Factors affecting the adoption of IT risk analysis

Vassilis Dimopoulos, Steven Furnell, Ian Barlow and Benn Lines

Network Research Group,
School of Computing, Communications and Electronics,
University of Plymouth, Plymouth, UK.
Email: nrg@plymouth.ac.uk

Abstract
Risk analysis is a necessary procedure for ensuring the appropriate protection of an organisation's IT infrastructure. However, its adoption within small and medium enterprise environments is often limited, with typical constraints including lack of in-house expertise, funding, and awareness, as well as the complexity of existing tools. This paper assesses these factors, and proposes the basis of an alternative methodology to enable small enterprises to conduct their own risk assessment. The proposal is based upon the use of predetermined protection profiles for assets, personnel and countermeasure solutions.

Keywords: Risk analysis, SME, protection profiles

1. Introduction

Numerous reports, surveys and related headlines from recent years have now firmly established the importance of IT security in the minds of many organisations. As such, the case for needing some form of protection, particularly in relation to Internet-based systems, is now difficult to argue against. However, significant questions still remain in relation to whether organisations approach the issue in the most effective manner. Without having properly assessed the risks to which its electronic assets are exposed, an organisation cannot be sure to have an appropriate appreciation of the threats and vulnerabilities its IT infrastructure is exposed to, and questions can be raised over the suitability and sufficiency of any security countermeasures that may have been introduced (e.g. are they actually providing the protection that the organisation requires, and to an adequate level?). As a result, risk assessment, a process which involves **analysing** and subsequently **managing** the risks, is widely recognised as necessary procedure in order to assess organisational security properly. As an indication of this, in the UK, it is mandatory that all governmental organisations and every other organisation they do business with to have performed a comprehensive risk analysis. (Spinellis et al. 1999)

2. Risk assessment in SME environments

Even though there are a number of relevant tools available in the market, surveys indicate that small and medium enterprises (SMEs) do not tend to undertake risk assessment and by not assessing the risks they are exposed to properly, enterprises leave important assets vulnerable to exploitation by anyone with malicious intent or even to accidental loss or damage, this way endangering a company's assets, reputation and credibility**.**

The focus of this paper is specifically upon the problem of risk analysis in small and medium enterprises (SMEs) as, according to surveys, the gap between the number of SMEs and large organizations that perform risk analysis is significant. For example, In 2000, only 37% of

organisations in the UK had carried out a risk assessment and the majority of those that had not were the small organisations (Department of Trade and Industry 2000), while in the National Computing Centre's 2000 survey results (NCC 2000) indicated that approximately a third of the businesses questioned had never undertaken a risk assessment, with the problem again focusing primarily upon small enterprises, as illustrated in Figure 1. More recently, in 2002, the percentage of organisations that had carried out a risk assessment had increased to 65% but the vast majority of those (85%) were again the large organisations (Department of Trade and Industry 2002).

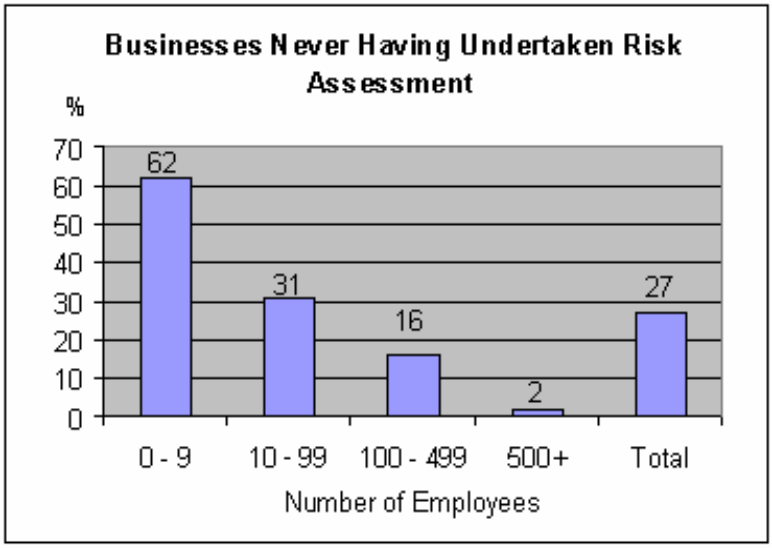

Figure 1: Use of Risk Assessment, by size of organization
(Source: NCC 2000)

Unfortunately, SMEs do not have less to fear in terms of security. Indeed, the protection of IT resources can be extremely important to the smooth operation of an SME, especially in the case of those organisations that have an increased business dependence on the Internet. Moreover, even though a large enterprise has the experience and resources to survive and recover from an attack, for most SMEs it could mean disaster as the loss of money, the damaged reputation and the potential legal implications of such an incident will have a 'fatal' impact on an SME that is striving to compete with the giants.

3. Factors limiting risk assessment in SME environments

There are several factors that may prevent existing risk analysis and management methodologies from becoming widely adopted in the SME contexts:

- **Restricted budgets**
  Industry surveys frequently suggest that the size of an organisation has a significant influence over the attention given to the security of its IT systems. Thus, a small enterprise (e.g. one with less than 100 employees or computers) will often be found to have less secure systems than those found in large enterprises (typically classed as those

with over 500 employees or systems). Apart from the difference in their network size, small, medium and large enterprises typically have a significant difference in their budget and spending for IT, which has knock-on consequences for what they will spend on security. To illustrate this, based on the findings of the ISM 2002 survey (Briney and Prince 2002), small enterprises devote approximately $132,000 per year for this purpose (an amount that represented 19.9% of their IT budget), while medium enterprises spend $360,000 (10.7% of their IT budget), and finally large organizations dedicate more than $1.3 million (representing 5% of their IT budget). From one perspective, this appears to be somewhat reassuring, in the sense that SMEs are apparently spending a larger proportion of their budget on security than their larger counterparts. However, the fact remains that SMEs still spend a lesser amount and since the vast majority of RA tools cost are considerably expensive; this prevents them from considering such investments

- **Lack of expertise**
  Since the dawn of modern computing, computer security has been left in the hands of "computer security experts" (Hoo 2000). When considering why SMEs fare so badly when having performed a risk analysis is in question, it is worth considering other aspects of their IT environment. For example, such environments are typically characterised by limited levels of in-house IT support, and thus maintaining a secure network often falls to a general IT administrator. It is common to find that this individual has no specific security training, and has a general knowledge in IT and networking instead. This is confirmed by the findings of the 2002 ISM survey which points out that 49% of small and 51% of medium organisations do not employ any employees with IT security training (Briney and Prince 2002). Having less to spend will also place some restriction upon the types of protection that an SME can introduce. For example, an SME would be less likely to devote funds towards employing a full-time security specialist to analyse and manage its risks. Indeed, survey findings indicate that the majority of security spending is directed towards technical measures as a first priority, overlooking people-centric initiatives (Ernst & Young 2003). This is why performing a risk analysis is often "*perceived as being complex, requiring specialist expertise and therefore something to be outsourced or basically delayed"* (Shaw 2002) especially when there is no full time security specialist on-site in order to perform such a task.

- **Lack of awareness**
  It can be conjectured that a non-security specialised administrator will primarily be aware of only the most well known security issues, such as viruses and hackers. Indeed, the first of these issues was indicated as the biggest administrative concern in the 2002 ISM survey, whereas the latter proved to be the biggest administrator concern in small and medium enterprises according to both the CSI/FBI 2003 (Richardson 2003) and DTI 2002 surveys (DTI 2002). With these perceptions in mind, it follows that many SME administrators would assume their systems to be relatively safe following the implementation of an antivirus system and a firewall (Lloyd 2002). Inevitably the same speculations can be made about the SME business managers, since their area of expertise is not IT security and thus one would expect them to rely on the administrator to take the related decisions. Consequently this lack of awareness creates a false sense of security

and SME administrators and managers do not appreciate the importance of performing a comprehensive risk assessment

- **Other reasons**
  There are several less important 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).

All these disadvantages can lead to the problem of SMEs experiencing avoidable security incidents as a result of not performing a risk analysis and not implementing the appropriate countermeasures.

4. Limiting characteristics of commercially available RA solutions

A way to discover reasons why risk analysis has not been widely adopted within SMEs is to investigate some of the major risk analysis tools and look for characteristics that make them inappropriate for this type of enterprise. An indicative example that is being discussed in many research papers is CRAMM, which is considered to be one of the most comprehensive risk analysis methods available. CRAMM originated in 1985, from the UK government's Central Computer & Telecommunications Agency, with several revised versions of the software having been released since (CRAMM 2003). In spite of its popularity, the specific risk analysis tool is attributed with many disadvantages. One of the main issues is ease of application, in the sense that the use of a comprehensive risk analysis method such as CRAMM is not something that could be left to a novice. Indeed, in the case of CRAMM, practitioners are required to undertake a training course in order to become qualified to apply it. If the organization concerned does not have this expertise, then this leads into the next potential problem, which is the associated cost of bringing in external consultants. CRAMM can, however, be forgiven for some of its drawbacks, since it was designed for government use, and therefore assumes a certain type of environment in the way that it approaches risk assessment.

However CRAMM is not alone in receiving criticism. An evaluation of three other major tools, which was performed by the State of California Employment Development Department and discusses the appropriateness and functionality of the methods, and again stresses certain disadvantages (Croft and Ramudo 1995). Amongst these findings was the problem that the results produced by two of the tools were difficult to comprehend, and were presented in a way that did not suggest why the vulnerabilities were significant. Secondly, the reports produced by the same two tools were considered to be excessively long, and could not be presented to management without important additions and alterations. A final complaint from the reviewers was that certain tools did not calculate some economic models that a risk analysis method would be expected to estimate (for example the Single Loss Expectancy). Even though there were still

some good elements, and not all tools suffered from the same drawbacks, one cannot help but notice that some of the issues related with risk analysis methods remain unchanged throughout the years, and are common for the major risk analysis tools today. Although these drawbacks could, to some extent, affect all potential users, it is again most likely that the SME audience will be the one most affected.

This is not to suggest that the need for special attention to SMEs has gone in the industry. Indeed, there are already some commercially available risk analysis products that are advertised as being suitable for SME environments. However, the authors' practical evaluation of such tools has still revealed some notable weak points. For the purposes of this investigation, two tools were tested, with positive and negative points being noted. While the products themselves will remain nameless, the observations arising were as follows:

Product 1

- ✓ It did not require particular expertise to perform the risk analysis, which took the form of answering questionnaires. The questions were not technical, and anyone who had taken part in setting up a network would know how to answer them.
- × The overall risk analysis process was particularly lengthy, and involved having to answer a very large number of questions (which in many cases were repeated multiple times). The resulting report was also extremely long. The proposed countermeasures came with no suggestions about how they could be implemented or configured, while the methodology did not take into consideration either the cost of deploying the countermeasures, or the value of the assets that need protection.

Product 2

- ✓ The tool considered the return on investment of security countermeasures as an element that was presented to the user, before having to choose which countermeasures would be implemented. At the same time, its cost which was low in relation with the very high prices for risk analysis tools commonly found in the market
- × The results were hard to interpret, and the rating of the threats was based upon the possibilities of them occurring (which could easily mislead a non-security trained SME administrator into neglecting some important threats, and create a false sense that assets are secure).

Finally, a third methodology that was initially under consideration was found to require a team from the organisation to obtain special training in how to utilise the tool - something that would possibly prevent an SME from selecting such a solution.

4.1 Other alternatives available to SMEs

At present there are several approaches available to companies requiring guidance on how to assess and strengthen their security without having to severely compromise their budget, but two are often suggested as the best options for SMEs. These are the use of security checklists (Chong 2003, Hurd 2000) and baseline guidelines, or a combination of the two (Young 2002). Security Checklists have the form of questions on common security issues, and can be used to raise awareness on security concerns and ascertain weaknesses (Heare 2001). Guidelines are an

alternative solution that can be followed in order to achieve security at a baseline level, but not as complete as the one accomplished after performing a risks assessment. A classic example of such documented security guidelines is ISO17799, the International Standard code of practice for information security management (British Standards Institution 2000),

Unfortunately, only a small proportion of businesses are aware of the contents of such standards and as table 2 suggests, with indicative data for the UK derived from the DTI 2002 survey, the problem once again concentrates on the small and medium businesses with 14% and 27% respectively.

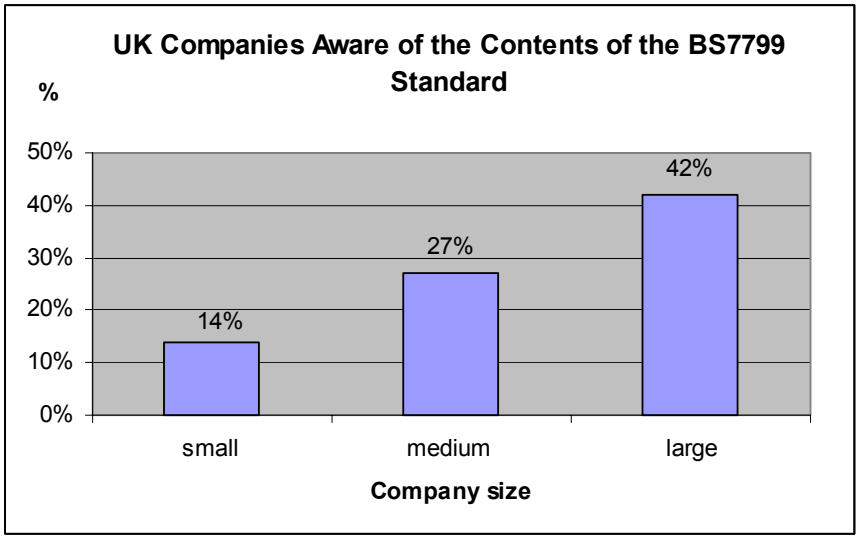

Figure 2: Organisational awareness of guidelines

The same survey also indicates that only 5.5% of all U.K. businesses are actually compliant with BS 7799 (the British Standards incarnation of the aforementioned baseline). This is most likely because guidelines mainly provide recommendations on the various threats to be faced and indications of how to counter them, without however going into detail on how to correctly deploy and configure the solutions. Considering the aforementioned lack of IT security expertise in SMEs it is clear how difficult the task of translating the guidelines to solutions really is. Therefore the problem in these cases is that they propose a solution that is too generic, and organizations without specific security expertise to guide them, may not recognize how certain elements apply to their environment. In addition, baseline security may not necessarily be sufficient, even for the requirements of SMEs, since being small does not mean that your systems are not business critical, and SMEs may well be utilising systems and data requiring a higher level of protection. Finally, another alternative suggestion is for SMEs to implement third-party managed security services (Paraskevas and Buhalis 2002, Spinellis et al. 1999). Third party security management is a solution to provide outside expertise and specialised support to SMEs that do not employ security specialists, but it can still represent significant expenses from the relatively small SME budget.

5. A proposed solution for simplifying risk assessment in SMEs

In order to tackle the problem of lack of risk analysis in SMEs there is a need for the development of a risk assessment methodology that includes several elements. Most importantly, a method intended for SME usage should be easy to apply. A desirable aspect of any new approach is that it needs to be comprehensive to the management, so as not to require a trained specialist in order to input the data and interpret the results. Making the results comprehensive to the management is actually desirable in any risk analysis scenario, since it is the management that approves the security-spending budget, and an increased managerial awareness on the threats and vulnerabilities towards the organizations assets would almost certainly guarantee an appropriate budget dedicated to assessing these risks by implementing countermeasures.

Making IT security comprehensive to the management is also why the methodology should take into account the Return on Investment (ROI) that is offered by implementing a security countermeasure solution. The ROI component is an issue that is mentioned in numerous articles as an element that is missing from existing risk assessment tools. A calculation of the Return on Investment from security investments facilitates "*executives understand the value of network security with regard to the economic consequences of a security breach"* (Cisco Systems 2003). Thus, after the assets and risks have been taken in consideration, calculating the ROI from implementing the countermeasures returns a feedback to the management which, as it is in financial terms, enables the management to make a decision on which solutions are necessary and which will mean overspending on the limited SME IT security budget.

Another requirement from a risk analysis methodology is to be generic enough to allow implementation by different types of organisations. A way to achieve this is to partition the generic approach in some way, and a means of doing this is based upon the concept of pre-determined protection profiles. A Protection Profile is *"an implementation independent statement of security requirements that is shown to address threats that exist in a specified environment"* (Commoncriteria 2003). In this sense, protection profiles represent a progression of baseline security. Baseline recommendations (such as ISO 17799) also aim for applicability across the whole range of organizations, domains, and platforms. The protection profiles however will take a more focused approach, and can be considered to provide baseline guidelines for different types of domain, different types of platform, etc, which organizations would then combine to suit their individual situation. This approach will use three different types of protection profiles to assess organisational security needs systematically. The first will be assessing the digital and physical **assets** of the organisation. At a first level asset-based protection profiles should assess the security requirements that are unique for each type of organisation (e.g. healthcare, manufacturing, banking, education etc), by indicating the assets that are common for organisations belonging within the same sector.

To demonstrate the concept of this, with the intention of being indicative rather than exhaustive, figure 3 illustrates how Asset Profiles will be structured. In order to assess the differing requirements of organisations, they need to be structured into suitable top-level categories. An organization performing the Risk Assessment would be expected to consider each of the top-level categories, select from a list the assets that are relevant to their case, and then guide the system by making the appropriate selections from the underlying sub-categories and profiles, and by

indicating information on issues like the physical location of these assets, the type platform they are stored in, etc. Recommendations will then be provided on the potential threats these assets are exposed to, and the possible countermeasures, according to their business function and the importance of the data that they carry.

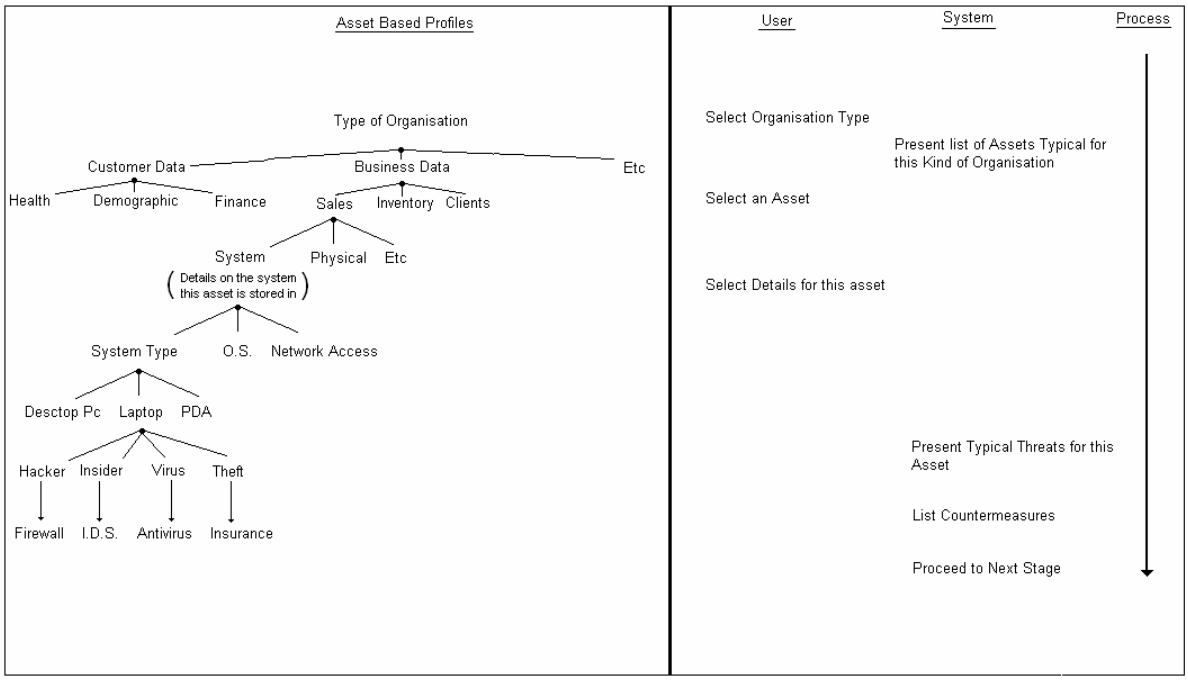

Figure 3: The Asset-Based Protection Profile Approach

Each profile at the final level would include a general statement of relevant threats along with suggestions for consequent countermeasures (including an indication of the level of protection that they would provide). Table 1 is an indication of how such a threat profile will be structured.

Threat Profile				
Threat name :	Malicious Code			
Definition:	Software or firmware capable of performing an unauthoried function on an information system [INFOSEC 99]			
Example:	Virus	Trojan Horse	Worm	Spyware
Likelihood level:	High			
Damage Level:	High			
Countermeasure:	O.S. Patches	Antivirus Software	Firewall	Awareness Initiatives
Importance Rating:	5/5	5/5	5/5	4/5
Implementation Order:	1	2	3	4

Table 1: Example of a Threat Profile

This aims to increase managerial awareness about the various threats, and assist with the selection of countermeasures, while also suggesting the order in which the countermeasures need to be implemented in the case of an SME not being able to deploy all the solutions (e.g. due to

budgetary constraints). This part mainly concerns the selection of countermeasures and not their configuration, which is an issue that is assessed by another type of protection profiles later.

Incorporating protection profiles into risk analysis aims to significantly reduce the amount of time required to perform a risks assessment since the protection profiles stage will cover the major known issues for each scenario, leaving the need for a final risk analysis which will only need to assess the issues that are specific for each organisation and cannot be generalised and included in the profiles. At the same time this approach will make the whole process more "user friendly" since there is not going to be a need for filling lengthy questionnaires.

The idea behind this methodology is that after the asset-based profiles point out the suitable solutions, these will go through certain other stages. The first of these will be the **ROI** stage, the outcome of which will give the manager the opportunity to select the countermeasures that make sense implementing. The other two types of profiles will then follow the ROI estimation – namely **personnel-based** profiles and **solution-based** profiles. The purpose of the first will be to assess, from a security perspective, the personnel that the organisation employs in terms of their job function, the level of access they require to various assets, the privileges they need to have within an organisations network etc. The solution-based profile stage will then attempt to assess and instruct managers on configuration issues of the security solutions that are going to be implemented. This guidance will be critical to achieving thorough security within an SME environment in which no security IT specialist is employed. Buying expensive security solutions with no security expert to configure them appropriately will not produce better results from buying the cheaper ones and setting them up correctly. For example, an expensive hardware firewall would probably make a manager feel more secure, but if it has not been configured correctly, it would not be more secure than a properly set-up standalone OS firewall which can be obtained for free. The solution-based profiles will provide suitable information to enable correct configuration by non-specialists.

6. Conclusions

By failing to assess the risks to which their assets are exposed, SMEs may leave themselves with serious weaknesses in their IT, which can have damaging consequences. Among the common reasons for this are lack of funds, and lack of expertise and awareness within the SME environment, as well as the disruption of employee activities that a lengthy risks assessment will cause.

The suggested approach attempts to eliminate (or at least reduce) these obstacles. Comprehensive assistance on the selection of security solutions, combined with the ROI element of the suggested methodology, offers more value to SMEs. The ROI element of the methodology can also serve as a way of raising awareness, by indicating to managers the trade-off in cost between securing an asset and potentially losing it. Finally, incorporating protection profiles in this methodology will reduce the length of the risk assessment process, while at the same time retaining an approach that is comprehensive enough to yield more specific recommendations than an organisation would obtain from simply utilising generic baseline standards.

References

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.

Chong C. K. (2003) *Managing Information Security for SMEs. May 2003*, Information Technology Standards Committee, URL www.itsc.org.sg/standards_news/2002-05/kinchong-security.ppt, Accessed 10 July 2003.

Cisco Systems. (2001) *The Return on Investment for Network Security*, URL www.cisco.com/warp/public/cc/so/neso/sqso/roi4_wp.htm, Accessed 12 July 2003.

Commoncriteria. (2003) *What is a Protection Profile (PP)?,* URL www.commoncriteria.org/protection_profiles/pp.html, Accessed 30 July 2003.

CRAMM. (2003) *The History of CRAMM*, URL www.cramm.com/history.htm, Accessed 20 July 2003.

Croft J. Ramudo A. (1995) *Automated Risk Analysis Tool Evaluation*. October 1995, The State of California Employment Development Department, URL http://workforcesecurity.doleta.gov/unemploy/txtdocs/finalrpt.txt, Accessed 9 July 2003.

DTI 2002. (2002) *Information Security Breaches Survey 2002*. Department of Trade & Industry. April 2002

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

Federal Aviation Administration. (2001) *Executing The Risk Management Process*, Nasdocs, URL http://nasdocs.faa.gov/nasiHTML/risk-mgmt/vol1/5_chapt.html, Accessed 9 July 2003.

Heare S. (2001) *Data Center Physical Security Checklist* December 2001, SANS, URL http://www.sans.org/rr/paper.php?id=416, Accessed 21 July 2003.

Hoo S. J. K., (2000) *How Much Is Enough? A Risk-Management Approach to Computer Security,* June 2000, Consortium for Research on Information Security and Policy, http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/06.doc, Accessed 14 March 2004.

Hurd D (2000). *Security Checklist for Small Business*, URL http://www.itsecurity.com/papers/nai.htm, Accessed 15 July 2003.

Lloyd I. (2002) *Step by step to safety. September 2002*, British Computer Society Computer Bulletin, p18, URL http://www.bcs.org.uk/publicat/ebull/sept02/step.htm, Accessed 30 July 2003.

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

Paraskevas A. Buhalis D. (2002) *Hosted application provision for small and medium sized*

Tourism Enterprises, Paper presented at ENTER2002 Conference, Innsbruck Austria, URL http://www.eyefortravel.com/ papers/ASpsSMTEs.pdf, Accessed 12 July 2003.

Richardson R. (2003) *Computer Crime and Security Survey*. Computer Security Institute, URL http://www.gocsi.com, Accessed 26 July 2003.

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://www-business.ecu.edu.au/profile/schools/mis/media/pdf/0029.pdf, Accessed 14 July 2003.

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

Spinellis D. Kokolakis S. Gritzalis S. (1999) *Security Requirements, Risks, and Recommendations for Small Enterprise and Home-office Environments*, URL http://www.dmst.aueb.gr/dds/pubs/jrnl/1999-IMCS-Soft-Risk/html/soho.html, Accessed 5 July 2003.