A PROTECTION PROFILES APPROACH TO RISK ANALYSIS FOR SMALL AND MEDIUM ENTERPRISES

Vassilis Dimopoulos[1] and Steven Furnell[1,2]
[1]Network Research Group, University of Plymouth, Plymouth, United Kingdom; [2]School oj Computer and Information Science, Edith Cowan University, Perth, Australia

Abstract: Performing a Risk Analysis has long been considered necessary security practice for organisations, however surveys indicate that Small and Medium Enterprises do not tend to undertake one. Some of the main reasons behind this have been found to be the lack of funds, expertise and awareness within such organisations, this paper describes a methodology that aims to assess these issues and be appropriate for the needs of this SMEs by utilising a protection profiles and threat trees approach to perform the assessment instead of lengthy questionnaires and incorporating other elements such as financial considerations and creation of a security policy.

Key words: protection profiles, risk analysis, threat trees, SMEs

1. 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 2004 survey findings from the UK Department of Trade and Industry (DTI, 2004), 74 % of the overall respondents had suffered a security incident during the previous year (as opposed to 44% in 2002, and 24% in 2000). Such incidents may result in financial losses to organisations, damage their reputation, disrupt the business continuity and sometimes may also have legal implications. Of these, a significant proportion is attributed to Small and Medium Enterprises (SMEs). Furthermore, according to the same survey, large businesses are more successful in repelling these attacks as less than one probe in a hundred resulted in a breach, whereas with smaller organisations the amount was one in fifty. There are several reasons for this apparent weakness of SMEs. Among others, the most important include certain characteristics that distinguish them and put them in a more vulnerable situation compared to large enterprises as far as their IT security is concerned. For example, SMEs have restricted budgets that reflect to their I.T. and I.S. investments; furthermore, as proved by various surveys including the author's own, there is a distinctive lack in personnel with specific IT security expertise being employed by SMEs (ISM, 2002; Dimopoulos et al., 2004b) and this reflects to their security practices, such as conforming with legislations, following industry standards and producing detailed and documented security policies and incident response procedures. These leave SMEs vulnerable to security threats and make them suffer incidents that are costly both to their budget as well as reputation and from which they are less likely to recover compared to well established large organisations. This lack of expertise usually means that security is left to the hands of the management or some general administrator which further raises an issue of lack of awareness on the methods available for securing critical IT assets and correct implementation of any selected countermeasures. 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).

There are several practices that are available for SMEs wishing to ensure they are protected from such incidents. A key step in establishing appropriate security for a system is to assess properly 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, and 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?). As a result, 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), is widely recognised as necessary procedure in order to assess organisational security properly. However, 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. Recently, the author's SME security survey found that in the UK 60% of the SMEs questioned have never performed a risk analysis.

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.

Figure 1 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. (2004a) 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.

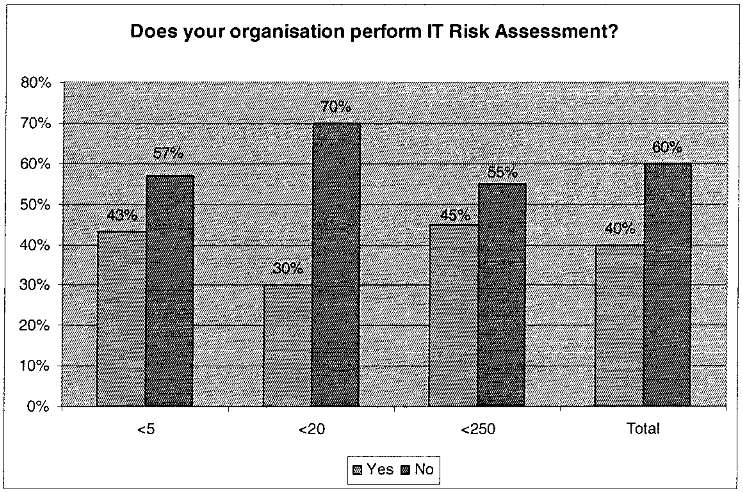

Figure 1. Organisations that perform risk analysis

The authors' survey further looked to establish the reasons why RA is not being performed and found that the main reason according to the respondents is the lack of in-house expertise as illustrated in Figure 2.

More recently, the author's SME security survey found that in the UK 60% of the SMEs questioned have never performed a risk analysis.

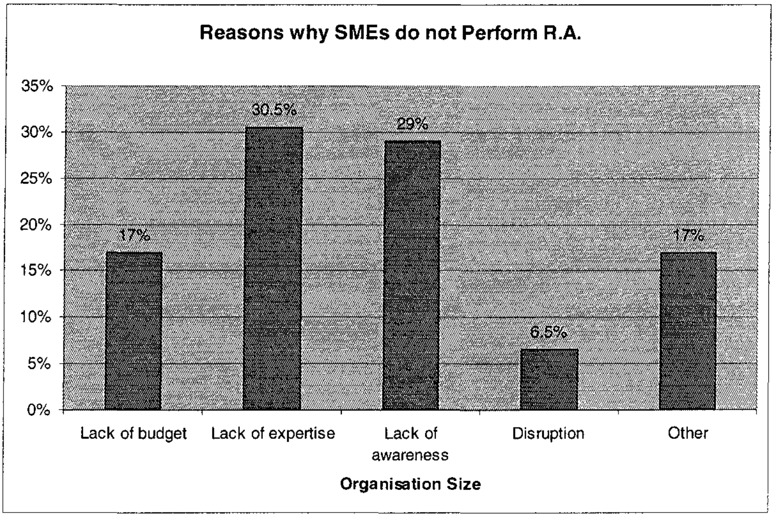

Figure 2. Reasons why some organisations do not assess risks

For organisations that are not capable of performing such an analysis due to the constraints described earlier there are theoretically several other solutions to follow. At present there are a number of 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, 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.

2. REQUIREMENTS

From what is discussed in the previous sections, it is clear that there is a need for a security methodology that addresses the problems associated with SMEs. In a previous paper, following is a summary of the requirements that have been established (Dimopoulos and Furnell, 2005) as necessary for this methodology that, if realised, will make it appropriate for this section of the industry.

- The awareness issue could also impede the new method, if not appropriately promoted.
- The methodology needs to be a progression of baseline, meaning that it would cover the security requirements of various types of organisations but without being too generic
- The methodology should be designed to enable anyone within the organisation who is aware of its requirements and assets to perform an analysis, resulting in a product which is user friendly, easy to use and produces comprehensive and easy to interpret results
- This investigation does not aim to produce a commercial product
- By incorporating economic elements such as the return on investment (ROI) and the annual loss expectancy (ALE) one of the aims is to make the management more aware of the impacts of a potential compromise (the other aim being to assist the management in selecting wisely which assets are worth protecting and how much should be spent on them)
- As part of the protection profile approach, at the outcome stage, the methodology should produce a profile of the organisations assets and implemented countermeasures which should be easily updateable.

3. ELEMENTS CONSTITUTING THE RESULTING METHODOLOGY

Generally, the resulting methodology will involve three major stages:

- The assessment stage, where information about the organisation and its network will be entered by the user
- The financial considerations stage, where the solutions that will appear as appropriate from the previous stage will be considered in terms of their cost-effectiveness for the organisation
- The output stage, where the user will be presented with the recommended solutions and further information that will be useful for the organisation

These stages are examined in the sub-sections that follow.

3.1 The risk assessment stage

Protection Profiles (PP) are used in this stage in order to simplify the assessment process. PPs are defined as "an implementation independent statement of security requirements that is shown to address threats that exist in a specified environment" (Commoncriteria, 2003). Therefore their function will be to identify what assets an organisation has, how important they are, what threats are associated with each asset and what countermeasures are relevant. In addition, the aim is to achieve this without requiring the user to fill lengthy and time-consuming questionnaires while at the same time enabling users with no security training to perform it. The structure for these profiles will have the form of simple threat trees which will commence from an asset and navigate the user through details for the asset, and conclude to a threat profile which is discussed later.

3.1.1 First profile stage (the initial profile stage)

To begin with, the person performing the analysis will be required to select from a basic set of options concerning the organisation being assessed, its size, function and other basic aspects that are described in this section. This will help build an initial organisational profile.

The type (i.e. which industry sector it is involved in) and size as well as the primary purpose of the organisation (e.g. research) will distinguish typical IT assets and personnel that are found in all organisations belonging in the same sector and rate their criticality to its operation. There are several types of organisations that need to be included, but the ones belonging to the same sector will typically have the same assets which will be of the same importance to them. According to the 2005 threat report from Symantec, even the organisations belonging to industry sectors that are very rarely targeted cannot neglect their security. On the contrary, by comparing the numbers in Figures 3 and 4, one can see that in proportion even though organisations such as manufacturing, transportation, entertainment and telecoms are rarely attacked, the impact of these attacks is the most severe. High tech, however, which is the most targeted industry hardly suffers any severe losses. Such results firstly highlight that organisations from all sectors should take security seriously but furthermore that for each type of organisation the impact of loss of one asset can be far more severe than for another. As an example the downtime of a high-tech organisation's IT network has far less impact, both financial as well as to its reputation, than if the network of a bank is compromised.

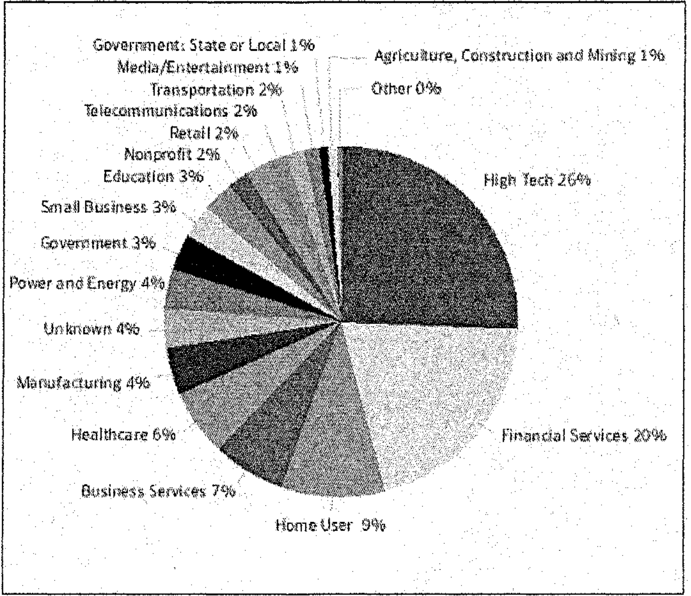

Figure 3. Percentage of attacks by industry sector (Symantec, 2005)

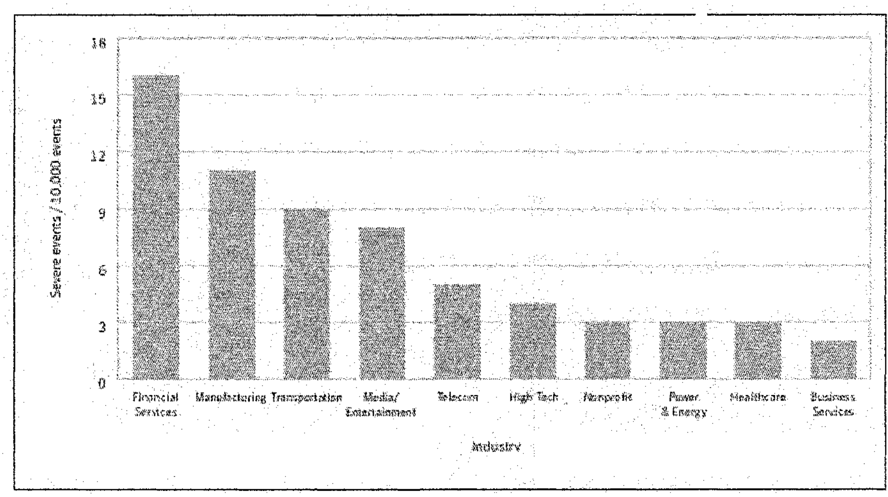

Figure 4. Attacks categorised by severity (Symantec, 2005)

A supplementary issue that needs to be investigated in this stage of the profiles is the geographical location of the organisation. This, in combination with the industry sector, will determine which legislations and standards an organisation needs to conform with. Hence there will be some knowledge in advance of which assets are the most critical and how to avoid their compromise as well as any resulting legal implications.

Another outcome that can be derived when selecting what industry sector the organisation being assessed belongs to and producing apart from producing a list of the typical assets found within such an organisation, will also produce a rating of how critical each of these assets is to the specific type of organisation, enabling this way the tool to set a threshold for the appropriate compromise between security and convenience (i.e. facilitating a decision on how much access and productivity can be compromised to tighten security as illustrated in Figure 5). For example, in a research/university institution it is normally essential that the employees have access to the Internet, while in a bank having an employee browsing web pages is often considered a misuse of resources.

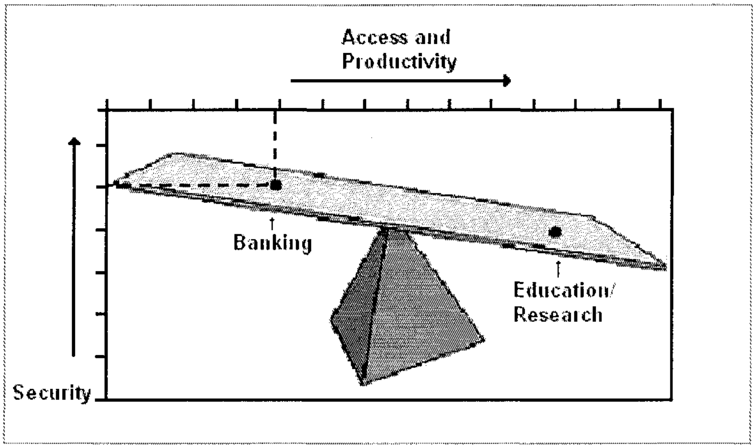

Figure 5. The essential balance between security and productivity (modified from Cisco, 1995)

In addition, producing a list of what type personnel is typically being employed will assist with configuration of the countermeasures issues and access rights to different assets and resources at the output stage of the methodology. Finally, what is further gained from weighing up the level of security instead of going for a "raw" tightening of security approach is that it will also assist in the effective operation of the organisation, in the sense that it will prevent excessive security from becoming a nuisance to employees that actually need quick access to certain organisational assets. As an example, however sensitive the confidentiality of patient records might be for hospitals, it would be almost completely impractical to deploy biometric access security to these resources to doctors that need emergency access to them and cannot afford false rejections when trying to access them in an emergency situation.

A further significant issue that will be evaluated in this stage is the position within the organisation and level of security expertise of the person performing the assessment. This will then determine how technical the particular assessment will be. As a result, if the user is aware of technical issues and (for example) is the one who has set up the network for the organisation, a straightforward analysis can be performed by identifying threats to the assets and what consequences they might cause, classifying the main threats with respect to the potential result towards an asset i.e. (Meyer, 1995):

- Disclosure: loss of confidentiality and privacy
- Modification: loss of integrity
- Fabrication: loss of authenticity
- Repudiation: loss of attribution

and how critical the effect of each would be to an organisation depending and on which industry sector it belongs to. The respondents can be distinguished to several levels in terms of their work function within an organisation, senior management, med and lower level management, supervisory and finally technical support staff. The advantages of making such a distinction within the methodology are that it enables even a person with no assumed technical IT knowledge at all (e.g. a manager) able to perform an assessment based on certain other aspects. Thus instead of asking technical issues, the assessment can be based on the business impact of breach of a specific asset and by considering the business functions of an organisation according to the type of the organisation and the sector thus identify the critical assets.

Moreover, making the methodology appropriate for anyone within an organisation who is involved at some level with the assets or the IT will help eliminate the significant issue of a tool becoming a disruption to company activities, since it will not require inputs from everyone but anyone involved with knowledge of the organisation will be able to perform at least some level of the analysis. This will be further complemented with the elimination of lengthy questionnaires by using profiles. In addition, the level of expertise of the user will not only affect the different types of approaches to the assessment that will follow, it will also affect the output of the methodology which will be tailored to match the expertise of the user. A final consideration that will be carried out in this section is that of security policy issues. The importance for an organisation to have a security policy is widely recognised therefore the aim is for the methodology to assist with creating one. This creates a need at this stage for the user to reply to questions related to the efficiency of any already existing policy if there is one.

All this initial information that is discussed in this section will lead to the tool producing a list of assets for an organisation which will then be used as an input to the next part of the methodology. Since these will include all the typical assets found within the type of organisation that is being assessed, the input of the user will again be required in order to review and discard any that are not appropriate to the specific organisation.

3.1.2 Second profile stage (main protection profiles)

Having established what assets can be found within the organisation and ranked them in terms of their importance (according to industry sector, legislations etc), the next step is to analyse the details for each asset and the possible threats and countermeasures. This will be achieved by creating threat trees, like the one in Figure 6, for each asset. The user will use threat trees to select appropriate solutions in a graphical mode describe these will be combined with a graphical interface aimed to illustrate to the person performing the analysis, the effects of the solutions

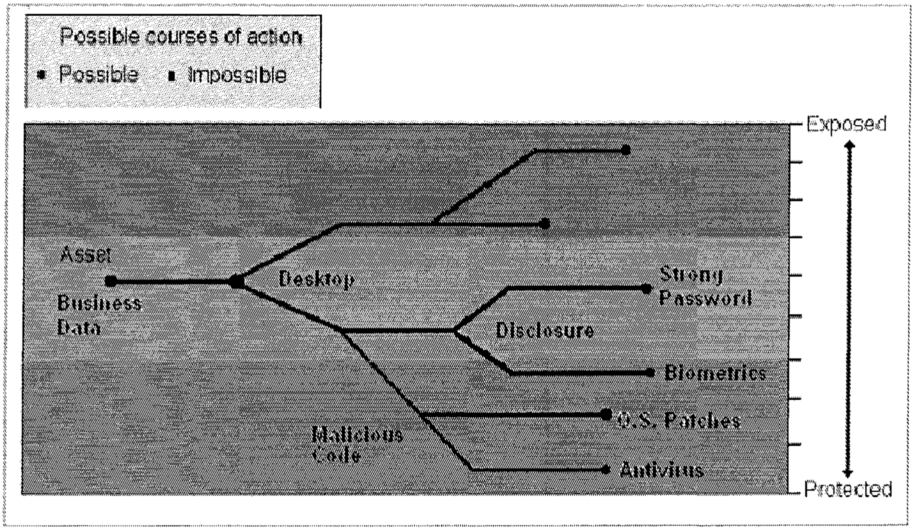

Figure 6. Graphical implementation using threat trees

At the end of each threat tree the tool will produce a threat profile for each asset being assessed.

Table 1. Example of a threat profile

Threat name :	Malicious Code			
Definition:	Software capable of performing an unauthorised function on a target system			
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

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. 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.

If this is done for each asset, at the end there needs to be a selection of only one countermeasure for each possibly by contrasting the importance of the asset with the probability of the risk it is exposed to and the resources required to protect it. All three of these factors will have a different value according to the type and the purpose of the organisation and also different weights. For example the probability of the risk will be a factor affecting the final selection of a countermeasure but will not have as much influence as the importance of the asset so that the security of the asset is not actually "left to luck".

3.2 The financial considerations stage

Once the tool will have constructed a list of possible security solutions relevant to the organisation being assessed and the threats it is exposed to there is a need for a financial consideration of the solutions. This is a general issue for all organisations since it is not good practice to invest more funds on securing an asset than what this asset will actually cost them if compromised. It is however an even bigger issue for SMEs that have a limited budget to start with. Evaluating the solutions from a financial perspective will also help raise managerial awareness since it will make clear to them how costly a loss of an asset will be. This stage will therefore estimate the Return on Investment offered by implementing security solutions, a fundamental step for the methodology to become this way a progression of baseline guidelines and standards but without requiring the level of knowledge RA requires from the user.

The basic aspects that need to be considered in the calculation of the ROI. are the frequency of occurrence of a certain threat multiplied by the damage that it will potentially cause if it occurs (in business terms the Annual Loss Expectancy - ALE) and then this will be compared with the cost of implementing a solution which would prevent this from happening.

$$\frac{A.L.E.}{C.m.C.} = R.O.I. \text{ (where C.m.C. is the Countermeasure Cost)}$$

If the ROI. factor in the result of the calculation is lesser than 1 (e.g. if the ALE is £1000 while the CmC. is £5000 this will give at the result an ROI. factor of 0.2) this will mean that securing the asset is not cost–effective for the organisation. The user will then be presented with certain other solutions. In general when investing in a security solution is not cost-effective the solution would be to either leave the asset unprotected which is not particularly wise or mitigate the risk for example insure the particular asset so the cost of a potential loss is actually transferred to an insurance company. In the case that the recommended solutions are cost-effective but due to budgeting issues the organisation cannot afford to implement all the required countermeasures, some other factors need to be taken in consideration and the solutions that have been proved to be necessary will need to be compared between them to determine which is more important in terms of cost in relation with the probability and frequency that a compromise of this asset will occur. The intention here is also to use the available budget as efficiently as possible. A main issue in this stage that requires future work is an investigation into A way to estimate the "weights" of assets, the costs of countermeasures and all the elements involved in this stage without needing to enter exact numerical values which would make it very time consuming.

3.3 The output stage

Finally the output stage which to be useful to an SME needs to be simple, updatable, produce policy and assist with the implementation (the updatable organisational profile).

It is essential for a tool with the specifications described earlier in this paper to have the flexibility to respond to new security concerns as they arise and to upgrade as new technologies become available (Cisco, 1995) but without the need to perform an analysis from scratch every time a new asset is introduced. Being updatable also makes the methodology more efficient from another perspective; since it will be designed to be performed by individuals with a variety of responsibilities within the organisation and accordingly produce results of a different format, what can happen is for example if it is initially performed by a manager and the output is of a more generic guidance form, a network administrator can then get back and perform it again producing more technical results that will compliment the initial ones.

Following the risk analysis, an organisation should develop a security plan to address those vulnerabilities, that present a high level of risk. The security plan should be implemented by a security policy, which defines how security will be handled. (Loukis et al., 2002). The importance of introducing a precise yet enforceable security policy is that it constitutes a first step towards enhancing a company's security by informing staff on the various aspects of their responsibilities, general use of company resources and explaining how sensitive information must be handled. The policy will also describe in detail the meaning of acceptable use, as well as listing prohibited activities (Danchev, 2003). This makes a security policy an important output of the tool and also of great use to an SME that does not employ a security specialist who would otherwise perform the task. This lack of expertise is the main reason why it is crucial that the methodology also produces a document assisting with the implementation of the countermeasures at the output stage. Figure 7 illustrates the complete block diagram representation of this methodology indicating where it will be necessary for the user to provide with inputs, as well as where there are outputs.

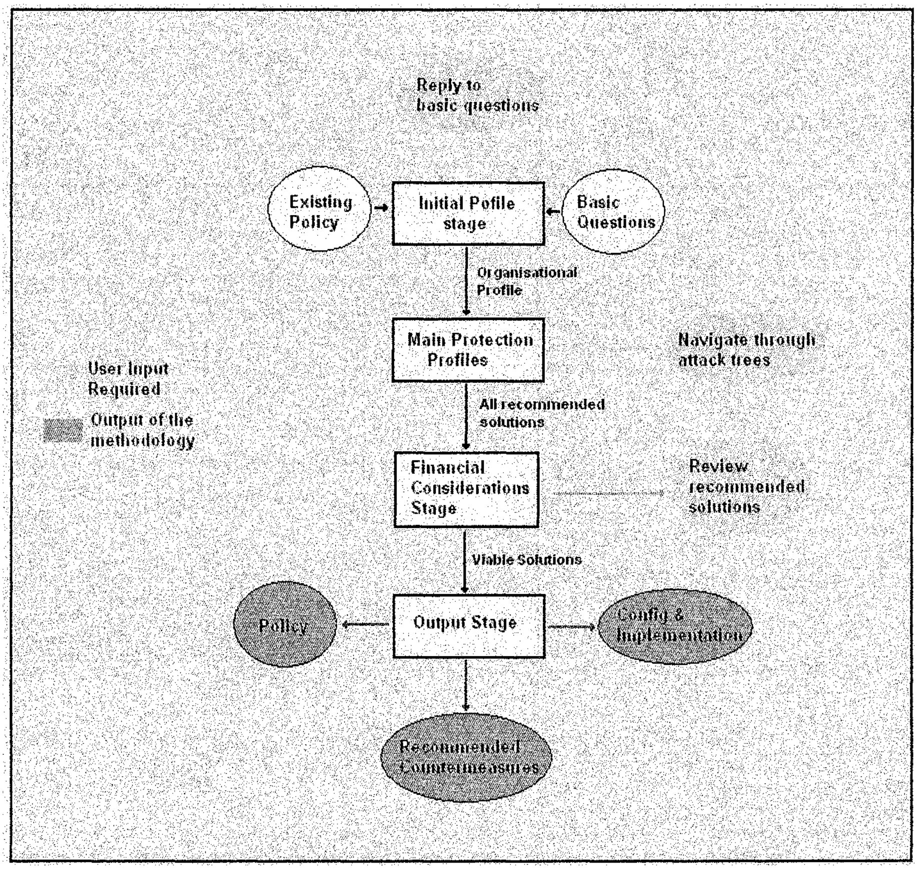

Figure 7. Resulting methodology

4. CONCLUSIONS

This paper has discussed a methodology can be derived that assesses the needs of SMEs. The need for, and requirements of, such a methodology were established from an evaluation of commercially available risk analysis tools for SMEs, as well as from a survey of SME attitudes towards risk analysis (details of which have been presented in previous papers). The discussion presented here was an initial consideration of all the elements that should constitute the methodology. Future work will include a detailed analysis of the components of each part of the methodology, its integration into a tool and subsequent evaluation of its effectiveness (the latter involving representative SME contexts, as well as feedback from security professionals).

5. REFERENCES

Blakely, B., 2002, Consultants can offer remedies to lax SME security, TechRepublic, 6 February 2002, http://techrepublic.com.com/5100-6329-1031090.html

Briney, A. and Prince, F., 2002, 2002 Information Security Magazine Survey, does size matter?, *Information Security Magazine*, September 2002, http://www.infosecuritymag.com/ 2002/sep/2002survey.pdf.

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.

Brake, J., 2003, Small business security needs for the changing face of small business, Micro and Home Business Association, 14 August 2003, http://www.security.iia.net.au/downloads.

Chong, C. K., 2003, Managing Information Security for SMEs. May 2003, Information Technology Standards Committee, http://www.itsc.org.sg/standards_news/2002-05/kinchong-security.ppt.

Cisco Systems Inc., 2005, Cisco IOS Security Architecture, 5 May 1995, http://www.cisco.com/warp/public/614/9.html.

Commoncriteria, 2003, What is a Protection Profile (PP)?, http://www.commoncriteria.org/ protection_profiles/pp.html.

Danchev, D., 2003, Building and implementing a successful information security policy, http://www.windowsecurity.com.

Dimopoulos, V., Furnell, S., Barlow, I. and Lines, B., 2004a, Factors affecting the adoption of IT risk analysis, *Proceedings of the Third European Conference on Information Warfare and Security (ECIW 2004)*, Egham, UK, 28-29 June 2004.

Dimopoulos, V., Furnell, S., Jennex, M. and Kritharas, I., 2004b, Approaches to IT security in small and medium enterprises, *Proceedings of The 2nd Australian Information Security Management Conference 2004 (InfoSec04)*, Perth, Western Australia, 25 November 2004.

Dimopoulos, V. and Furnell, S.M., 2005, Effective IT security for small and medium enterprises, *Proceedings of the 4th Security Conference*, Las Vegas, USA, 30-31 March 2005.

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

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.

Heare, S., 2001, Data center physical security checklist December 2001, SANS, http://www.sans.org/rr/paper.php?id=416.

Hurd, D., 2000, Security checklist for small business, http://www.itsecurity.com/papers/nai.htm.

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, http://news.bbc.co.uk/1/hi/technology/2428983.stm.

Loukis, E., and Spinellis, D., 2002, Information systems security in the Greek public sector, *Information Management and Computer Security,* 2002 http://www.dmst.aueb.gr/dds/pubs/jrnl/2000-IMCS-pubsec/html/ispa.html.

Meyer, K., Schaeffer, S., and Baker, D., 1995, Addressing threats in World Wide Web technology, *11th Annual Computer Security Applications Conference*, IEEE Computer Society Press, pp123–132

NCC, 2000, *Business Information Security Survey 2000.* National Computing Centre, http://www.ncc.co.uk/ncc/.

Shaw, G., 2002, Effective security risk analysis, April 2002, http://www.itsecurity.com/papers/insight2.htm.

Suppiah-Shandre, H., 2002, Security - top priority for all, SME IT Guide, International Data Group, Singapore, February 2002, http://smeit.com.sg.

Symantec, 2005, *Symantec Internet Security Threat Report Trends for July 04–December 04*, Volume VII, March 2005, http://www.symantec.com.