Considering IT Risk Analysis in Small and Medium Enterprises

Vassilis Dimopoulos
Steven M. Furnell
Ian Barlow
University of Plymouth

Network Research Group
School of Computing, Communications and Electronics
University of Plymouth
Plymouth, UK
info@network-research-group.org

Abstract

Surveys frequently indicate that a significant percentage of Small and Medium Enterprises (SMEs) do not tend to perform IT risk assessment and management. Even though there are a number of risk analysis tools available in the market, there are also several constraints to their adoption that need to be identified. A lack of related expertise and resources often means a lack of security awareness in SMEs, restricting their risk assessment options to the use of checklists, guidelines and managed security services. However these also have drawbacks, and there is a need for a risk analysis methodology that suits the needs of SMEs and can be applied in a more straightforward manner. It is considered that the use of predetermined protection profiles offers a means to simplify risk assessment, and make it accessible to small and medium enterprises from all sectors of the industry.

Keywords: Risk analysis, Risk management, SME

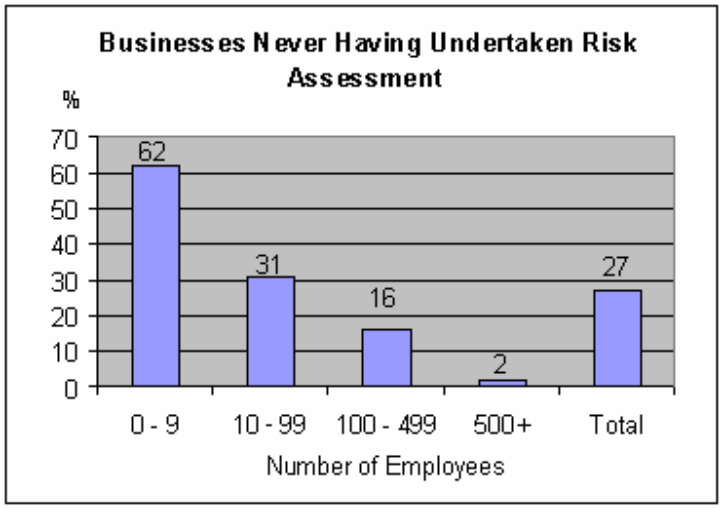
INTRODUCTION

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. Although this can partly be explained by the fact that a large enterprise uses more IT (and so naturally has to spend more to secure it), 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).

A key step in establishing appropriate security for a system is to properly assess the risks to which it is exposed. Without having done this, an organization cannot be sure to have an appropriate appreciation of the threats and vulnerabilities facing its assets. As such, questions could be raised over the suitability and sufficiency of security countermeasures that they may have introduced (e.g. are they actually providing the protection that the organization requires, and to an adequate level?). A way to accomplish this is by performing a risk analysis, 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 to those assets (Network Working Group 1997). After the completion of risk analysis ensues the process of risk management, which involves controlling, minimizing and potentially eliminating the acknowledged security risks, for an acceptable cost (British Standards Institution 2000).

The focus of this paper is specifically on 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, a 1996 survey from the UK National Computing Centre (NCC) showed that only 21% of small organizations had a formal approach to Risk Analysis (NCC 1996). This figure increased to 28% for medium organizations, while for large organizations it ranged from 47% to 83%, increasing in relation to the size of the organisation. More recently, the NCC's 2000 survey results 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.



(Source: NCC 2000)

Figure 1: Use of Risk Assessment, by size of organization

When considering why SMEs appear to fare so badly here, 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. As the 2002 ISM survey points out, 49% of small and 51% of medium organisations do not employ any employees with IT security training (Briney and Prince 2002).

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.

Unfortunately, this does not mean that SMEs 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, which serves to expose their assets to a variety of new threats.

BARRIERS TO TRADITIONAL RISK ANALYSIS IN SME ENVIRONMENTS

It should be clear that conducting a risk assessment would give an organization a considerable advantage in selecting appropriate protection. So why then do a significant proportion apparently not bother? In most cases, the reason is likely to be linked to the difficulties associated with risk analysis, which can limit its use in some environments. The aforementioned NCC surveys from 1996 and 2000 highlighted that the lack of Risk Analysis was mainly apparent in SMEs. There are several reasons why risk analysis is not particularly popular with SMEs. Firstly, and as previously indicated, it is "*perceived as being complex, requiring specialist expertise and therefore something to be outsourced or basically delayed"* (Shaw 2002). In addition, one of the major disadvantages of performing a risk analysis 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.

A way to discover reasons why risk analysis is not popular 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 an evaluation of more recent tools, which was performed by the State of California Employment Development Department and discusses the appropriateness and functionality of three major methods, 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 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. Finally, another complaint from the reviewers was that certain tools did not calculate some economic models that they would desire a risk analysis method to estimate (for example the Single Loss Expectancy). Even though there were obviously 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.

IDENTIFYING SECURITY REQUIREMENTS IN AN SME WITHOUT RISK ANALYSIS

At present there are several approaches available to companies wishing to assess and strengthen their security, 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 like ISO17799, 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), but these again are not suitable for implementation by non-security educated administrators since they mainly provide recommendations on the various threats to be faced without going into detail on how to implement the solutions. This, in combination with the lack of security awareness discussed earlier, is perhaps why the DTI 2002 survey indicate that only 5.5% of all U.K. businesses are compliant with BS 7799 (the British Standards incarnation of the aforementioned baseline). 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.

An alternative suggestion is for SMEs to implement managed security services. These can be either managed by a third party (Paraskevas and Buhalis 2002, Spinellis Kokolakis and Gritzalis 1999), or can be automated (Computer Weekly 2002). Third party security management is a solution to provide outside expertise and specialised support to SMEs that do not employ security specialists. In this case, the third party can be either the network service provider of an enterprise (Alcatel 2002), or a company dedicated to providing such services (IBM 2003). However an important issue in this case is the fee that employing such a service would incur, which can be a barrier to many small and medium companies with budget constraints. For the case of automated security management services that target SMEs, an indicative case is that of the Microsoft Security Toolkit (Microsoft Corporation 2003). The specific product offers a variety of services to the SME, claiming to "*provide a baseline level of security for servers connected to the Internet*". In order to do this, the toolkit consists of Guides, Updates and Tools. Guides are similar to the checklists described earlier and aim to give an idea of how the system can be configured securely. Updates include software bug fixes and security patches, while Tools include an analyser for security misconfigurations, a tool that configures servers to operate securely (e.g. analyse HTTP requests, selection of the technologies that the server may support) and a subscription to an e-mail security bulletin. In addition, this particular service has the advantage that the company distributes it at no charge. It has however some clear disadvantages; first of all it does not assess the case of insider misuse but instead organisations are advised to be guided by their own security policies for confronting this issue. Secondly, it is only useful for companies that are running a particular operating system on their servers. Finally, even though it eliminates security exploits that are due to the operating system, it does not assess a majority of other threats, such as malicious viruses that do not actually take advantage of operating system bugs but still have destructive results. Thus it is possible that such a tool would create a false sense of security to the SME manager or administrator, who might believe that the system is secure once it has been assessed. This does not mean that this sort of solution is worthless; in contrast it is very useful, but it simply does not provide complete security on its own.

ENHANCING THE EFFECTIVENESS OF RISK ANALYSIS METHODS FOR AN SME

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. Although this requirement can be met by the aforementioned checklist and guideline approaches, the problem in these cases is that they propose a solution that is too generic, and therefore those organizations without specific security expertise to guide them, may not recognize how certain elements apply to their environment. A potential alternative 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) aim for applicability across the whole range of organizations, domains, and platforms. The protection profiles would take a more focused approach, and could 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.

In order to assess the differing needs of organisations, protection profiles need to be structured into suitable top-level categories, according to the type of protection they provide (e.g. system, data, personnel, physical etc.). Within technical profiles reccommendations will be provided on the different security requirements for desktop PCs, laptops and PDAs and within these, further recommendations will be provided on their security needs according to their

business function and the importance of the data that they carry. In a similar way, personnel protection profiles will assess the priviledges that employees at various levels within an organization should have within the network, and physical protection profiles will address the varrying needs that different organisations require in terms of physical security (e.g. according to factors such as their geographic location, and the types of buildings they occupy). An illustration of such a structure is shown in Table 1. An organization would be expected to consider each of the top-level categories, then select any of the underlying sub-categories and profiles, as appropriate to their environment. Each profile at the final level would include a general statement of relevant threats and common vulnerabilities, along with suggestions for consequent countermeasures (including an indication of the level of protection that they would provide).

Profile Category	**Sub-category**	**Profile**
Physical	Location	Rural Urban
	Building	Old Modern
	People	Public-access Private
	Etc.	
System	System type	Desktop PC Laptop PDA
	Operating Platform	Windows Linux MacOS
	Network access	None LAN Internet
	Etc.	
Data	Business data	Clients Inventory Sales
	Personal data	Demographic Health Finance
	Etc.	
Personnel	Access	End user Manager Contractor
	Etc.	

Table 1: Examples of protection profile categories

The information in the table is intended to be illustrative rather than exhaustive, and many more sub-categories and profiles would be incorporated in practice. It is also considered that, for some categories, different profiles would apply for different domains (e.g. different profiles for physical protection might apply in the sensitive, but public environment of a healthcare establishment, versus the premises of a commercial organization in which controls upon public access could be more easily applied).

Another 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. This is one of the reasons why the methodology should take into account the Return on Investment (ROI) that is offered by security countermeasure solutions. 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). As such, there would be a distinct benefit in incorporating a perceived ROI value as part of the protection profiles within a practical realization.

CONCLUSIONS

Internet and information technologies play an increasingly necessary role in the operation of all modern organizations, including those classed as belonging to the SME sector. The consequent reliance has increased the importance of implementing appropriate IT security safeguards. However, if risks are not properly assessed, then organizations cannot be sure to have introduced appropriate protection, and are therefore taking a gamble that their network assets are secure, while in reality they may be exposed to numerous threats and vulnerabilities.

The paper has identified various reasons why SMEs may not be benefiting from existing approaches to risk analysis, and why the current alternatives open to them may not provide an adequate solution in all cases. The proposed approach involving protection profiles is perceived to offer an appropriate compromise, and is currently being pursued as a research project within the authors' group. Further details will be published as the methodology is developed.

REFERENCES

Alcatel Technical Paper. (2002) *Security in DSL Networks Issues and Solutions for Small-to-Medium Sized Enterprises*, URL http://www.alcatel.com/doctypes/opgrelatedinformation/child1/Security_tp.pdf, Accessed 15 July 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

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

Computer Weekly. (2002) *Microsoft's SME security toolkit is light on tools but heavy on product plugs*. November 2002, URL http://www.computerweekly.com/ Article117635.htm, Accessed 20 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

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

IBM. (2003) *Managed security services, protecting your e-business*, URL http://www-1.ibm.com/services/continuity/recover1.nsf/ers/mss+home, Accessed 20 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

Microsoft Corporation, (2003) *Microsoft Security Tool Kit: Guides, Updates, and Tools*, URL http://www.microsoft.com/technet/treeview/ default.asp?url=/technet/ security/tools/tools/stkintro.asp, Accessed 15 July 2003

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

NCC (1996) *The Information Security Breaches Survey 1996*, National Computing Centre, URL www.ncc.co.uk, Accessed 15 July 2003

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

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

Young C. (2002) *Strategy Clinic: Consult the experts*, November 2002, URL http://www.computerweekly.com/articles/, Accessed 25 July 2003

COPYRIGHT