Effective Information Assurance for SMEs

V.A. Dimopoulos[1], S.M. Furnell[1,2] & N.L. Clarke[1,2]

[1]School of Computing, Communications & Electronics, University of Plymouth,
Drake Circus, Plymouth, United Kingdom.
[2]School of Computer and Information Science, Edith Cowan University,
Perth, Western Australia

Abstract

Evidence suggests that SMEs are frequent victims of security incidents. Even though there are a number of solutions, ranging from baseline guidelines to a detailed Risk Assessment, these are often not employed due to constraints such as lack of budget and related skills. This paper proposes a method specifically tailored to SMEs lacking in-house security expertise. It can assist them in understanding the threats they face, while at the same time presenting appropriate information to enable management to evaluate their organisation's current IT security situation and select appropriate countermeasures.

Keywords:

Risk Management, Risk Assessment, SME, Risk Methodology, Information Assurance

1. Introduction

Every year more and more organisations become networked and depend on IT to conduct business, advertise, and interact with business partners and customers (GAO 2001). A recent survey by the Organisation for Economic Co-operation and Development states that 95% of businesses are connected to the Internet in OECD countries (OECD, 2008).

However, given this reliance upon the Internet and information technology, businesses unfortunately under-estimate the importance of information security. Whilst Enterprise-level organisations have significantly improved their security standing, Small to Medium Enterprises (SMEs) still have significant issues when ensuring appropriate security protection. The *Information Security and Breaches Survey* commissioned by the Department for Business Enterprise and Regulatory Reform (BERR) specifically stated that (BERR, 2008a):

> *"...small businesses continue to bear the brunt of security incidents. While six breaches a year may not seem a lot, for a business of fewer than ten employees, security incidents remain a significant drain on time and resources."*

The survey, which draws respondents from UK companies (of which SMEs make up 99.9% (BERR, 2008b)), continues to illustrate that whilst businesses have begun to implement basic core security controls, their understanding and handle on the problem still falls far short. Key findings include:

- 79% are not aware of the contents of ISO 27001;
- 52% do not carry out any formal security risk assessment;
- 84% of companies do not scan outgoing email for confidential data;
- 78% of companies that had computers stolen have failed to encrypt the hard drive;
- 67% do nothing to prevent confidential data leaving on USB sticks, etc.

The problem faced by SME's has remained the same, with the Symantec Threat Report VIII in 2006 indicating that when talking about attack activity by industry (successful attacks), small businesses come first with 38%, while as far as 'targeted attacks by industry' is concerned, small business comes second behind education. The same survey states that *'Small businesses are less likely to have a well established security infrastructure, making them more vulnerable to attacks'* while at the same time small business personnel are known have an "It would not happen to me" mentality (Diamond, 2004).

Although many security solutions exist, the fact that organizations continue to report major losses, suggests that they are not addressing the issue appropriately. SMEs are often leading in bad security practices while at the same time reporting significant losses from incidents (Jennex and Addo, 2004).

This paper proposes a novel mechanism for providing effective information assurance for SMEs. The paper begins by reviewing the core concepts of risk analysis in section 2 and then proceeds to describe the architecture of the new tool. A discussion of the advantages of the proposed tool is presented in section 4, followed by the conclusions and a discussion of the future directions of the research.

2. Risk Management and Assessment

The process of Risk Analysis is defined as "the assessment of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence" (ISO17799, 2005), and involves the identification of assets that need to be protected and the identification of threats and vulnerabilities related to those assets (Network Working Group, 1997). An illustration of the process is shown in Figure 1.

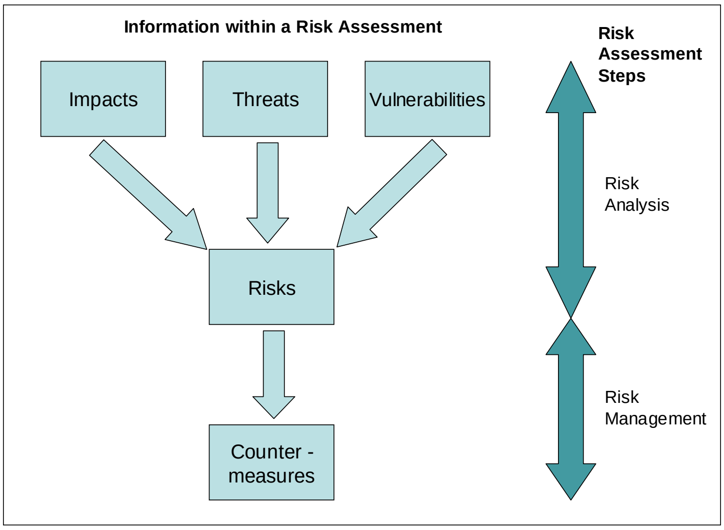


Figure 1: The Risk Assessment process

The steps in the risk assessment process are:

1. Identify **assets**. An asset is anything that is of value to an organisation. Thus it can be anything from physical assets to information assets, even specialised personnel can sometimes be considered as assets to the organisation.

2. Identify and characterise **threats.** Generally speaking, threats are events that could occur and cause loss or damage to the assets that have been identified.

3. Identify **vulnerabilities.** Vulnerabilities are weaknesses that would create a condition allowing the threat to materialise and trigger a loss of assets. This stage of the Risk Assessment attempts to determine how vulnerable the systems are to the identified threats.

4. Analyze the **risks** for a certain asset-threat-vulnerability scenario to occur and determine the potential **losses** that would emerge if it does**.**

5. Identify and select **countermeasures** to reduce risks**.** Countermeasures are security controls which, when put in place, can eliminate, reduce or mitigate the impact of a threat occurrence.

Successfully collecting this data is one of the most important elements of Risk Analysis and a person that is not specialised in practising RA could easily overlook many of these elements or fail to identify their importance. RA is a process intended to be performed by security analysts who have a complete understanding of the IT system's operation and objectives (Gray, 2005), thus being performed by an inexperienced user may lead to an inaccurate analysis. This is also the reason why RA usually involves the input of key personnel in several different positions. There are several methods to perform the information gathering, but the most common as listed by the NIST Risk Management Guide for IT Systems (Stoneburner et al., 2002) involves a combination of the following:

- Using **questionnaires.** This process requires applicable technical and management personnel to fill questionnaires created by the people performing the assessment and which mainly concerns the design and management of the IT system under assessment.

- Performing **on-site interviews.** Such interviews of IT and management personnel, should be performed to allow the RA team to gather information about how the IT system is operated..

- Conducting a **document review.** By reviewing all the security and policy related documents that exist within the organisation, the RA people can gather information regarding system and data criticality and sensitivity as well as the security controls planned and used within the organisation. Use of an **Automated Scanning Tool.** While no automated tool exists that can perform the RA without the need for human input, approaches such as network mapping tools can be used to obtain certain information more rapidly.

As one can infer from this list, not only is some **certain expertise on the** area of RA required but also a considerable amount of time in order to perform these operations.

The common way to perform a RA is by the use of one of the commercially available specialised RA tools. However, many of these tools and methodologies are specifically designed for enterprise organisations and are unfortunately not appropriate to SMEs.

3. Profile-Based Risk Analysis and Management (PRAM)

From the current literature a series of requirements have been identified and can be grouped together to establish four key aspects necessary in RA addressing SMEs:

1. Focus on the characteristics of the SME users. This means it should be easy to use (not get too technical) enabling a non trained user to perform the assessment, provide the necessary assistance to the user. The process should also be relatively short so as not to cause disruption and definitely not require multiple people, thereby making it expand over multiple days. In addition, it should provide the user with the appropriate assistance as is necessary so that an automated tool assists the user with all the selections by indicating relations between assets, threats and controls.

2. Adapt to the organisation being assessed. In contrast to baseline guidelines and RA tools that have the similar approaches in identifying risks, this framework should consider the actual organisational sector, requirements and characteristics as the basis of suggesting and selecting controls. This solution should address organisation-specific issues that the existing solutions do not, such as considering appropriately the size, budget and value of assets to the organisation, considering impact of risks to the organisation, the organisations desired security requirements/levels and based on these suggest appropriate while at the same time cost-effective controls.

3. Produce a comprehensive output. Care should be given to the final output to the user. The framework should provide a concise but comprehensive output report which gives the user the no more than the appropriate information to justify risks and spending to the management, and to assist the user assigned with the task with the setting up of the controls.

4. Manage security weaknesses and risks even after the end of the RA. To be successful, information security solutions need to be managed, not simply deployed (Chong, 2003). Management should not end when the appropriate controls having been suggested but also provide the SME with support afterwards. The framework should allow reporting of the effectiveness of controls and appropriate updating of the organisations profile (created by the assessment) in case there is a change in the assets. It should also include an administrative interface which enables the easy updating of the tools lists of assets, risks and controls to ensure an organisation’s estimated risks and implemented security are always up to date.

3.1. Overview of Methodology

Figure 2 illustrates how the typical RA process needs to be modified to include the elements discussed above and solve the problems prohibiting SMEs from adopting RA.

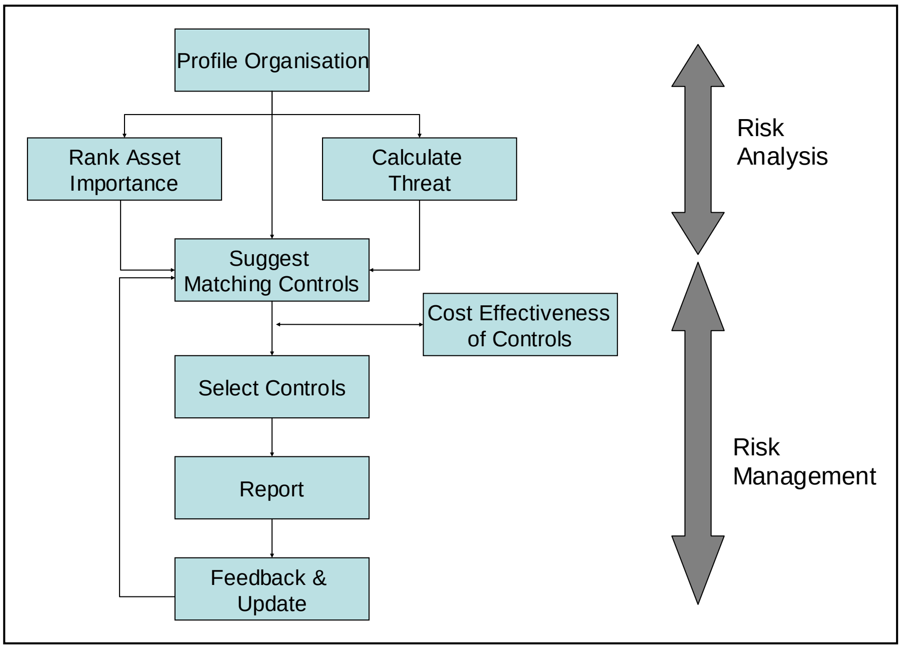


Figure 2: The RA process which suits SME Requirements

The three main elements within a risk analysis methodology are Assets, Risks and Controls. Risk can be the connection between the applications and the controls. Certain applications introduce certain risks and then certain controls reduce these risks. What is then needed is to evaluate how important these applications are to the organisation to establish which needs more protection and what the organisation is spending on security controls to choose the most cost effective solutions from the whole list of controls.

3.1.1. Risk Analysis Phase

This section suggests how the analysis of risks should be approached in the proposed methodology.

- Profile the organisation - Gathering general data on the organisation and the applications that are used within it.

- Rank Asset importance - Rating the importance of the applications selected as existing in order to prioritise the applications/functions.

- Calculate threat - The identified and rated applications are subject to certain threats. Having pre-determined the threats that correspond to the application profiles the user has selected, these threats are awarded points to generate 'threat scores' that quantify how much each threat may affect the organisation.

3.1.2. Risk Management Phase

Following the analysis of the risks, the novel methodology should include these steps in order to manage them.

- Suggest matching controls - The methodology needs to suggest controls to the user. Therefore in this part controls that correspond to the threats the organisation is under while at the same time are appropriate for the selected applications need to be pointed out to the user

- Cost effectiveness of controls - Having established which controls are appropriate for the organisations' needs, a final criterion assisting the user with the selection of the desired best options is the consideration of the cost effectiveness of the controls. The user can here consider which controls are cost-effective judging by the suitability of a control to protect an asset and reduce a threat (presented to the user previously), the importance of this control and the potential losses by the threats it is under versus the cost of implementing the controls.

- Select Controls - Considering this information, this enables the user to select the best options for the SME's limited budget. In this section the methodology should illustrate to the user how selected controls affect the risk levels the organisation is under, as well as how it affects the budget. Once the user is satisfied with the achieved levels for both these, the process is virtually finished and can present an output to the user

- Report - Because the report is addressing SME personnel with all the characteristics identified earlier, presenting a report with the selected controls to the user does not mark the end of the risk management stage. To successfully manage risks, controls need to be implemented correctly therefore sufficient information to realise this should be provided.

- Feedback - Managing the risks does not end at deploying countermeasures either, and as such, a methodology that aims to overcome problems related with existing RA solutions should ensure that, in the absence of a security expert, the organisation receives the appropriate level of assistance even after the controls have been implemented

The idea behind how controls are selected is, at a certain stage, similar to the philosophy used by the widely utilised CRAMM method (CRAMM, 2006). The difference with CRAMM is that after calculating the risk levels the organisation is under, the choice of controls is left to the users' judgement, having presented them with the appropriate data to facilitate the decision (risk levels for the organisation, applications found within ranked in terms of importance and economic considerations such as the Return of Investment (ROI) and Annual Loss Expectancy (ALE).

3.2. PRAM Processes

Both the requirements and the methodology have been presented. However, in order to achieve this desired methodology in practice several process engines need to be designed and their inputs and outputs combined together appropriately. The following five process engines have been used to create a framework that effectively addresses all the requirements.

- Organisation Profiler Engine (OPE)
- Application Importance Rating Engine (AIRE)
- Risk Ranking Engine (RRE)
- Cost Effective Risk Management Engine (CERME)
- Feedback/Update Engine (FUE)

This section will describe the function of these process engines. The databases and other background engines and mathematics used to produce results will not be discussed in detail in this paper.

3.2.1. Organisation Profiler Engine

This engine is required to perform the initial profiling of the organisation. To achieve this, some specific information is required and the input source for this engine is the user. The sector an organisation belongs in is inherently related with the level of threat the organisation is under. To illustrate this, according to the findings of the Symantec survey, the 'Accounting industry' receives 18% of the targeted attacks while at the same time organisations belonging to the arts/media sector only receive 1% of the entire spectrum of attacks. This methodology attempts to first evaluate what levels of threat the organisations are under and therefore it is logical that the first factor in estimating threat will be the inherited risk due to the industry sector an organisation belongs to.

The size of the organisation is required to determine the cost of controls when examining cost effective solutions. Even the simplest of controls is relevant to the organisations' size, from physical controls such as safe doors to software controls such as antivirus, all their costs rise according to the size of the organisation. For the same reasons of evaluating the cost-effectiveness of the possible controls, the IT budget is required at this stage. Furthermore the IT budget, combined with the number of employees and certain surveys that point out the spending of organisations belonging to specific industry sectors per employee, can determine a recommended minimum security spending to the user in case they are not sure what percentage of the budget they should devote to IT security.

Another novel point of this methodology is to consider what the IT security requirements of the organisation are. It has already been discussed that different organisations have different information security requirements and for instance an academic organisation would require easier access for its users in contrast to the more intrusive and need for constant security (e.g. identity authentication) within a military organisation. This methodology, which aims at assisting organisations structure their security, should consider which of the approaches the organisation being assessed desires in order to suggest more appropriate controls later on.

Finally, the main information required from the user here are the applications found within the organisation. The user will be required to declare what applications/types of data and functions can be found within the organisations' IT infrastructure. These introduce the corresponding risks towards the organisation..

What the Profiler engine essentially does is gather specific information about the organisation from the user and then store it in specific locations and order (the organisation profile) so as to enable the following process engines to later on, when required, access and retrieve or update this information. Figure 3 illustrates what information from this first stage is needed by the following stages.

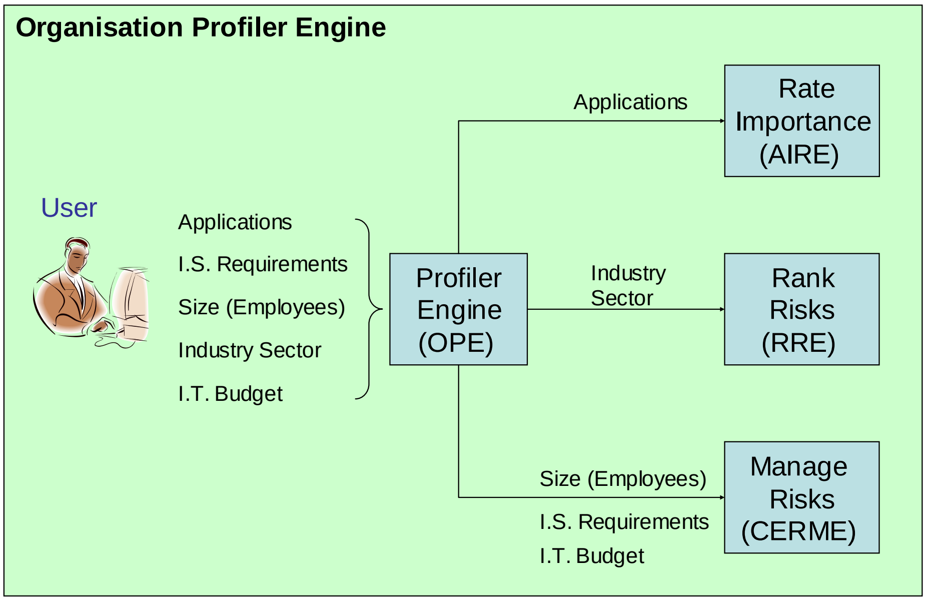


Figure 3: Relationships between Profiler Engine and later stages

To illustrate why this specific data is required from the user, this process engine is the product of reverse engineering, meaning that the information needed by the remaining modules was identified and this engine provides the interface for the framework to acquire this information. The user selected applications that exist within the organisation will at a later stage be required by the AIRE engine so that the applications' importance is rated. The industry sector information is required by the engine that calculates risks to provide an initial input. The size, information security requirements and IT budget information are all considered when selecting controls in the CERME engine. The CERME engine addresses SME requirements of ease of use by not requiring technical details (but instead hiding it in the background i.e. recognising technical information according to applications) and length of process by introducing industry/sector profiling instead of lengthy questionnaires.

3.2.2. Application Importance Rating Engine (AIRE)

The function of this process engine is straightforward: It should first access the 'organisational profile' and retrieve the selected as 'existing applications' and then prompt the user to rate their importance.

There are three essential inputs to the AIRE process engine, all related to each other:

- First there is the input, from the previous engine, of the applications/functions that exist within the organisations IT infrastructure.

- This is complimented with help text. This is predetermined text within the tool that is linked to each application, this process engine retrieves the text that is relevant to the selected applications and provides information on how such applications can be compromised and what the results are. Providing information like this to the user makes the scoring of the applications more accurate as it ensures the user will not misconceive how a compromise of an application and its related assets might affect the organisation.

- The applications and the 'help text' are then presented to the user who is required to consider how a compromise of each application may affect the organisation and therefore rate the importance of each application on the three fields: what the effect of loss of confidentiality could be, what the results of a compromise of integrity, and how the organisation is affected if application availability is lost.

The sole output of this process engine is an updated 'organisational profile' where the users' ratings of applications importance have been added next to each of the previously selected applications. As Figure 4 illustrates, this output provides the basis for two considerations in the subsequent engines.

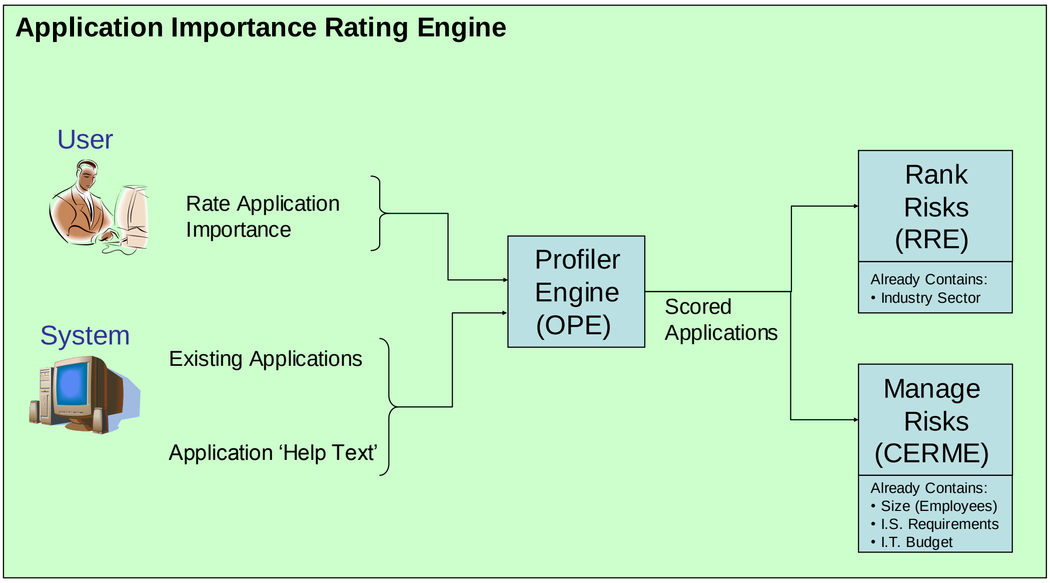


Figure 4: Scoring applications using the AIRE

Firstly it constitutes the second element that determines the level of threat the organisation is under based on predetermined lists of threats that correspond to applications (essentially threats that have been introduce because of the existence of an application). Furthermore the output of the AIRE engine provides one of the inputs to the CERME, the engine that assists in the selection of controls, since one of the criteria, the recommendation of appropriate controls by the framework to the user, is naturally the controls that are suitable and applicable to the available applications requiring protection. The SME requirement addressed by the AIRE engine is to provide assistance to user (partly since at this stage the user is assisted with understanding the importance of applications and rating it more accurately).

3.2.3. Risk Ranking Engine

This process engine (Figure 5) utilises the data output from the two previous engines (industry sector and existing applications, rated in terms of importance to the organisation) combined with survey data to establish how much the organisation is at risk from existing threats. Risk is what connects the analysis with the management.

As discussed earlier, the industry sector that an organisation belongs to may influence the likelihood of a targeted attack. Furthermore, each element within the organisations' IT infrastructure introduces certain threats itself. The new element added here is predetermined values for threat impact. These are initially (since later on in the feedback they are adapted to the organisation according to the users input) taken from survey findings and are a product of the reported annual losses due to threats and the frequency of occurrence of a threat. The reason behind using all this information for estimating the risk levels is that there was a need to adapt these values of risk to the organisation as much as possible since later on it is the basis for selecting controls. Using the traditional values of the effect of a threat and the frequency from surveys would give a threat score for each threat, however, this would be the same for all organisations. The requirement for this methodology was to assess the requirements of different organisations, operating differently and relying more upon different assets (e.g. there is a different dependence, and associated losses, of a bank to customer details than of a university). Therefore the specific risk associated with an industry sector an organisation belongs to was considered and furthermore the threats and potential losses because of the specific applications and types of data the organisation being assessed has that make its environment unique from the rest and especially differentiate it from organisations from different sectors.

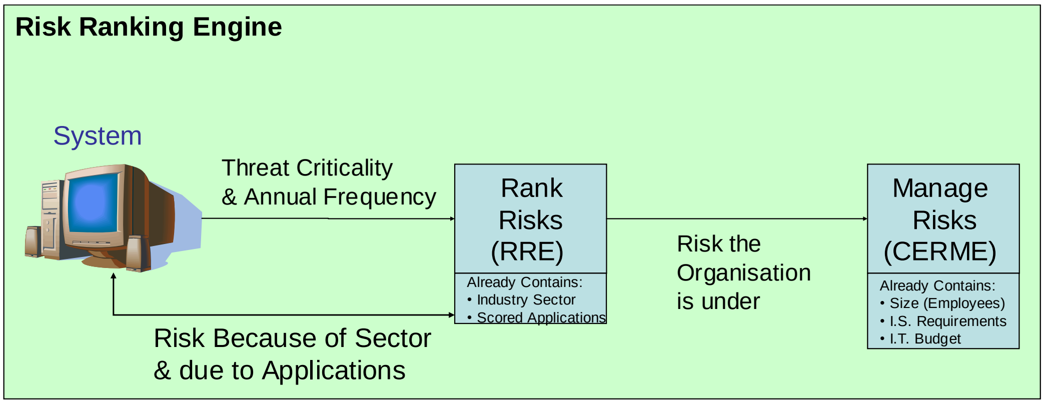


Figure 5: Risk calculation using the RRE

The RRE engine addresses the requirement of SMEs for Risk Impact Analysis and consideration of threats specific to the organisation.

All these factors sum up to produce a threat factor for each threat which is the main function of this module. These threat factors are all progressed to the Risk Management engine which is where they find their primary use.

3.2.4. Cost-Effective Risk Management Engine (CERME)

The previously described process engines mainly constitute the risk analysis part of the framework and gather all the required data and process it so as to feed it to this process engine. The CERME process engine is essentially the risk management part.

This engine (as illustrated in Figure 6) is the 'heart' of the RA framework, its basic function is to gather all the information from the previous modules and transform it to useful information for the user. The information gathered includes, organization budget, size, information security requirements, all available applications and the risk levels the organisation is under. The reasons why all this information has been gathered is clear when looking at the output of this engine.

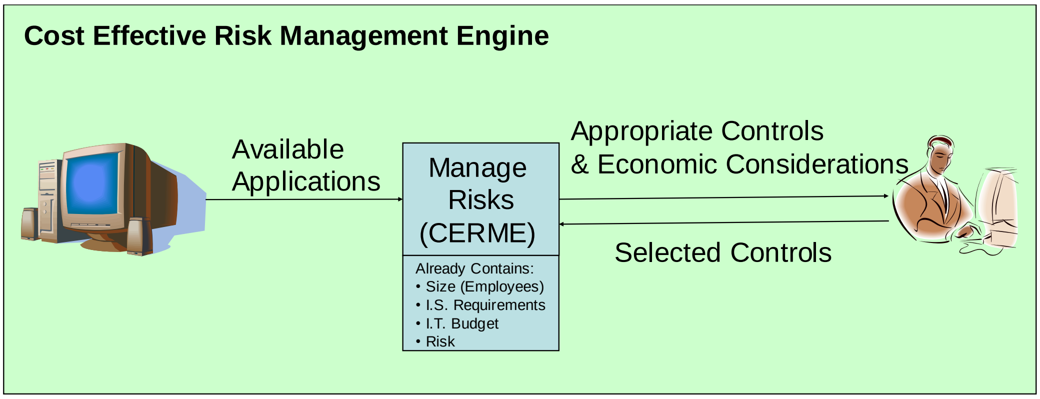


Figure 6: Selecting appropriate controls with the assistance of CERME

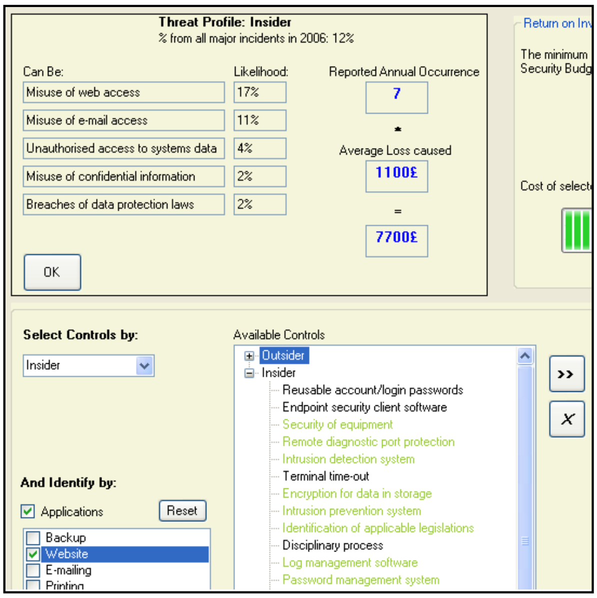
The collected data needs to be presented to the user in a comprehensive way, so as to enable the selection of appropriate controls. In order to achieve this, the data presented to the user is:

The ‘threat profiles’ including Annual Loss Expectancy. To begin with, the user should be made aware of the level of risk the organisation is under and what the likelihood of occurrence is. Also the system should indicate what potential losses may result should these risks occur. It is required that this data is presented in a comprehensive manner in order to be useful, therefore the idea conceived here is to include a graphical display which progresses from green to amber and then red and the threats are illustrated on it being the more into red as the threat increases. Equally when controls are chosen later on the threats can decrease into green according to the effect of the control on each threat.

The framework needs not just to present a list of all available controls but should distinguish and assist the user by presenting those controls that correspond to the available applications and the specific risks the organisation is under. Also before distinguishing those controls the framework should consider what the information security requirements of the organisation are, security or easier access.

Having presented the user with only the potential losses from threats and a list of all the appropriate controls (as indicated in various sources such as ISO 27001 which includes a comprehensive overview of all controls, Muller (2003) that focuses on network security and Garfinkel (1997) focusing on server security), the framework should also present to the user what the cost of the controls are and therefore assist them in selecting the most cost-effective options while at the same time reducing the risks at the desired levels. Having been illustrated this information, an option for the user is also to modify the risk (Meritt, 1998) if the level of risk or the ALE does not justify the required high investment for securing this risk. Addressing an SME user, the framework should avoid leaving the budget allocation entirely up to a user who is not particularly security aware, it will be therefore useful to also provide recommendations of what budget should be spent on security controls by the organisation. Considering the size sector and budget the system can suggest a minimum security spending based on survey data of what other organisations with the same characteristics do.

Therefore the whole concept of the CERME is to display the current risks and risk levels to the user, then suggest what controls, based on statistics, correspond to the organisations requirements by illustrating those that match the specific identified risks and applications. The controls will be ranked also after considering the level of ‘intrusive/hard’ security the organisation requires. This will have enabled the user to select controls that are matching to the organisations characteristics, what the framework should now do is suggest what budget should be devoted to information security controls and allow the user to experiment with different configurations, illustrating each time the cost of controls against the budget, the potential loss because of a threat and the effect the controls have on the existing identified threats. This should enable the user to eventually select the most appropriate controls that reduce the risks to acceptable levels while at the same time not exceed a certain budget or the actual losses from a compromise. This provides the organisations that will adopt this methodology with a form of ROI consideration when selecting security solutions. By establishing ROI data, the management can make more informed decisions regarding which controls to implement, based upon initial cost, but also on the current threat exposure of the organization (Hamilton, 2002). This process as presented in the prototype is illustrated in Figure 7.



Threat Profile: Insider
% from all major incidents in 2006: 12%

Can Be:	Likelihood:
Misuse of web access	17%
Misuse of e-mail access	11%
Unauthorised access to systems data	4%
Misuse of confidential information	2%
Breaches of data protection laws	2%

Reported Annual Occurrence: 7
*
Average Loss caused: 1100£
=
7700£

Select Controls by: Insider

And Identify by:
☑ Applications

☐ Backup
☑ Website
☐ E-mailing
☐ Printing

Available Controls
- Outsider
- Insider
  - Reusable account/login passwords
  - Endpoint security client software
  - Security of equipment
  - Remote diagnostic port protection
  - Intrusion detection system
  - Terminal time-out
  - Encryption for data in storage
  - Intrusion prevention system
  - Identification of applicable legislations
  - Disciplinary process
  - Log management software
  - Password management system

Figure 7: PRAM assists the cost effective selection of controls

3.2.5. Overall Output

It was identified in the requirements that the output of such a framework should be a report with all the necessary elements considering the described characteristics of the users that it addresses and aims to assist.

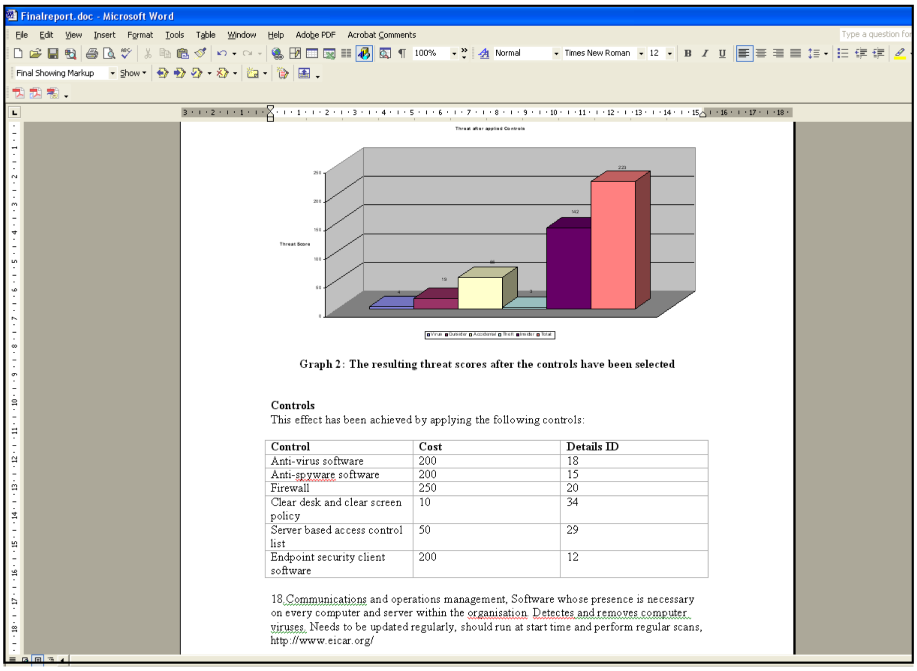
For this reason, the report of this framework includes certain key elements:

- The applications identified as existing within the organisation and a graphical representation of the levels of risk they are under.

- Naturally this is followed by a list of the selected controls, including their costs and another graphical representation of how much the risks have been reduced after the controls have been applied.

- Finally another essential element in such a report is the required explanations on how to set-up, configure and use these controls. This information will be presented to the user as selected links to resources appropriate for the SME target user.

Therefore the SME requirements for a comprehensive output and deployment assistance are addressed by this engine. These are illustrated in Figure 8.



Graph 2: The resulting threat scores after the controls have been selected

Controls

This effect has been achieved by applying the following controls:

Control	Cost	Details ID
Anti-virus software	200	18
Anti-spyware software	200	15
Firewall	250	20
Clear desk and clear screen policy	10	34
Server based access control list	50	29
Endpoint security client software	200	12

18.Communications and operations management, Software whose presence is necessary on every computer and server within the organisation. Detectes and removes computer viruses. Needs to be updated regularly, should run at start time and perform regular scans, http://www.eicar.org/

Figure 8: An aspect of the PRAM Output

3.2.6. Feedback & Update Engine (FUE)

This engine provides an element identified as missing from the existing solutions to the SME that uses this framework. That is the ability to also maintain secure and adapt to situations that were not foreseen or did not even exist when security solutions were initially considered and implemented.

This is a supplementary process engine, as it is not part of the actual RA process and does not need to be run when performing the assessment. It is a “support” engine, only used after the RA should certain specific situations occur, this is why its function shall not be analysed as with the previous process engines but instead both the input and output information is described in brief. The FUE performs three distinct functions that each requires different inputs and produces different outputs. These are:

1. Assess the effectiveness of the implemented controls. In order to check if the implemented controls have been successful, this module requires the user to declare what threats have occurred during the period that the controls have been applied. The controls have been selected according to the risks the organisation is under which in turn are related to survey data on the annual frequency of a risk occurring and the potential losses. Here the framework can estimate annual occurrence rates and losses due to risks which are specific for this organisation. If these exceed the ones that were the basis for the selected controls then the framework should re-assess the situation by calculating this time the risks based on the actual figures provided by the user. This way selected controls can be re-considered based on more realistic data.

2. Reconsider security if the organisation profile is altered, that is if new applications are introduced or old ones removed. Both of these situations can have an effect on security. The first might leave new applications vulnerable or introduce new risks while the latter may leave the organisations with controls in place that are no longer needed. To ensure both these situations are avoided this framework enables the user to modify the applications within the ‘organisation profile’ and reconsider the risks the organisation is under and the selected, required controls. A necessary requirement here is to enable the user to do this without wasting user time and constituting a disruption to the normal operations therefore not requiring the user to go through the entire process from the beginning.

3. Easy update to the framework’s data with new information. This is required for two reasons. Firstly the data used to perform the calculations behind the framework is based on the most recent survey data,

especially on the risks and their likelihood and impact. It would be useful to be able to perform a straightforward update to this information when newer is available. Secondly, there is the need for the framework to always be up to date with available applications and controls since there is no security expert to do this for SMEs. Thus the input here is all the aforementioned data but through an easy to use administrative interface. The primary goal is to enable the update of the framework's data without need rebuilding the whole application, acquiring it, installing it and performing the whole process again.

Even though they were not identified anywhere, this functionality should be included to any tool that claims to offer management of risks, since management does not end when the controls have been deployed. Risks continue to exist even after this and any of these three situations described can have a disastrous effect to an organisations security if they are not considered. What is stressed here is that risk management should be ongoing and occur as threats occur, assets changed or new data becomes available, if instead it is performed periodically it leaves an organisation vulnerable and exposed from the time any of the three happens to the time the re-assessment takes place.

This process engine even enables SMEs that have already deployed security solutions to check the appropriateness of the selected controls by going through the whole framework and then suggesting to this engine certain threats that have occurred and see what improvements they can deploy to the current security. This engine therefore covers the SME requirement for dynamic feedback and update.

4. Discussion

Through using the process engines described in this paper, all the requirements identified as needed from an RA tool were assessed:

1. The methodology included many elements throughout to achieve the first requirement and enable its use by, non-experienced in the sector, users. The use of profiles is the main element which simplifies the process as it eliminates the technical part of an RA and also significantly reduces time needed to perform an assessment. Using applications instead of specific assets as means for identifying threats makes the analysis process suitable for every user with some knowledge of the organisation. Rating the applications importance in terms of importance of C-I-A instead of actual economic value also simplifies the use of the tool and widens the spectrum of personnel within the organisation that are able to perform the analysis. Furthermore, including graphical displays and maximum assistance and backup data to the user throughout the process and particularly with the selection of controls, a stage which includes significant decisions by the user, has reduced the complexity compared to traditional RA.

2. An important addition to this framework that overcomes problems related with existing RA methodologies and their suitability for SMEs is the inclusion of cost effective considerations when selecting controls and the actual suggestion of controls based explicitly on the organisations needs, namely both the exact levels of threats the organisation is under (based on both sector and applications within) as well as the actual applications that can be found within the organisation (and at the same time considering which applications are the most important to the specific organisation).

3. The output report by this framework is short but practical as it includes all the data identified as necessary in the requirements. A graphical illustration of the risk and how it can be reduced with the selected countermeasures (and their cost), in order to raise awareness and justify spending to the management. A description of the nature and operation of the controls, together with external links on how they should be implemented, configured and used, will enable the targeted SME user to select, acquire and deploy security solutions.

4. The feedback and update process engine enables users to re-assess the organisations information security situation if the selected measures have not been successful or if there is a change in the organisational structure, providing real-time support to the SME management that does not employ someone who can otherwise do this.

5. Conclusions

RA is an essential part of organising and implementing effectual and cost-effective IT security. As this research established, SMEs are more in need of such practices than other organisations particularly as their majority does not employ any full-time information security specialists to analyse risks, implement and manage security countermeasures. It is unlikely that organisations will stop facing information security threats, and therefore SMEs will always be in need of such a practice. However, as long as the solutions face the setbacks discussed they will continue not to be adopted by SMEs. The methodology discussed in this paper embraces those characteristics that an SME would require from such a solution. A fully operational RA solution can be produced which can be widely adopted by SMEs leading to improved 'full-time' security, with significant savings both from the selection of cost-effective controls as well as from thoroughly addressing the specific threats an organisation faces.

Future work will seek to evaluate the PRAM prototype with an appropriate SME end-user audience in order to understand and assess the practical implications of the proposed framework.

6. References

BERR. 2008a. "The Annual Survey of Small Businesses' Opinions 2006/07". Department for Business Enterprise and Regulatory Reform (BERR), February 2008. URL: http://www.berr.gov.uk/files/file42727.doc

BERR. 2008b. "The 2008 Information Security & Breaches Survey". Department for Business Enterprise and Regulatory Reform (BERR), URL: http://www.berr.gov.uk/files/file45714.pdf

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 2006.

CRAMM (2006), "Overview: How it works", Insight Consulting 2006, URL: http://www.cramm.com/overview/howitworks.htm, Accessed 17 November 2006

Diamond B., (2004), Why Small Businesses Need to Secure Their Computers (and How to Do it!), URL: http://www.securitydocs.com/library/2106, Accessed 25-11-2006

GAO (2001), "Management Planning Guide for Information Systems Security Auditing", 10 December 2001, URL: http://www.gao.gov/special.pubs/mgmtpln.pdf, Accessed 15 December 2006

Garfinkel S., (1997), "Web Security & Commerce", O'Reilly, June 1997, ISBN: 1-56592-269-7

Gray B., (2005) "The Role of the Security Analyst in the Systems Development Life Cycle", SANS Institute, 12 January 2005, URL: http://www.sans.org/reading_room/whitepapers/awareness/1601.php, Accessed 26-11-2006

Hamilton C., (2002) *"Risk Management and Security"*, RiskWatch, Inc., July 2002 URL: http://www.riskwatch.com/Whitepapers/Risk_Management_and_Security_11-07-02.pdf, Accessed 15 May 2006

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, URL: http://www.irma-international.org/conferences/2004/,

ISO17799 (2005), British Standards Institution. '*Information technology. Code of practice for information security management*. BS I.S.O/IEC 17799:2005. 16 June 2005. ISBN 0 580 46262 5.

Meritt W. J., (1998) "Risk Management", Proceedings of the 1998 National Information Systems Security Conference (NISSC), URL: http://csrc.nist.gov/nissc/1998/proceedings/paperE5.pdf, Accessed 16 December 2006

Muller J. N., (2003), "Network Manager's Handbook", McGraw-Hill, ISBN:0071405674, pp 503-527

Network Working Group (1997) *Site Security Handbook.* RFC 2196, September 1997, URL: http://www.faqs.org/rfcs/rfc2196.html, Accessed 19 December 2006

OECD. 2008. "The Future of the Internet Economy: A Statistical Profile". Organisation for Economic Co-operation and Development, Ministerial Meeting, 17-18 June, 2008.

Stoneburner G., Goguem A., Feringai A., (2002) "N.I.S.T. Special Publication 800-30: Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology", National Institute of Standards and Technology, July 2002, URL: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Symantec, (2006), Symantec Internet Security Threat Report, March 2006, www.symantec.com