Effective IT Security for Small and Medium Enterprises

Vassilis Dimopoulos and Steven Furnell

Network Research Group, School of Computing, Communications and Electronics,
University of Plymouth, Plymouth, United Kingdom

nrg@plymouth.ac.uk

Abstract

Surveys frequently indicate that a significant percentage of Small and Medium Enterprises (SMEs) do not appropriately assess the threats to which their assets are exposed, even though there are a number of potential methods that may be utilised. This paper discusses the typical characteristics found within SMEs, such as the lack of security awareness, time, funds and expertise, which are serving to impede and deter the adoption of suitable security methods. The discussion proceeds to identify the requirements that a security methodology needs to fulfil in order to be more applicable for these enterprises. This leads to the proposal of a methodology that aims to eliminate the drawbacks of existing solutions, by incorporating elements such as the use of Protection Profiles and calculation of the Return on Investment offered by deploying security countermeasures.

Keywords: IT security, SMEs, Risk Analysis.

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.

Small and medium enterprises (SMEs) probably depend on the Internet more as means of competing with large organisations. This is illustrated by the findings of a recent survey conducted by the authors (Dimopoulos et al 2004), which indicated that the majority of SMEs are connected to the Internet, while all the respondents have indicated some level of dependence on their IT systems. However, being connected on the Internet has introduced a variety of threats, and can leave an organisation’s assets vulnerable to a number of threats - especially if their IT security is not well considered. From the findings of this survey, 31% of the respondents declared that they felt “somewhat dependant” upon IT, while 69% said their business was “totally dependant” upon these systems. 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 this paper investigates some of the fundamental approaches to achieving this. Because of the situation just described, 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?).

This paper discusses the current solutions available to SMEs wishing to secure their IT infrastructure, whether they are being adopted and the drivers behind their adoption as well as how they can be altered in order to become more viable. The focus of this paper is particularly placed upon SMEs because their low budgets mean that they are the ones facing significant IT security problems but having limited solutions available to them.

Steps available to SMEs to strengthen their IT security

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, 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 Figure 1 suggests (with indicative data for the UK derived from the DTI 2002 survey (DTI 2002) the problem is once again concentrated within the small and medium businesses with 14% and 27% respectively.

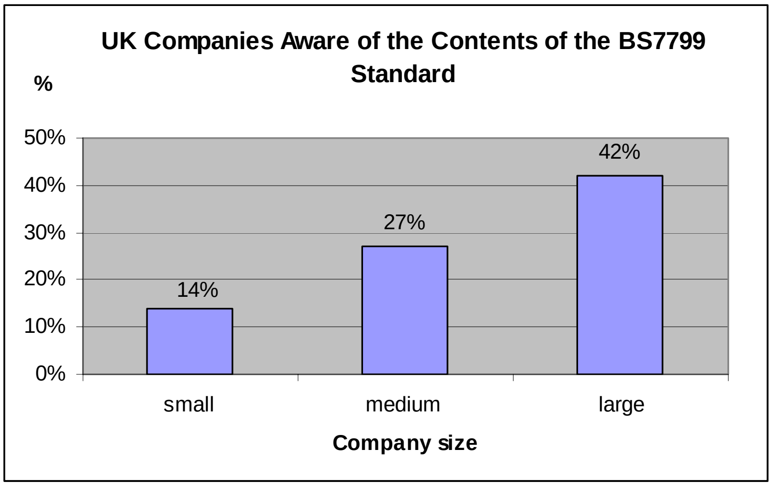

Figure 1: Organisational awareness of guidelines

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 organisations 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.

Another alternative suggestion is for SMEs to implement third-party managed security services (Paraskevas and Buhalis 2002; Spinellis et al. 1999). This involves providing 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. This is possibly the reason why the authors' SME security survey found that this solution is again not being adopted by SMEs, with only about 10% of the respondents

In order to establish the specific requirements of an organisation and thereby determine the applicability of guidelines, a solution available to SMEs is to perform a Risk Analysis. That is "*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*" 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). Risk analysis is therefore considered standard practice for organisations wishing to secure their IT assets and in many cases, like for example with government organisations in the UK, it is mandatory that such an analysis is performed. Once again however, surveys have established that risk analysis is not being adopted by SMEs, 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). More recently, the author's SME security survey found that in the UK 60% of the SMEs questioned have never performed a 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. 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 2, based upon results from 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.

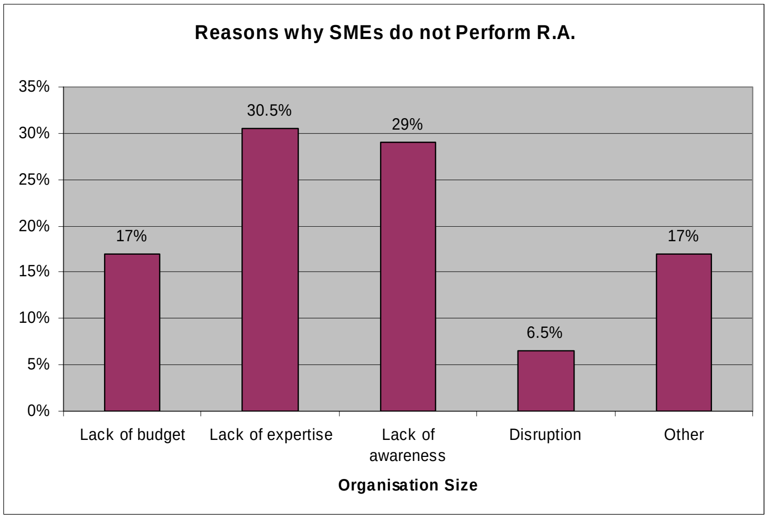

Figure 2: Reasons for not performing risk assessment

It should be noted that the impression conveyed in Figure 2 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.

A further issue is that even those who do perform a risk analysis, still do not perform it as often as they should, this has been confirmed in the authors' survey where all from the respondents that actually perform a risk analysis stated that they only go through this process on an annual basis, while such a process should ideally be performed every time new assets are introduced to the IT configuration, leaving this way assets vulnerable until the next analysis is performed.

The requirements for a new methodology

Table 1 summarizes the reasons why SMEs do not employ any of the aforementioned solutions that are available to them. The background to the majority of these reasons has been discussed in a previous paper (Dimopoulos et al 2004), and this paper takes the investigation a stage further by deriving the requirements for a new methodology by considering the drawbacks related to the existing solutions.

Security method available	Reason why SMEs have poor approach towards security	Requirements for a new methodology
Baseline Guidelines	Lack of awareness, management is not aware of their existence and usefulness	The awareness issue could also impede the new method, if not appropriately promoted.
	Recommendations are too generic, not useful if there is no in-house security expert to configure the suggested countermeasures	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
Outsourcing	Lack of funds dedicated to IT security within SMEs	The methodology should be designed to enable anyone within the organisation who is aware of its requirements and assets to perform an analysis

Risk Analysis	Commercially available RA tools are way too expensive for the SME budget	This investigation does not aim to produce a commercial product
	Lack of an in-house expert who is specifically trained on performing a RA as most tools require	The methodology and resulting product need to be user friendly, easy to use and produce comprehensive and easy to interpret results
	Lack of managerial awareness on the importance of performing a RA.	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 being to assist the management in selecting wisely which assets are worth protecting and how much should be spent on them)
	Length of process, mainly because it is questionnaire based RA is a lengthy process that can result in the disruption of company or individuals activities	By using a "protection profile" approach instead of questionnaires i.e. *"an implementation independent statement of security requirements that is shown to address threats that exist in a specified environment"* (Commoncriteria 2003).
	Even those organisations that do perform a RA, they still do not perform it when necessary, e.g. when a new asset is introduced to the network but instead perform it periodically or even never again.	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 updatable.

Table 1: Requirements as derived from SME characteristics

A further requirement deriving from the fact that SMEs have a restricted budget should be for the methodology to consult the user upon which solutions need to be implemented in order of significance, as well as periodically remind to the management of the ones that have not been implemented yet.

Besides these requirements, ISO 17799 points towards the direction of what an organisation needs to do to establish the appropriate security requirements. More specifically there are three essential steps to be taken:

1. Assess risks to the organisation; this can be fulfilled by performing a thorough and analytical Risk Analysis.

2. Assess legal statutory and contractual requirements that an organisation, trading partners, contractors and service providers have to satisfy;

3. Have a particular set of principles, objectives and requirements for information processing that an organisation has developed to support its operations.

The resulting methodology

For the purpose of comparison with the new methodology proposed here, Figure 3 illustrates the characteristic elements that a Risk Analysis methodology would typically consist of, as described previously in this paper:

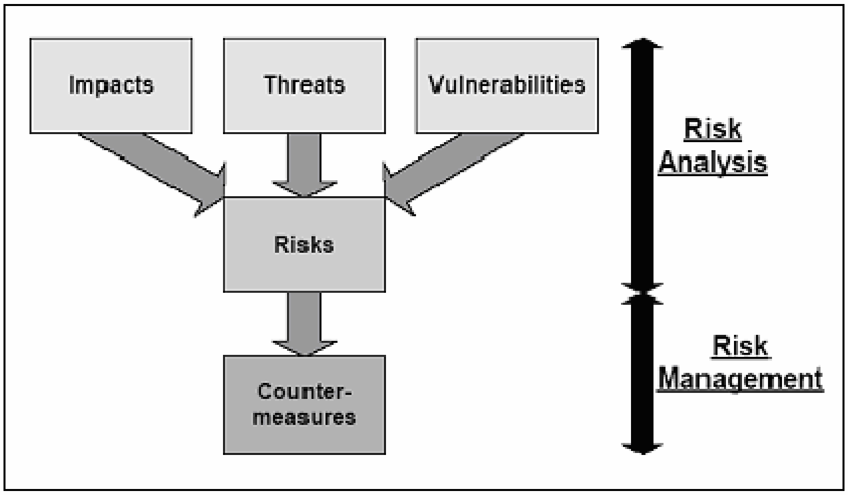

Figure 3: Typical Risk Assessment Process

The proposed new methodology, illustrated in Figure 4, is a progression of typical Risk Analysis methodologies since it introduces the elements previously discussed in table 1 as missing from current approaches to assessing risks.

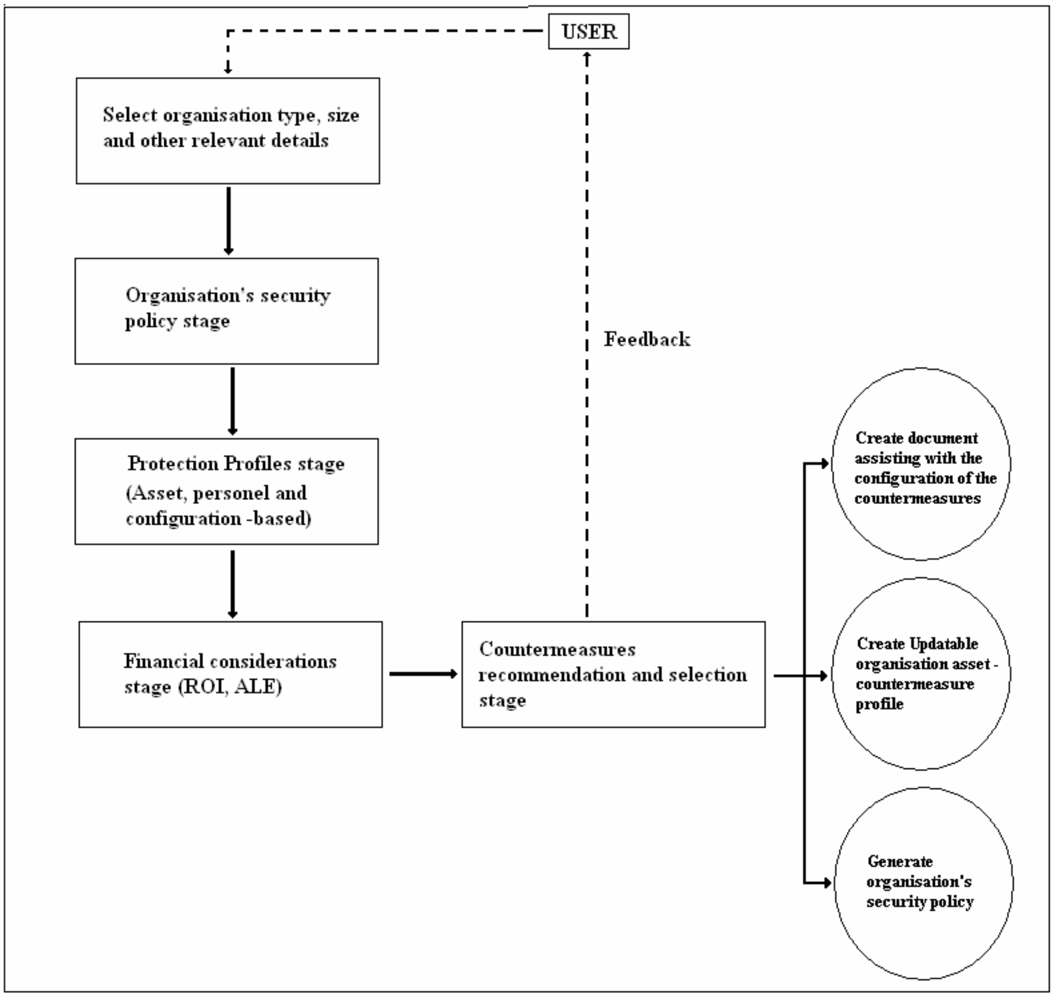
USER
Select organisation type, size and other relevant details
Organisation's security policy stage
Protection Profiles stage (Asset, personel and configuration -based)
Financial considerations stage (ROI, ALE)
Countermeasures recommendation and selection stage
Feedback
Create document assisting with the configuration of the countermeasures
Create Updatable organisation asset - countermeasure profile
Generate organisation's security policy

Figure 4: The proposed new methodology

- **The User:** Can be anyone in the organisation aware of the organisations business assets and purposes

- **Select type and size of organisation**: the aim of this stage is to establish certain elementary characteristics about the organisation being assessed which are however very useful at a baseline level since organisations belonging to the same industry sector and of similar size have a number of basic similar assets and security requirements. Generalising such data will eliminate at a certain extend the need for lengthy questionnaires. Generalising the requirements in such a way will also offer the opportunity to present the organisations with appropriate recommendations derived from relevant legislation (of either a general nature, such as the EU Directive on data protection, or that which is specific to a particular domain, such as HIPAA for healthcare), and which the SME administrator and management might not be aware of.

- **Organisation's security policy stage:** this stage shall target both organisations that have already got a documented security policy, as well as those who do not. with a small number of relevant questions the aim is to establish what is acceptable and what is not in a certain organisation as well as facilitate the creation of a security policy at the end of the methodology.

- **Protection profile stage:** This part aims to eliminate completely the requirement for the user to answer lengthy and time-consuming questionnaires. The protection profiles will be of two types, the asset based ones and the personnel based ones. The first type will aim to assess and record the assets of an organisation in a simple manor while the second one will assess the personnel the organisation is employing and what privileges they need to have within the IT systems. To demonstrate the concept of this, with the intention of being indicative rather than exhaustive, Figure 5 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.

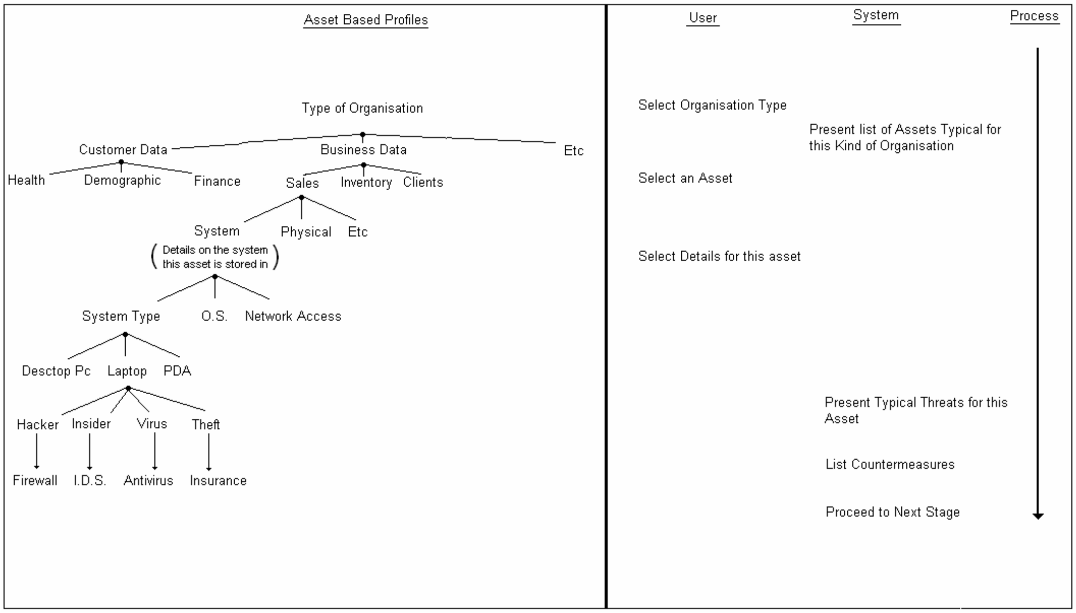

Figure 5: The Asset-Based Protection Profile Approach

- **Financial considerations:** By introducing certain financial elements in the methodology such as the Return on Investment (ROI) offered by security solutions and the Annual Loss Expectancy (ALE) expected by an asset that has not been secured properly, the aim is to assist the user select the countermeasures that are worth implementing from a financial perspective as well as raise the awareness of the management as far as the consequences of a potential compromise are concerned. ROI and ALE need to be expressed in such a way so as not to have to use exact figures as these will vary throughout time, regions etc. therefore qualitative and quantitative approaches need to be combined as the first would be too vague and potentially inaccurate as, for one, prices vary and change, while the second would be too general. i.e. financial estimations of assets to be included but also rate them in terms of how probable it is for an event to occur which would cause such a damage. Thus it could be approached by combining the best out of each one of the approaches. Table 2 gives a general indication of how this could be displayed.

Asset – Backup Server	
Cost to secure this asset	Medium Low (£1000-£2000)
Probability of compromise based on importance of data	Medium High (75%)
Probability of compromise based on existing security measures	High (90%)
Potential compromise cost	Medium (£2000 - £5000)

Table 2: Example of a possible way to express financial data on assets

This could be progressed even more by indicating other assets that would be influenced in case of a compromise of a certain asset as well as other implications in case of compromise such as legal for example.

The system will be required to estimate the value of each asset. This information will be reviewed by the user who will further determine its accuracy. The system will then evaluate, using other knowledge that has been input earlier (like for example the size of the organisation will affect the licensing costs of countermeasures), the added value of the required countermeasures for one asset. Then determine whether it is worth implementing the countermeasures and according to a rating of how much the organisation depends to this asset (based on the type of the organisation primarily) will decide whether it is possible not implementing all of the required countermeasures but only the ones that are cost effective (at this point it is worth requesting from the user a percentage of ROI desired, e.g. value of asset > by 5, 10, 15% from value of countermeasure), the dependency ratings will be firstly based on previous knowledge, i.e. patient records are important for healthcare, website for e-commerce etc. then potentially user should be asked for certain other assets.

- **Countermeasure recommendation and selection stage:** this is the stage at which the system will take into consideration all the data that has been input by the user, as well as the outcomes of the previous stage, and the recommended countermeasures shall be presented to the user. At the bottom level of the protection profiles, “threat profiles” will be presented in order to facilitate the non-security expert user with consciously making the right decisions on which countermeasures need to be implemented plus which the organisation can afford to neglect and at what cost. 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 3 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 3: 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.

- **Document assisting on the configuration of the countermeasures:** taking into account the data that has been entered previously the aim of this stage is to assist the non-expert user with the actual configuration of the selected countermeasures. Thus by considering the size and internal structure of the organisation, the network topology and other appropriate data, the system can make recommendations on various configuration issues such as for example the access rights to certain assets that individuals should be allowed to have according to their position in the organisation

- **Updatable organisation profile:** one of the most important outputs of this methodology will be the updatable profile of the organisation's assets and implemented countermeasures which will assist the user and reduce the time and effort required for a risk analysis by eliminating the requirement to perform an analysis from scratch every time a new asset is introduced. This part of the methodology is also particularly useful in the feedback stage described later on.

- **Generation of an organisations security policy:** will be an essential step for those organisations that have not got a security policy. This stage can also serve in preventing many avoidable incidents by enabling the distribution of the organisation's security policy to the employees (which can also be automated by email for example) to make them aware of the required and acceptable practices within the organisation.

- **Feedback:** this is an essential step through which the user will monitor the effectiveness of the selected security solutions and have the opportunity to alter any selections that are not considered sufficient or useful, the updatable security protection profile should allow such changes and make them more straightforward than having to go through the whole process again.

Conclusions

SMEs are facing a number of challenges that are potentially preventing them from securing their IT infrastructure and assets from the variety of threats that they are exposed to. Having analysed these problems, this paper presented the requirements for a new methodology that should enable organisations of this type to adopt a better approach towards their security. An obstacle that needs to be overcome if this is to happen is how to make them aware of that need at the first place, given that the majority lack the awareness that there is such a need until a major security related event actually occurs.

References

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.

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

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

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

Dimopoulos V, Furnell S, Jennex, M, Kritharas I., (2004) *Approaches to IT Security in Small and Medium Enterprises*, Proceedings of INFOSEC 2004 conference, Perth Australia, November 25-26 2004

Dimopoulos V, Furnell S, Barlow I., Lines B., (2004), *Factors affecting the adoption of IT risk analysis*, Proceedings of the ECIW 2004 conference, Royal Holloway, June 2004

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.

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

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