of smaller organizations have a network event logger, as opposed to 76% of organizations with up to 249 employees.

Q11 Which of the following IT security software application do you have in place that help you guard against these security threats currently and which are you planning to acquire? ... Less popular measures...



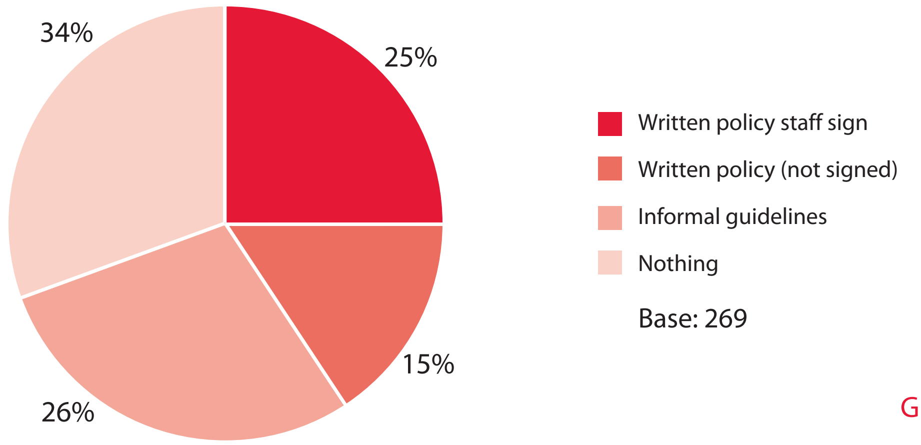
Graph 9

Yet without this technology, organizations have absolutely no way of tracking who has accessed what information/devices and when. They have no control over the use of USB sticks and iPods which can be used both to download sensitive data and introduce viruses such as the 'Conficker' worm which has infected over 10 million machines since January 2009 via the uncontrolled use of USB sticks.

This lack of corporate security through poor technology control is further undermined by an endemic lack of security processes to address the internal threat to corporate data. An extraordinary 60% of organizations have either no policy at all to regulate access to the network by portable devices or only informal guidelines (Graph 10).

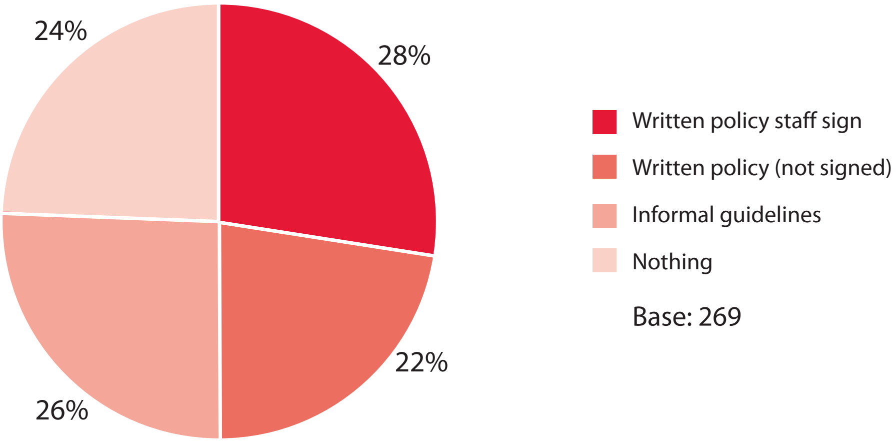
Opting for informal guidelines is of little value since they typically reflect low user awareness and understanding. If policies are not clearly defined and clearly explained, employees cannot be expected to understand the implications of their behaviour or change attitudes to sensitive data accordingly. Yet only 25% of these organizations have a written policy that must be signed by staff.

Security Policies in place
Q12 to regulate access to the network by portable devices...



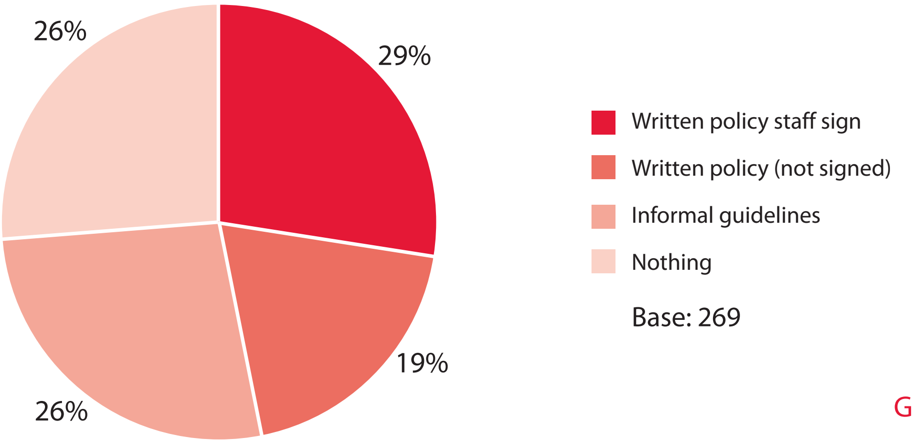
Graph 10

Security Policies in place
Q13 to control access to, copying of and dissemination of confidential data...



Graph 11

Security Policies in place
Q14 to specify what data/information employees are permitted to copy/hold copies of/take with them...



Graph 12

Similarly, only 50% of organizations have a policy in place to control access to, copying of and dissemination of confidential data. 28% have a signed written policy and 22% an unsigned policy (Graph 11).

Furthermore, 52% of companies have no formal policy in place to specify what data/information employees are allowed to hold/take copies of/ take with them (Graph 12).

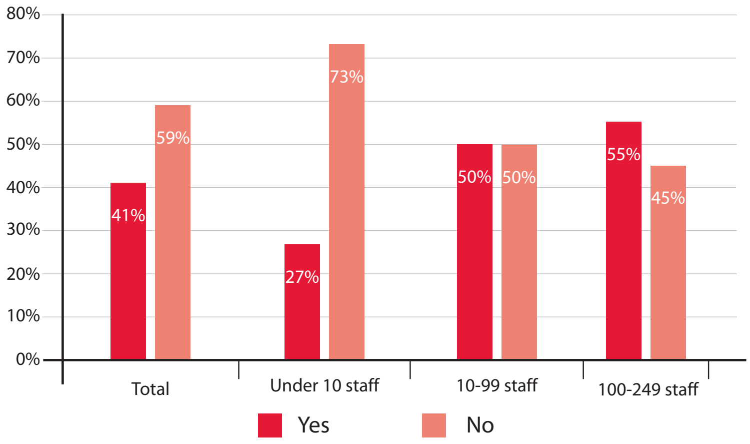
By failing to put in place formal policies, these organizations are enabling employees to undertake any number of activities that could seriously compromise the business – from using an external hard disk, to copying every customer detail and sales proposal on the database, to maliciously or unintentionally introducing a virus or simply compromising network performance by downloading large, personal music and video files.

Unless users have a clear understanding of policies and procedures, an organization simply cannot impose any degree of operational control over its essential corporate data. And however well trusted an employee may be, inadvertent actions that result in data loss or corruption can have just as devastating a corporate impact as any malicious activity.

Sensitive Data

In a climate of increasing data protection legislation and concerns about the security of both employee and customer data, the survey reveals a disturbing lack of control over information storage and management.

Q15 Do you have a formal process for catergorizing company data according to its sensitivity and restricting access accordingly?



Base: 269 (total)
120 (under 10 staff); 106 (10-99 staff); 42 (100-249 staff)

Graph 13

The majority of organizations (59%) have failed to put into place a formal process for categorising company data according to its sensitivity and restricting access accordingly (Graph 13). When broken down by company size, this rises to 73% for organizations will less than 10 employees. However, company size has a clear influence in this area, with 50% of those with 10-100 and 55% of those with 100 to 249 employees putting in place formal processes.

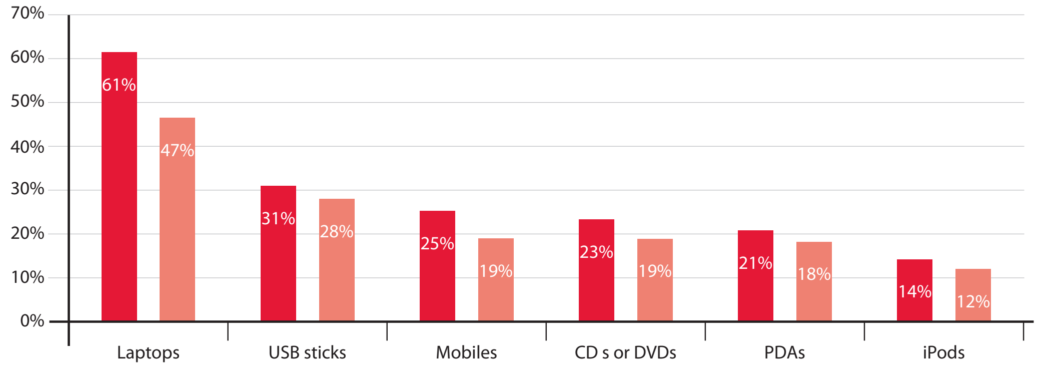
But these figures are still low given the fact that these organizations are all storing vast quantities of potentially sensitive/confidential data. Over three quarters (77%) store customer contact details – yet only 61% can track where this data is being stored at any point in time. This means over a third have no idea which desktops and laptops hold copies of this information.

Nearly three quarters (72%) store current financial data, but only 60% can track its location; 62% store customer account details, but only 52% can track its location. Disturbingly, while 56% are storing staff salary details, less than a half (49%) are actually tracking where this data is being stored at any one point in time, while only 46% can track staff employment records/HR files.

Organizations have a duty to store and manage this information securely – from customer credit card details to employee data. Without either the policies or technologies in place to control access to this information, organizations have absolutely no way of knowing whether or not this data is being abused or misused by employees intentionally or otherwise.

The reason for this lack of control is revealed by the widespread inability of these organizations to track or log the use of various devices on the network, from laptops to USB sticks and iPods.

Q17 Considering each of the following types of devices that staff might use, in eace case can you say whether network administrators can track/log a)which ones have been connected to the company network and when and b) what they uploaded?



🟥 a) Which connected and when

🟥 b) What was up/downloaded

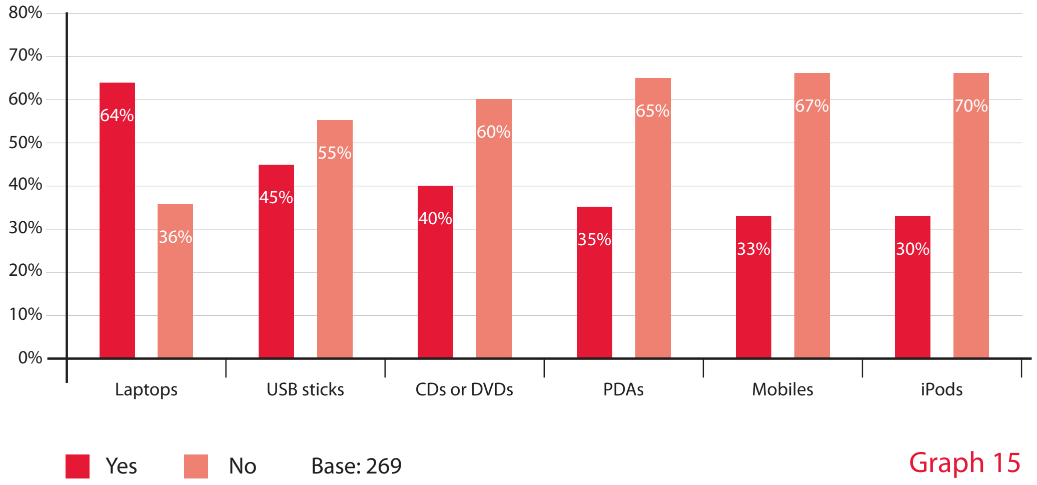
Base: 269

Graph 14

Indeed, while 61% of companies can track which laptops are connected to the network and when, less than a half (47%) can track what information or software has been uploaded or downloaded (Graph 14). The figures are far more shocking for other commonly-used devices. Only 31% of companies can track when a USB stick is connected, and only 28% know when information has been downloaded or uploaded via that device. With mobiles, only 25% can track connection, and 19% data loading; with very similar figures for CDs/DVDs and PDAs. With iPods, the figures drop further to only 14% tracking their use on the network and only 12% tracking whether data has been uploaded or downloaded.

Similarly, only laptops are routinely screened by specific security applications before access to the network is granted, with 64% of organizations having this technology in place. This drops to 45% for USB sticks, 40% for CDs or DVDs and a paltry 30% for iPods (Graph 15).

Q18 When someone connects one to the following devices to the network will it automatically be screened by specific security applications before access to the network is granted?



Graph 15

The survey also revealed a worrying lack of awareness of the need to retain and securely store emails. Only 35% of organizations currently have rules or policies stating how long emails must be held, although 26% are apparently planning to put something in place. Similarly only 41% have rules stating where emails should be stored – although, again, 21% are planning to put a policy in place.

Certainly pressure to comply with regulations and/or quality standards appears to have created a greater need to archive, catalogue and store email correspondence accurately and efficiently than five years ago, to a greater or less extent for 74% of respondents. However, 26% claim no pressure even to improve the quality of email storage and retention to boost the quality of service offered to customers – underpinning the continued lacklustre strategies in place to manage and secure this critical corporate information.

Conclusion

The recession is having an effect on every aspect of the organization and no business, of any size, can afford to ignore the changing security threat. Yes, smaller organizations typically enjoy greater levels of trust with employees as a result of close working and personal relationships. But with growing numbers of employees fearing job loss in 2009, however tight-knit the business, levels of trust are going to drop.

In addition to looking to leverage corporate information to boost their potential status in the job market, as individuals suffering financially become more desperate, they are also far more likely to fall prey to phishing attacks or other cons that lure them into revealing sensitive company information.

Getting through the next 12-18, even 24, months will be tough for the vast majority of the UK's SMEs. Adding a major security breach, such as the loss of key customer information to a competitor via a redundant employee, will make survival even tougher – especially if it results in a media furore.

These organizations have got to become far more concerned about data security and far more realistic about the source of security threats. Today's focus is not about protecting information assets from viruses. It is about protecting data from being lost, stolen, corrupted or tampered with. It is about knowing who is accessing what data, how and when – and just what they are doing with it.

As this survey reveals, too many organizations are underestimating the internal threat and relying on anti-virus software, spam filters and user password protection to secure the business. While these tools remain essential, they patently fail to address the fast-emerging internal threat level.

Companies need to look again at security plans, assess the fast-changing threats and put in place the culture, backed up by formal policies and suitable technology, to mitigate those threats.

Critically, organizations need to accept that the security threat is not just about Internet-borne viruses and face up to the very real human aspect. Putting in place formal policies to secure, control and monitor access to sensitive/commercial data is a fundamental step that must then be reinforced with technologies that control and track the use of devices on the network.

This fast-changing threat has certainly been recognised by larger organizations, with leading global research organizations such as Gartner suggesting that security spending will increase during 2009. This GFI survey has revealed that the UK SME sector is failing to keep up with its larger competitors and, as a result, adding unnecessary business risk at a time when business continuity and stability are critical.

About GFI

GFI is a leading software developer that provides a single source for network administrators to address their network security, content security and messaging needs. With award-winning technology, an aggressive pricing strategy and a strong focus on small-to-medium sized businesses, GFI is able to satisfy the need for business continuity and productivity encountered by organizations on a global scale. GFI has offices in the US, Malta, UK, Hong Kong and Australia which support more than 200,000 installations worldwide. GFI is a channel-focused company with over 10,000 partners worldwide. GFI is a Microsoft Gold Certified Partner. More information about GFI can be found at http://www.gfi.com.