Web-based Risk Analysis for SMEs

R. Kunder and N.L Clarke

Centre for Security, Communications and Network Research
Plymouth University, United Kingdom
e-mail: info@cscan.org

Abstract

Information technology has made its present felt everywhere around the world. Organisations too heavily depend on information technology for carrying out their day to day work. Hence it is of utmost importance that the IT infrastructure must be guarded against the various threats that are looming over every other organisations infrastructure. Today, large organisations are taking every step to see to it that their assets are protected from the various threats by doing various risk assessments. Unfortunately but true, various survey and researchers have found out that small and medium enterprises (SME) hardly ever follow security practices. Although there are many solutions available in the market for SME to carry out risk assessment but due to lack of in-house expertise and budget constraints they are unable to carry out such security related assessments since the available tools and other solutions either have high costs or require some expertise to use those solutions.
The purpose of this research is to identify all the problems that act as a hurdle for the SMEs when it comes to performing risk analysis and come up with a novel methodology that can be implemented into a web based risk analysis tool which in return be an useful solution for the SMEs as the tool would be available free of cost, user friendly and most importantly suggest cost effective controls which would ensure the balance between the control implementation cost and also keep the threat levels under check. The designed methodology was then implemented into a working prototype called ERAS (Effective Risk Analysis Solution). The prototype was put under test by involving users from Information security background to check if the tool was successful in achieving the aims with which it was developed. It was clear from the users feedback that the tool was easy to use and understand and also the organisation profiling which is employed by the tool proved to be better than the time consuming questionnaire based approach used by other RA tools and solutions.

Key words

Risk Analysis, SME, Security, Risk Management

1 Introduction

SMEs are organisations where there are less than 250 employees and have an annual turnover of not more than € 50 m (European Commission, 2003). In order to protect the IT infrastructure unlike the SMEs, large organisations spend a considerable amount of money which in turn ensures safety of their critical assets. Whereas SMEs they do not hold such security practise. The managers of the SMEs are least cared about the security of their IT related assets. ISBS(2010) claims that SMEs are more vulnerable to security related attacks and this comes as no surprise because in the same survey it has been stated that on an average only 10% of IT budget is spent by SMEs on their security (ISBS, 2010). The main problem of SMEs when it comes to

risk assessment is the lack of technical expert staff and less amount of budget is available (Kelleher, 2009). As per the ISBS (2012) only 5% of the total SME spent more than 25% of their budget for information security, which is lower than in the year 2010 which was 8%. There are different RA solutions and tools available in the market (e.g. CRAMM, COBRA) but SMEs find it difficult to understand or use them in a more effective manner (Dimopoulous et al., 2003). The problem with using this tool is the lack of skills to interpret the results given in the output by these tools. According to the ISBS (2012) survey, contingency plans were in place by majority of the SMEs when it came to virus infection, staff misuse of information system, confidentiality breach and access control. but the real problem lies in the fact that although there are still cases where contingency plan is in place but not that effective, 23% organisation failed when it came to system failure or data corruption. Hence, this clearly indicates that due to poor selection of controls SMEs still face a problem in having an effective solution to minimise the risk that they face.

Considering the problems of SMEs relating to the Risk analysis this research would focus mainly upon understanding the main root cause of the problem and coming up with a novel methodology which would be best suited for the SMEs and when this methodology would be implemented into a working prototype then it should meet all the requirements of the SMEs so that they can perform risk analysis without much problems..

2 Risk Analysis and SMEs

Risk analysis is a major concern for all organisations, especially small and medium sized enterprises which are particularly sensitive to business risk and competition (Alquier and Lagasse, 2006). According to (McKierna and Morris, 1994), SMEs are characterized with the central role of the owners and multiplicity of duties and close identity with employees. Enterprises in their start-up phase often underestimate risks or even ignore them completely (Smith, 1998). Start-up SMEs usually face a high degree of uncertainties and the necessity to make quick decisions. Henschel (2008) states that risk management is a challenge for SMEs in contrast to larger firm they often lack of the necessary resources, with regard to human capital, data base and specificity of knowledge to perform a standard and structured risk management. Most of SMEs do not have the necessary resources to employ specialists at every position in the firm (Matthews and Scott, 1995). They rather focus on their core business and have generalists for the administration function. In contrast to larger organisations, very few SMEs have one of the owners as a part of the management team. His intuition and experience are important for managing the firm (Dickinson, 2001). Therefore, owner manager in SME is often more responsible for many different tasks and important decisions. Although risk analysis principles are common to all types of enterprises, the manager's risk perception and his attitude towards risk analysis influences the adequacy of the enterprise's risk analysis actions deployed (Ntlhane, 1995). In SMEs, the risk analysis function usually resides with the owner's assessment of threats and opportunities pertaining to the enterprise (Watt, 2007). Implied in SME, risk analysis is the core principle that management focus should be focussed at recognising future uncertainty, deliberating risks, possible manifestations and effects, and formulating plans to address these risks and reduce or eliminate its impact on the enterprise (Ntlhane, 1995). One of the skills

required of entrepreneurs is the ability to identify and analyse risks to ensure that advantage is taken of calculated risks (Watson, 2004).

The fact that a risk is beyond the control of the managers, does not absolve the manager from the need to anticipate the risk, and reducing the impact of the risk occurrence to achieve organisational goals. Managers should be educated in risk management principles, risk handling techniques available and risk control programmes that can be used, but care should be taken in the application of risk management principles, as although risk principles are common to all types of enterprises, the application thereof differs substantially between small and larger enterprises. However, many SMEs practice intuitive risk management when they assess the risk involved in decisions (Ntlhane, 1995). SMEs do not tend to use special techniques to optimize significant risks. Empirical studies show that the attitudes of SMEs towards risks and their risk assessment differ significant from that of large firms.

2.1 Existing RA solutions for SMEs in the market

There are many numbers of tools and standard baseline guidelines available for carrying out risk analysis specially designed for SMEs. Few of the solutions that have been selected for this research purpose are discussed below.

The OCTAVE-S which is specially developed for the SMEs but it is more of a self assessed, streamlined process and produces similar results and also it includes only a limited exploration of the computing infrastructure (CERT, 2008). Small and Medium sized companies do not have the ability to run or interpret the results of vulnerability tools all by themselves due to lack of expertise hence OCTAVE-S is not suited for SMEs. Speaking about COBRA then, it is a process that takes the risk assessment more as business issue rather than a technical one. The tools are not available for free downloads. Theses tools help in self-assessment of the risks (Riskworld, 2011). SMEs refrain from using this tool due to its cost and it also takes long time to fill up the questionnaire thus increasing the analysis time. (Dimopoulous, 2007).

There are other solutions available like the ISO/IEC 27002:2005 Code of Practice which is intended to provide a framework for international best practice in information security management (IS027002, 2012) and NIST Special Publication (SP) 800-30, Risk Management Guide for Information Technology Systems is the US Federal Government's standard. This methodology is designed primarily to be used for qualitative approach, it relies on the skill set and experience of the security analysts working with system owners, and technical experts to thoroughly identify, evaluate and manage risk in IT systems (NIST SP 800-30, 2011). But again both these standards require some amount of expertise to understand and apply the same to the organisation. Hence SMEs abstain from using these solutions too.

3 The Prototype: Effective Risk Analysis Solution (ERAS)

After researching on the problems of the SMEs the main obstacles in the path of effective risk analysis were determined and using this, a new methodology was

deigned to suit the SME risk analysis process. The new methodology would take care of the following issues.

- The process of new methodology would be short in length.
- The tool would be simple to use and understand.
- The tool shall be hosted over internet thus it would be freely available to the users.
- Proper assistance would be provided while the user selects assets and controls so as to help the user to get a proper understanding about the relation between the assets, threats and the controls that they need to apply.
- Cost effective controls would be suggested to maintain a balance between the control implementation cost and the threat value level.
- The new methodology should be such that even after RA is finished the tool should give further support in terms of determining effectiveness of controls and allow the user to make further changes.

3.1 Overview of methodology

As shown in figure 1 instead of using a traditional questionnaire based approach here the tool would make use of the organisation based profiling. The organisational profile evaluation table would be used to identify their risk context. The organisational risk context is derived from the business and the external environment of an organisation and can be divided into four risk areas: Legal and Regulatory, Reputation and Customer Confidence, Productivity, and Financial Stability (ENISA, 2007). Figure 2 shows you the prototypes user interface which is implemented using the current methodology. Once the organisation profile is selected (Figure 2.) then the controls are mapped corresponding to the assets identified. The controls are of two types namely, Organisational based controls and Asset based controls.

- Organisational based control cards are that which contain controls applicable to the organization horizontally and are concerned with practices and management procedures.
- Asset based control cards that are applicable to critical assets and are asset-category-specific.

As shown in the figure 2 below data is asked from the user related to the four risk areas and hence from the input of the user the profile is decided. Each area is classified in three classes: High, Medium and Low (corresponding to Medium size, Small size and SOHO respectively). These classes express quantitative criteria for the organisation in question with regard to the risk area and help identify a risk level. "As a rule of thumb the highest risk identified in a risk class defines the overall business risk profile. A high risk carried in the financial risk class marks a high risk profile. Equally, a medium risk leads to a medium risk profile and low risks to low risk profiles" (ENISA, 2007). For example a low risk carried in the reputation and confidence, in legal and regulatory compliance and productivity but a high risk in financial stability risk class concludes to a high organization risk profile. Organisational based profiling (risk profiling) should be considered as a very important decision which subsequently leads to the risk related selection of assets and their protection via control.

Once the organisation profile is selected then users selects the corresponding organisational based controls.

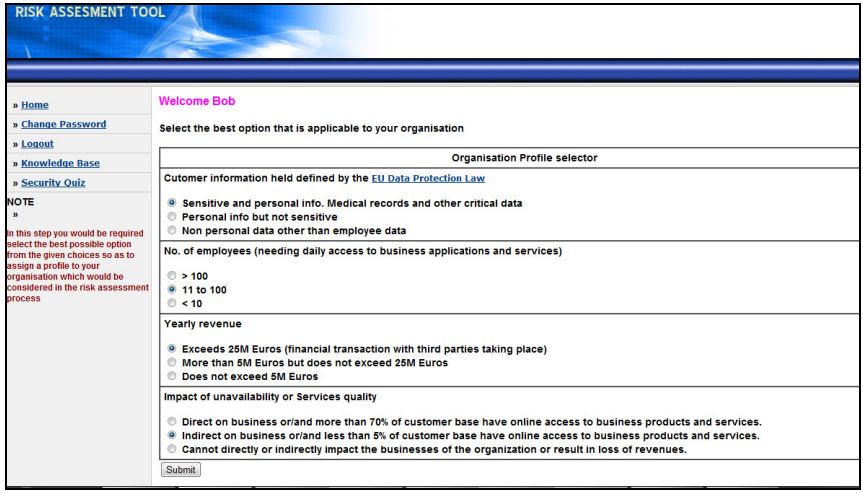

Figure 1: Selection of organisation profile

After choosing the applicable assets the user is then presented with the asset based controls for each asset and also the user has to rank the assets as per their importance (Figure 3). The user selects and submits the controls along with the asset ranking to the system.

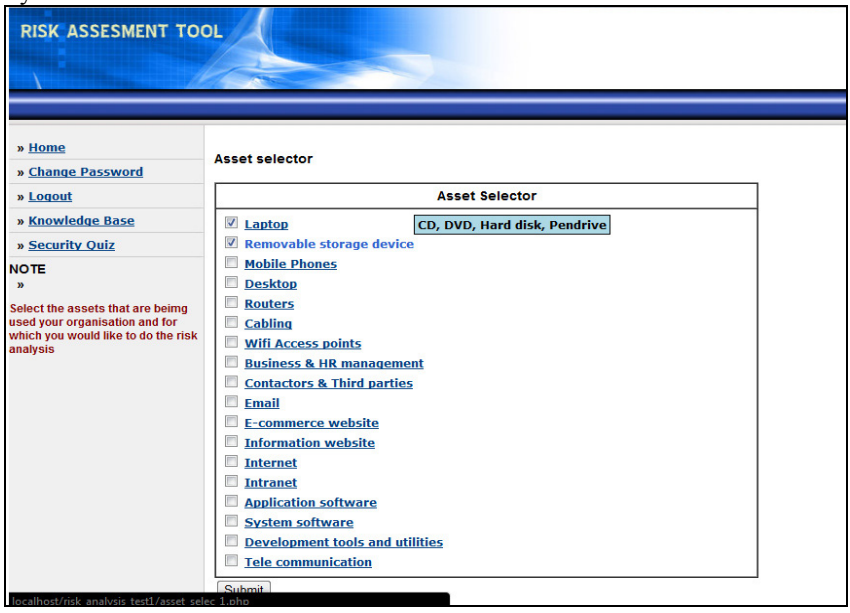

Figure 2: Asset selector and ranking

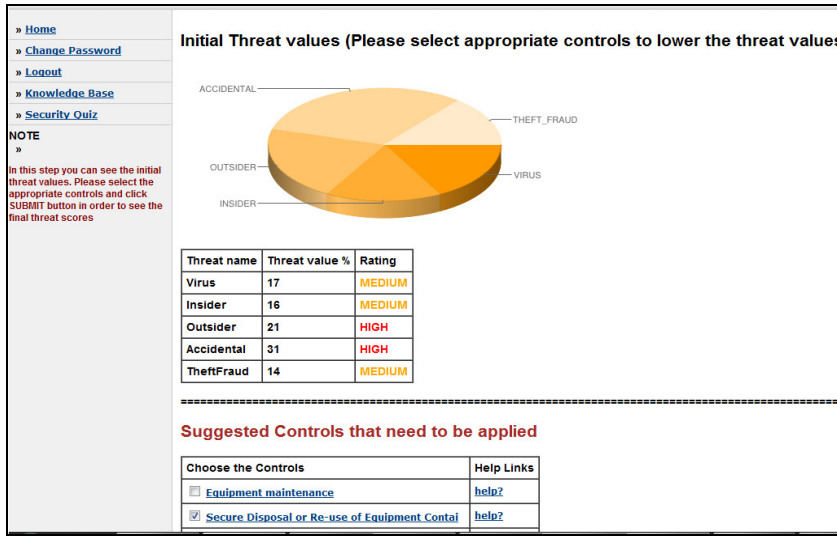

Figure 3: Initial threat value display along with suggested controls

After this step the initial threat values for the organisation are then displayed. This threat level can be brought under control by selecting the specific cost effective controls that have been displayed to the user. The user can select as much controls as possible until the threat level has decreased to a safe level. This calculation is done using the control effect value that is associated with each control. This value is used as a diving factor either the threat value. Thus as long as control specific to a threat are selected the particular threat value would decrease. Eventually after we have selected the controls keeping in mind the budget of the organisation, we get the final threat value. At present the prototype is not considering the economical values like ROI and ALE,

3.2 Evaluation

The prototype was put under test to investigate whether the aim with which the development of prototype was achieved to what extent. The main purpose of taking feedback from selected users was to get feedback on the tools ease of use, how effective and useful is the output of the tool and the overall functioning and process flow of the tool. Participants who had some background in information security or may be working for an SME carried out the evaluation. The feedback obtained revealed that ERAS prototype's user interface was easy to use and even a person who is not trained in RA could easily use it. The organisation profiling approach was considered far better than using the tradition time consuming questionnaire approach. More users would try it as the tool would be available free of cost. However there is still room for improvement as the users desire more detailed and descriptive output and also more should be included in the output so as to make it more descriptive. Also more informational links and help text should be provided which would help in raising the security awareness among the users of the tool.

4 Conclusion

The methodology discussed above in the research is very easy to understand and also it is not time consuming. Help links are provided for every control in the prototype so as to help the user to implement those controls. Future work on this prototype would be to include a feedback system which would assist the user even after the assessment is over by suggesting controls that might still be required to implement to reduce certain threats.

5 References

Alquier, B. and Lagasse, T. (2006). *Risk management in small- and medium-sized enterprises*. Prod. P. & C., 17(3): 273-282

CERT(2008) OCTAVE [WWW] CERT. Available from: http://www.cert.org/octave/ [Accessed 19/01/12].

Dickinson, G. (2001) Enterprises risk management; its origins and conceptual foundation, The Geneva Papers of Risk and Insurance, 26(3), pp. 360-366.

Dimopoulos, V., Furnell, s.m., and Barlow, I.M. (2003).Considering IT Risk Analysis in Small and Medium Enterprises. Proceedings of the 1st Australian Information Security Management Conference 2003 (InfoSec03), Perth, Australia, 24 November 2003

ENISA (2007), *ENISA deliverable: Information Package for SMEs* [WWW]. Available from: http://www.enisa.europa.eu/activities/risk-management [Accessed 29/05/2012].

European Commission (2003), *COMMISSION RECOMMENDATION of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises* [WWW] Accessed from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:EN:PDF [Accessed 12/01/2012].

Henschel, T. (2008), "Risk management practice for SMEs; Evaluation and implementation effective risk management system", Berlin Erich Schmidt, 2008.

ISBS (2010) *Information Security Breaches Survey 2010, April 2010*. Technical Ed. PricewaterhouseCoopers LLP.

ISBS (2012) *Information Security Breaches Survey 2012, April 2012*. Technical Ed. PricewaterhouseCoopers LLP.

ISO27002 (2012) *ISO/IEC 27002* [WWW]. Available from: http://www.iso.org [Accessed 30/05/2012].

Kelleher, D. (2009) SME security: SME mindset must change [WWW]. Available from : http://www.scmagazineus.com/sme-security-sme-mindset-must-change/article/136052/ [Accessed 11/01/12].

Matthews, C.H., Scott, S.G. (1995) Uncertainty and planning in small and entrepreneurial firms; an empirical assessment. Journal of Small Business Management, 33(4), pp. 34-52.

McKieranan, P., Morris, C. (1999) Strategic planning and financial performance in UK SMEs: Does formality matter. British Journal of Management, 5, pp. 31-41.

NIST SP 800-30(2011) *Guide for Conducting Risk Assessments.* United States: Joint Task Force Transformation Initiative, SP800-30.

Ntlhane, K.E. (1995). *The application of risk management principles to smaller enterprises*. Research report (Masters of Business Administration in the Faculty of Management), University of the Witwatersrand.

Smith, J.A. (1998) Strategies for startups. Long Range Planning, 31(6), pp. 857-872.

Watson, G.E.H. (2004). *A situational analysis of entrepreneurship mentors in South Africa.* Dissertation submitted (Masters of Commerce in Business Management), University of South Africa.

Watt, J. (2007). *Strategic risk management for small businesses*. In: Reuvid, J. (ed.). *Managing Business Risk.* 2nd ed. a practical guide to protecting your business. London – Philadelphia: Kogan Page.