Approaches to IT Security in Small and Medium Enterprises

Vassilis Dimopoulos[1], Steven Furnell[1], Murray Jennex[2], Ioannis Kritharas[1]
[1] Network Research Group, University of Plymouth, Plymouth, United Kingdom
[2] San Diego State University, United States of America

Abstract

Organisations of all sizes are now significantly reliant upon information technology and networks for the operation of their business activities. All therefore have a consequent requirement to ensure that their systems and data are appropriately protected against security breaches. Unfortunately, however, there is evidence to suggest that security practices are not strongly upheld within small and medium enterprise environments. The paper presents a survey of specific security practices within such organisations in Europe and the USA, with particular focus upon whether adequate attention is given to the issue of risk assessment. The survey reveals that SMEs are characterised by lack of adequate attention to IT security, with related responsibility frequently unassigned, or allocated to someone without appropriate qualification. This is shown to have consequences in terms of adherence to good practice, with the significant majority of organisations not having developed a security policy or undertaken a risk assessment.

Keywords
Risk Assessment, SMEs, Security Survey.

INTRODUCTION

The growth of the Internet as a medium for business and commerce has caused information and systems security to be a growing problem. According to the Department of Trade and Industry 2004 survey findings (DTI 2004), 74 % of the overall respondents suffered a security incident during the previous year (as opposed to 44% in 2002, and 24% in 2000). Such incidents usually result in financial losses to organisations, damage their reputation, disrupt the business continuity and sometimes may also have legal implications. Reliance upon the Internet leads to organisations being more exposed, with the 2003 CSI/FBI survey (Richardson 2003) indicating that 78% of attacks towards organisations had originated from the Internet. With such statistics in mind, organisations would do well to ensure that they are appropriately protected, and one of the fundamental approaches to achieving this is risk assessment. This paper investigates the adoption of such approaches, alongside other information security practices. Within this discussion, specific attention is devoted to Small and Medium Enterprises (SMEs), since these are frequently characterised by a distinctive IT security environment which leaves them much more vulnerable.

THE NEED FOR RISK ASSESSMENT

At a time when new threats and vulnerabilities are discovered almost on a daily basis, a key step in establishing appropriate security for a system is to properly assess the risks to which it is exposed. Without this, an organisation cannot be sure to have an appropriate appreciation of the threats and vulnerabilities facing its assets, and questions could be raised over any existing countermeasures (e.g. are they actually providing the protection that the organization requires, and to an adequate level?). A way to accomplish this is by conducting a Risk Assessment, "*A systematic and analytical process to consider the likelihood that a threat will endanger an asset, individual, or function and to identify actions to reduce the risk and mitigate the consequences of an attack*" (Hamilton 2004) Risk assessment can be split into two distinct processes:

The first is the process of Risk analysis can be defined as "*the assessment of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence*" (British Standards Institution 2000), and involves steps such as the identification of assets that need to be protected and the identification of threats and vulnerabilities related to those assets (Network Working Group 1997). After this comes the process of risk management, which involves the identification, selection and implementation of countermeasures that are designed to reduce the identified levels of risk to acceptable levels, this way controlling, minimizing and potentially eliminating the acknowledged security risks, at an acceptable cost (British Standards Institution 2000). Figure 1 sums up the five main elements that need to be taken into account when performing Risk Assessment (Hamilton 2002).

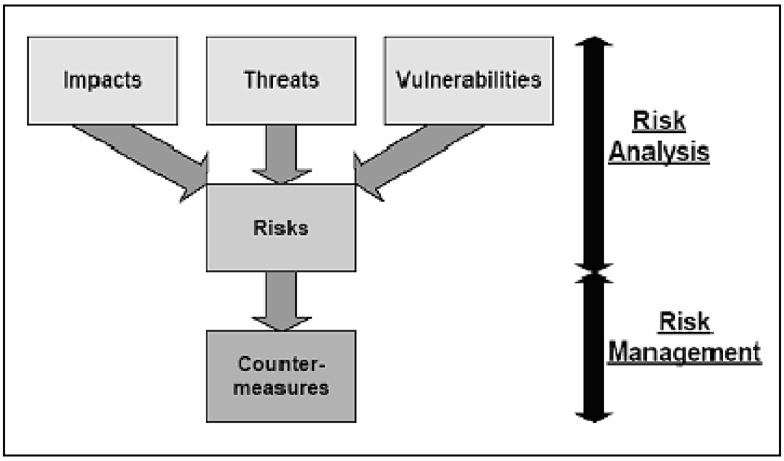

Figure 1: Typical Risk Assessment Process

Even though the value and importance of a risk assessment is widely recognised, surveys still indicate that a significant proportion of companies do not perform any risk assessment at all, as well as suggesting that the likelihood of the issue being addressed is closely linked to organisation size. For example, the 2000 survey from the UK National Computing Centre (NCC 2000) survey results indicated that approximately a third of respondents had never undertaken a risk assessment, with the problem again focusing primarily upon small enterprises. In organisations with 100 to 499 employees, the proportion that had not conducted risk assessment was a fairly respectable 16%. However, the figure increased to 31% in organisations employing 10 to 99 employees, and rose to 62% in those with fewer than 10 employees.

There are several reasons why risk analysis is not particularly popular with SMEs. One of the major disadvantages is that it can disrupt management and employee activities throughout its duration. This disruption becomes a more significant problem if the analysis points out deficiencies that need to be assessed (Federal Aviation Association 2001). A further setback is that no well-understood economic model exists for evaluating the benefits of reducing the risks versus the investment in security technology and management, i.e. the absence of an accepted industry-wide measurement system that would enable managers to judge the importance and the effects of the threats (Robins 2001). However, these points are also largely common to larger organisations, and it is therefore relevant to consider other aspects that may affect their attitude or ability of SMEs to address this issue, and indeed the topic of IT security in general. To this end, some of the characteristics of an SME that may contribute to a weaker stance on IT security have been gathered by Jennex and Addo (2003) and the main issues are summarised below:

- A relaxed culture and a lack of formal security policies (Blakely, 2002).
- A small IT staff with no security training (Blakely, 2002).
- Scarce investments in security technologies (Blakely, 2002).
- A lack of either business continuity or disaster plans (Blakely, 2002).
- Time, cost, and resource constraints restricting security efforts (Brake, 2003).
- Overly complex security solutions confusing SME staffs (Brake, 2003).
- Not knowing where to start (Brake, 2003).
- Security simply being put aside for more important things (Brake, 2003).
- Proliferation of 'always-on' connections increasing security risks (Suppiah-Shandre, 2002 and Donovan, 2003).
- Believing that they will not be targets of hackers or cyber terrorists and that anti-virus software is sufficient (Jones, 2002).
- Reliance on vendors and consultants for knowledge and expertise (Suppiah-Shandre, 2002) or on a single systems administrator (Donovan, 2003).

With these characteristics in mind, a survey was designed to investigate how they currently affect SME security practices.

A SURVEY OF SME SECURITY

The SME security survey is being conducted in both Europe (mainly the UK) and the US, by the University of Plymouth and San Diego State University respectively, in order to compare Small and Medium organisations attitude towards security. The reason for considering both geographical areas is because different security and data protection legislation apply in each continent, and the purpose is to investigate to what extent and how they influence organisations approaches to security. The survey is currently ongoing and the results in this paper are based upon 40 organisations from Europe and 81 from the US that have participated this far. The survey was distributed by hand or email to personnel related to the IT / security operation within organisations of various sizes. For the purposes of this paper, organisations with up to 250 employees are classed as SMEs mainly to allow for the results to be comparable with those in the latest DTI (2004) survey. The distributed survey had an identical main body in both European and US incarnations, and all reported results that show both survey's data are based on this main body. However, the European version also incorporated an additional section, which further investigated the issue of risk analysis – an area of security of particular interest to the ongoing research.

Figures 2 and 3 indicate that, despite the different legislation and requirements, respondents in both continents have a similar attitude towards IT security – and although there are some noticeable differences in some aspects (e.g. organisations in Europe appear to be better at applying operating system patches, while those in the US are better with implement password policies), the general picture suggests some significant areas of weakness in SME security. Even amongst the high-scoring categories (e.g. antivirus and firewalls), the results suggest that a fair proportion of organisations have not attended to these issues.

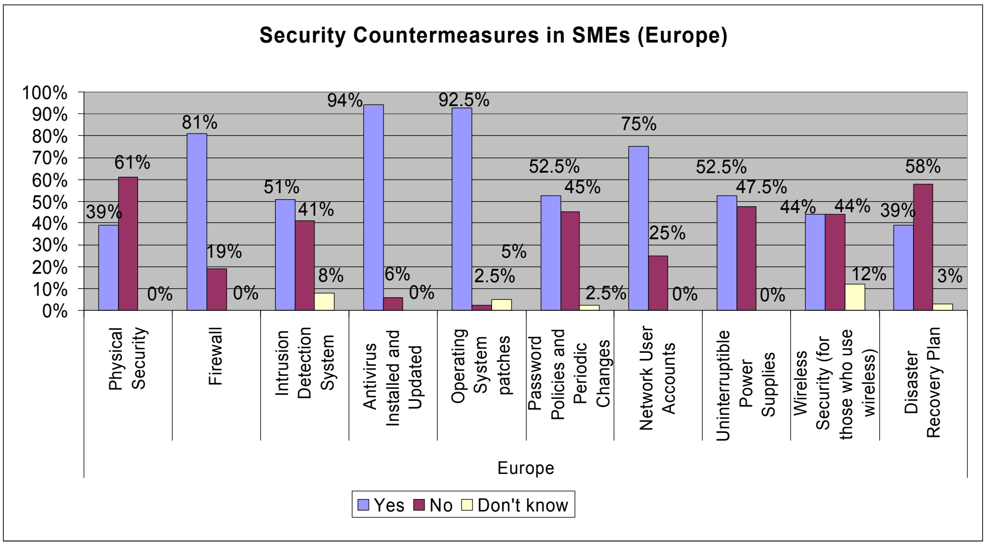

Figure 2: Security Countermeasures in Europe

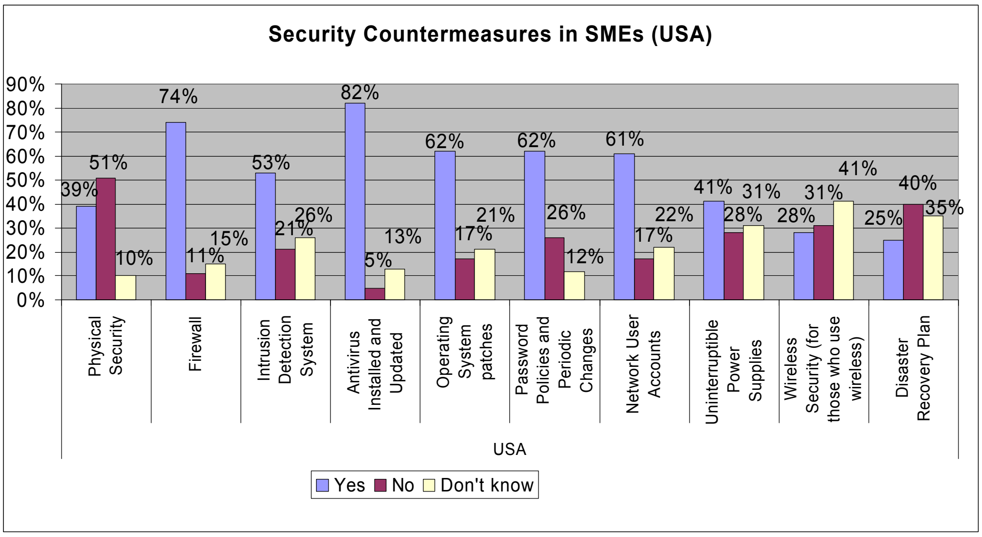

Figure 3: Security Countermeasures in the US

A key point is that these results are particular to the SME environment, and posing the same questions in larger organisations reveals substantially different findings. Indeed, in the US version of the study, where the questionnaire was also distributed to over 100 organisations with 500+ employees, the 'yes' responses were an average of 21% higher across these ten categories (although in some cases, such as attention to wireless security, even the large organisations still faired badly, with only 34% responding positively). Going beyond the results from the authors, it can be observed that the SME findings are also significantly lower that those in the CSI/FBI 2004 survey (Gordon et al. 2004) where, for example, 99% of organisations used antivirus, 98% used firewalls and 68% use intrusion detection (noting that the CSI survey primarily assesses organisations of more than 500 employees, and revenues of over $10M per annum).

As discussed previously, without having properly assessed the risks, questions can be raised upon the selection of countermeasures. These first findings from the survey prove this point, since it is obvious that SMEs concentrate on deploying antivirus software and keeping their operating systems up to date. However, while viruses are indeed indicated as the biggest concern surveys such as those already cited from the CSI/FBI, the same surveys also suggest that insider misuse results in some of the most significant losses. Our findings however establish that effectively half the SMEs do not take any action to prevent this.

EVIDENCE OF SME CONSTRAINTS

One of the key factors contributing to a number of the above points is that SMEs have restricted budgets. Industry surveys, like for example the ISM 2002 survey (Briney and Prince 2002), frequently suggest that the size of an organisation has a significant influence on its IT spending, which has knock-on consequences for what they will spend on security. From our survey, only 15% of the overall SME organisations questioned actually had a budget dedicated to security.

Another significant point is that SME environments are characterised by lack of IT security expertise. From the SME survey in the US, there was initial investigation on the percentage of organisations that employ a person who is responsible for the security of the organisation. As Figure 4 illustrates, the majority of organisations do employ someone who is assigned this task, and the proportion increases with the size of the organisation. However, there are still a significant percentage of cases in which responsibility is apparently unassigned, and the organisations concerned could consequently face serious difficulties if an incident occurred, as there would be no clear point of contact.

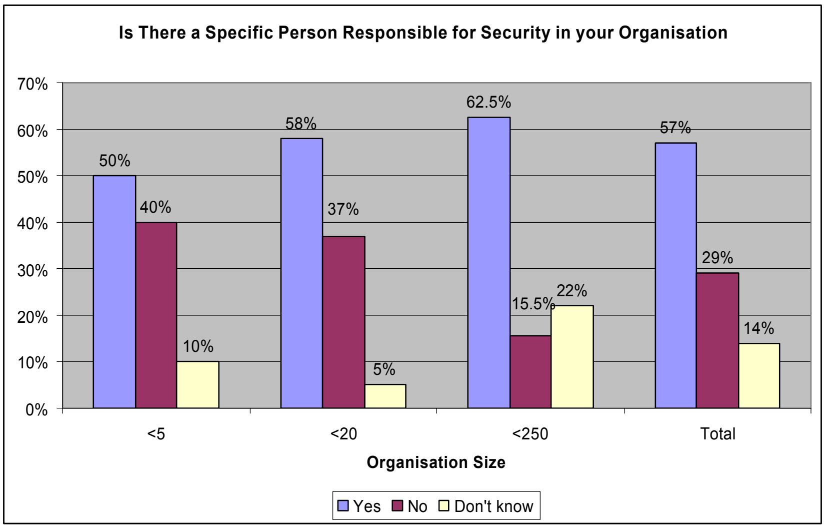

Figure 4: Existence of a Person Responsible for IT security in SMEs

Although designating responsibility is a good start, it is not the only issue. In Europe, the survey looked further in to the background of the person who has the responsibility of keeping an organisation's network secure. The associated findings are showing in Figure 5, and suggest that the percentage of SMEs that employ a dedicated security officer is negligible, with most assigning responsibility to the general IT administrator. In the smallest organisations, even this was unlikely, with the task falling to another person (commonly the owner or the manager), mainly because the number of employees is so small that no IT administrator is employed and that task also falls to the owner or the managing director. Post-survey interviews established that the same situation also held true for the US respondents.

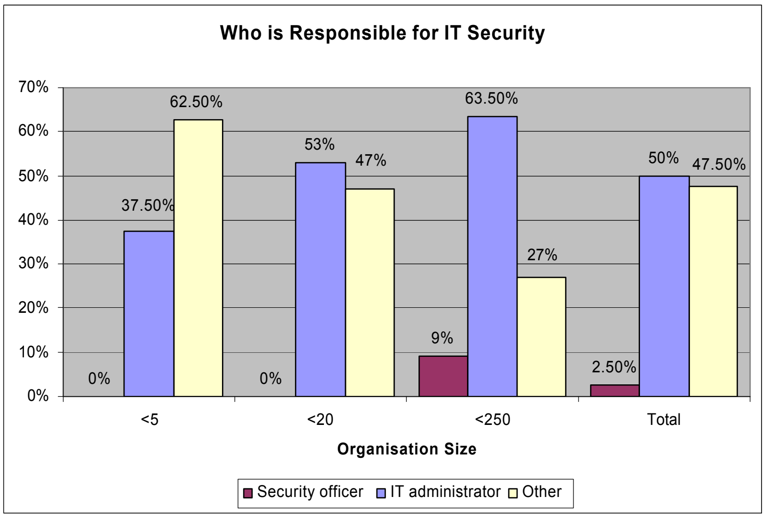

Figure 5: Background of the Person responsible for IT security in SMEs

When asked whether the designated security administrator had any formal qualifications, only 25% answered positively (note: the reason that the second category in Figure 6 has more security experts than the others is that respondents in this range they tended to outsource security more than others did – a factor that introduces significant extra costs). The overall findings suggest a significant lack in expertise within SMEs, and raise questions over their ability to adequately address their own security.

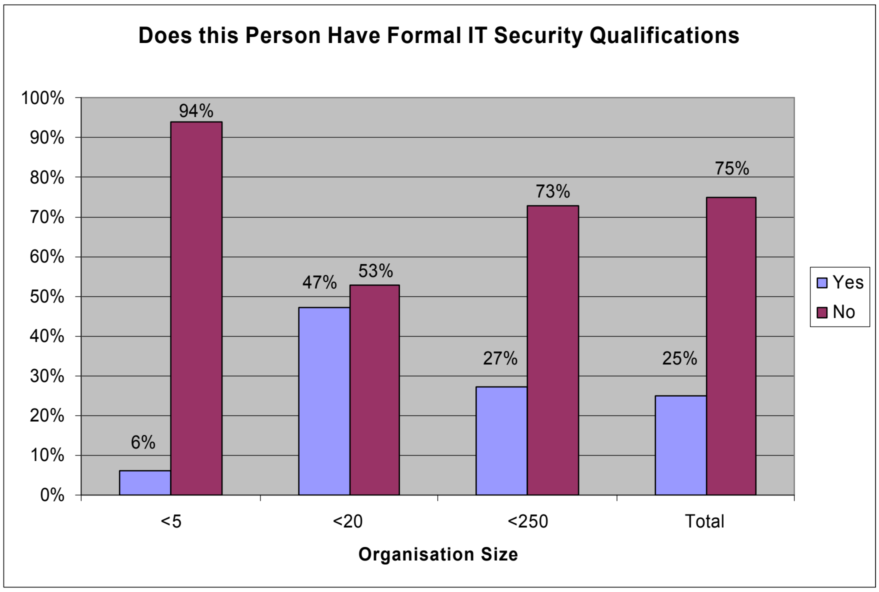

Figure 6: Does the person responsible for security have any formal qualifications

The consideration of these various constraints brings us back to the issue of whether our respondents had conducted a risk assessment. Having cited the earlier statistics from the NCC, Figure 7 depicts the more recent findings arising from the authors' SME survey in the UK. These findings suggest a somewhat more worrying situation than the NCC findings, and further analysis reveals additional causes for concern. For example, of the respondents that perform a risk assessment, 15 of them (73%) claimed to do it in-house. However, only 2 respondents claimed to use a risk analysis tool, and none used any security baseline guideline like ISO 17799. This, considered together with the limited proportion of organisations that actually employ any security specialist, raises doubts about how thorough or effective their assessment may have been. Indeed, given that risk analysis is often "perceived as being complex, requiring specialist expertise" (Shaw 2002), and that an evaluation of current commercially available risk analysis tools by Dimopoulos et al (2004) has shown that even they are not easy to use without appropriate expertise, it is apparent that many respondent SMEs are not well placed to assess risks for themselves.

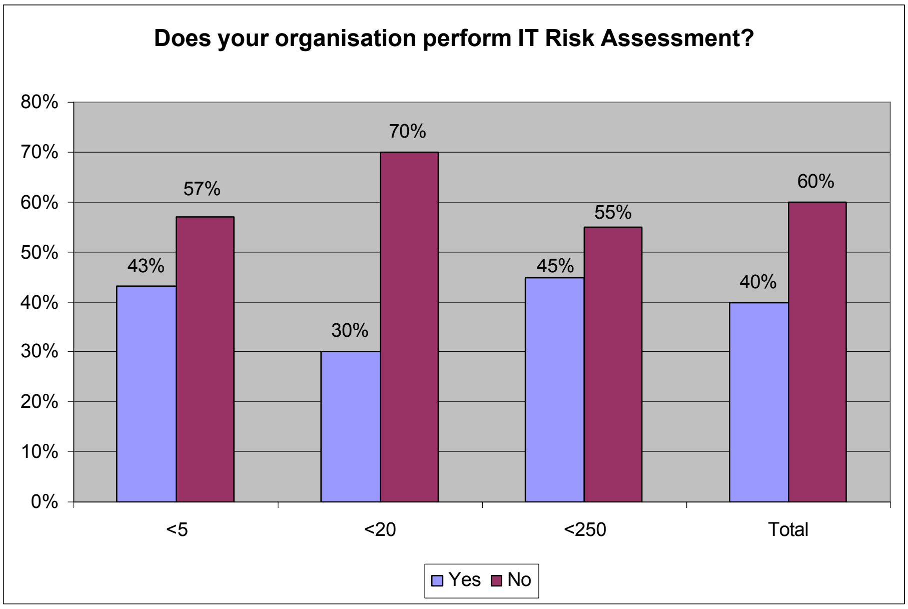

Figure 7: Organisations that perform risk assessment

Of course, lack of in-house expertise does not mean that the issue must go unresolved, and indeed it was already observed that several respondents claimed to outsource their security. For others, however, one of the key reasons that they had not conducted a risk assessment was lack of awareness of the need to do it. This situation is illustrated in Figure 8, based upon results from the UK respondents. One obvious reason for this lack of awareness is the aforementioned lack of security experts to act as advocates within SMEs. Another reason is that, even in some larger organisations, management is very rarely kept informed of the status of security incidents. Evidence for this particular assertion comes from respondents in the Global Information Security Survey 2003 (Ernst & Young 2003), with 14% revealing that they never provide the board of directors with a report about their organisation's information security status, while 19% only do it annually, and another 19% less often than that. However, since it is ultimately the management that approves security spending, they need to be kept more aware.

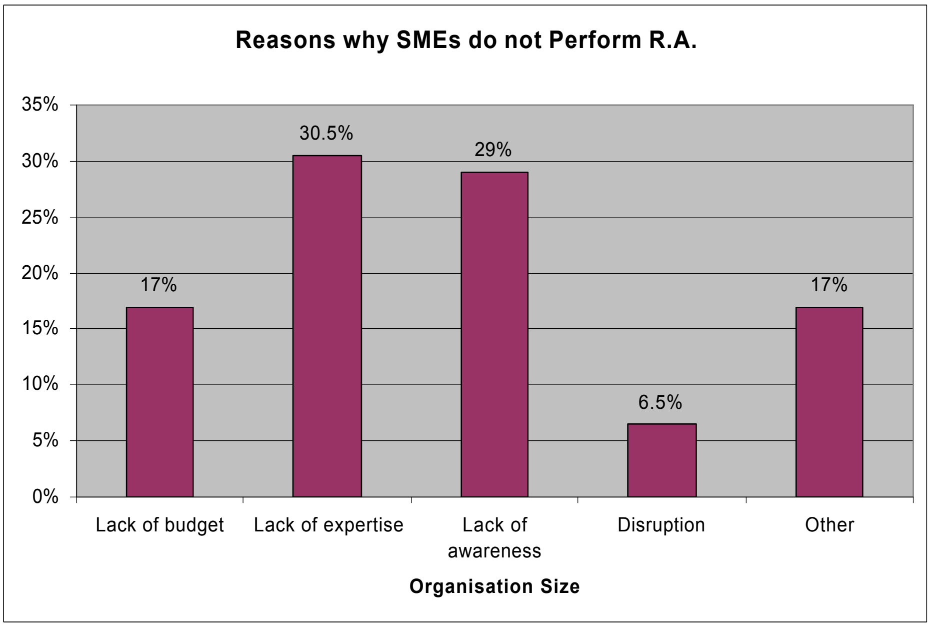

Figure 8: Reasons for not performing risk assessment

It should be noted that the impression conveyed in Figure 8 is not unique to our survey. All these characteristics listed above are again confirmed by the findings of the Global Information Security Survey 2003, where budget constraints (56%), resource priorities (48%) availability of skilled staff (32%) and management commitment (26%) and awareness (24%) are amongst the top-rated obstacles that prohibit effective information security.

The absence of risk assessment is not the only way in which lack of awareness may be manifested. Our findings also reveal that SMEs typically lack formally documented security policies. When considering internationally accepted standards such as ISO 17799, a security policy is the essential foundation for a successful security strategy, defining issues such as the IT security goals of the organisation, what specifications and guidelines need to be followed, and therefore what is acceptable and what is not. Without having defined these goals, an organisation cannot proceed to a comprehensive risk assessment. Of course after the R.A., the organisations security policy can be updated according to the finings. However, our survey investigated the percentage of small and medium organisations that have a documented security policy. Figure 9 illustrates the findings for the UK and the US, and it is worth noting that in this context the 'don't know' responses are effectively the same as 'no' responses, since even if the organizations concerned do actually have a policy, they are evidently not promoting it to their staff in an successful manner.

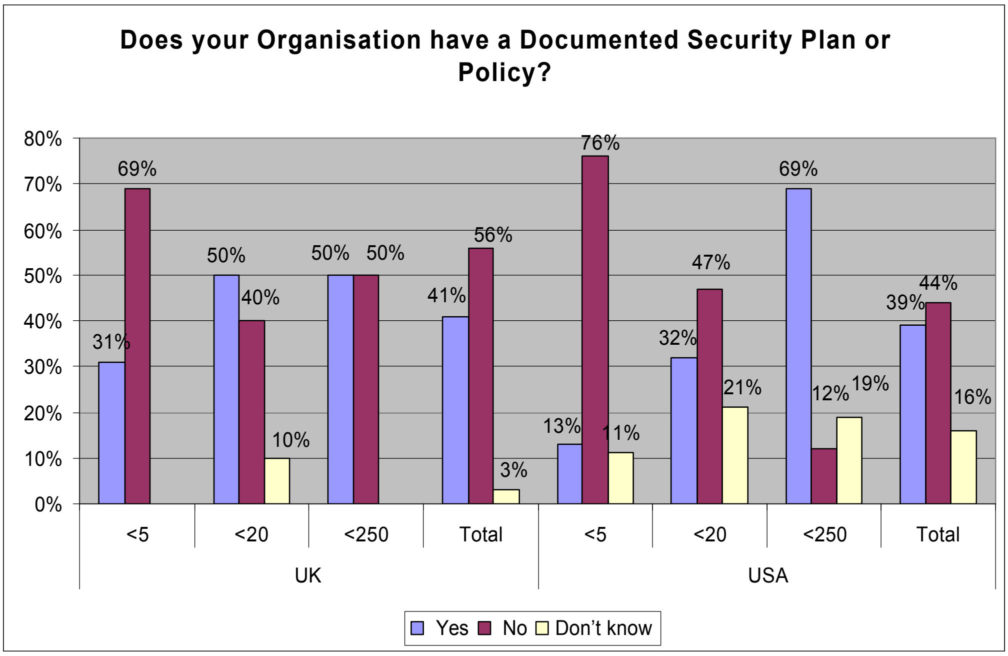

Figure 9: Documented Security Policies in SMEs

When these results are again compared with the findings of the DTI 2004 survey one can see the similarities in the findings. According to the DTI, in 2004, only 34% of small (1-49 employees) and 45% of the medium (50-249 employees) enterprises have a formal, documented security policy. A somewhat reassuring observation is that, according to the DTI, the percentage of organisations with a policy has marginally increased – in 2002 only 27% of small and 41% of medium enterprises had addressed the issue.

CONCLUSIONS

This investigation has provided evidence of a significant security problem in SME environments, and may lead to them experiencing avoidable security incidents as a result of not performing a risk analysis and not implementing the appropriate countermeasures. Recent publications estimate cybercrime costs small firms in Europe 22bn Euros a year to clean-up and recover from, while virus outbreaks can put company networks out of action for days and at the same time produce an average cost of 5000 euros in order to "clean up" (BBC 2004).

However, with the recognised constraints of in terms of expertise, awareness and budget, it is difficult to see how the situation for SMEs will improve without more fundamental changes to the approaches available to them. As such, one of the issues arising from the findings is the requirement for a new risk analysis and management methodology, which will aim to eliminate (or at least reduce) the drawbacks and assist SMEs to assess the risks their assets are exposed to. This aspect represents an ongoing element of research within the author team (Dimopoulos et al. 2004).

REFERENCES

BBC. (2004) “Small firms fail security checks”, BBC News Online, 30 March 2004, URL http://news.bbc.co.uk/2/hi/technology/3580105.stm, Accessed 5 August 2004.

Blakely, B. (2002) “Consultants Can Offer Remedies to Lax SME Security”. TechRepublic, 6 February 2002, URL http://techrepublic.com.com/5100-6329-1031090.html, Accessed 3 October 2003.

Brake, J. (2003) “Small Business Security Needs for the Changing Face of Small Business”. Micro and Home Business Association, 14 August 2003, URL http://www.security.iia.net.au/downloads, Accessed 3 October 2003.

Briney A. Prince F. (2002) 2002 Information Security Magazine Survey, does size matter?, Information Security Magazine, September 2002, URL www.infosecuritymag.com/ 2002/sep/2002survey.pdf, Accessed 15 July 2003

British Standards Institution. (2000) *Information technology - Code of practice for information security management*, BS ISO/IEC 17799:2000, 15 February 2001, ISBN 0 580 36958 7.

Dimopoulos, V., Furnell, S., Barlow, I. and Lines, B. (2004), “Factors affecting the adoption of IT risk analysis”
in *Proceedings of 3rd European Conference on Information Warfare and Security*, Royal Holloway, University of London, UK, 28-29 June 2004.

Donovan, J. (2003) “Small Business Security – Identifying Gaps And Providing Solutions,” Symantec Security, 28 February 2003, URL http://www.security.iia.net.au/downloads, Accessed 3 October 2003.

DTI. (2004) *Information Security Breaches Survey 2004*. Department of Trade & Industry, April 2004. URN 04/617.

Ernst and Young. (2003) *2003 Ernst & Young Global Information Security Survey*, URL www.ey.com, Accessed 10 July 2003.

Federal Information Processing Standards Publication 191. (2000) “Guideline for the analysis of local area network security”, March 2000, URL http://www.itl.nist.gov/fipspubs/fip191.htm

Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Richardson, R. (2004) *Ninth Annual CSI/FBI Computer Crime and Security Survey*. Computer Security Institute.

Hamilton, C. (2002) “Risk Management and Security”, RiskWatch, Inc., July 2002, URL http://www.riskwatch.com/Whitepapers/Risk_Management_and_Security_11-07-02.pdf

Hamilton, C (2004) “Are You at Risk? How to Assess Threats & Your Ability to Respond” Virgo Publishing, Inc., 2004, http://www.publicvenuesecurity.com/articles/3b1feat3.html

Jennex, M.E. and Addo T. (2004) “SMEs and Knowledge Requirements for Operating Hacker and Security Tools”. *IRMA 2004 Conference*, New Orleans, Louisiana, 23-26 May 2004

Jones, H. (2002) “Small Firms Warned Over Hackers,’ British Broadcasting Company, BBC News, 9 November 2002, URL http://news.bbc.co.uk/1/hi/technology/2428983.stm, Accessed October 4, 2003.

NCC. (2000) *Business Information Security Survey 2000.* National Computing Centre, URL http://www.ncc.co.uk/ncc/, Accessed 23 September 2003

Network Working Group (1997) “Site Security Handbook”. RFC 2196, September 1997

Robins G. (2001) “E-government, Information Warfare and Risks Management: an Australia Case Study”, Paper presented at the Second Australian Information Warfare and Security Conference 2001, URL http://wwwbusiness.ecu.edu.au/profile/schools/mis/media/pdf/0029.pdf, Accessed 14 July 2003.

Richardson R. (2003) “Computer Crime and Security Survey”. Computer Security Institute.

Shaw G. (2002) “*Effective Security Risk Analysis”*, April 2002, URL www.itsecurity.com/papers/insight2.htm, Accessed 16 July 2003.

Suppiah-Shandre, H. (2002) “Security - Top Priority For All”. SME IT Guide, International Data Group, Singapore, February 2002, URL http://smeit.com.sg Accessed 3 October 2003.

COPYRIGHT