RISK MANAGEMENT: SMALL AND MEDIUM ENTERPRISES

Upasna Saluja and Norbik Bashah Idris

Centre for Advanced Software Engineering (CASE), University of Technology Malaysia (UTM),
Jalan Semarak, 54100 Kuala Lumpur, Malaysia
upasnasaluja@gmail.com , norbik@citycampus.utm.my

ABSTRACT

It is information security that ensures on going confidentiality, integrity and availability of information. Information security risk management assures correct protection of assets from the relevant range of risks through the information security risk management process which typically begins with a risk assessment. Due to the recognition of the importance of information security risk management, formal standards and guidelines have been released that detail a base process. However, there is no "widely accepted" optimum risk assessment methodology for Small and Medium Enterprises. This paper talks about the available Risk Assessment methodologies along with the specific constraints of SMEs. A risk assessment methodology for Small and Medium Enterprises (SMEs) has been proposed. The proposed risk assessment methodology helps quantify the security gaps between the assessed and the desired assurance levels. Relative Risk Benchmarking (RRB) proposed in this paper is an open and transparent benchmark to measure relative risks faced by any organization. Today risks faced by an SME; are diverse and varied; and are interrelated with each other as well as to the overall risk (and thereby security posture). A risk-management framework based on RRB would bring out the relative importance of different elements of Information Security to the business with respect to the overall status of the information security of an enterprise. Output of the RA process based on RRB shall provide necessary guidance for enterprise security managers for allocation of resources.

Keywords: *Information Security, SME, Risk, Security, Enterprise Risk, Risk Analysis, Risk Management*

1. INTRODUCTION

Information is a key asset in today's knowledge based economy. Organizations across industry sectors are embracing IT to improve operational efficiency and automate routine tasks. The increased reliance on IT systems brings with it the inherent security risk to information assets of organizations. The term 'risk' refers to the threat of loss of an organizational asset, incorporating the asset's value, its vulnerabilities and the range of threats to that asset measured in terms of probability and impact (ASIS International, 2002; Visintine, 2003; Frosdick, 1997). Traditionally, organizations have sought to minimize security risk through implementing preventive, detective and corrective controls. Implementation of such controls reduces risk to a point; however, security risk can never be eliminated completely.

The element of security risk is dependent on numerous factors and tends to be dynamic with reference to time, organizational growth/structure, location, type of business/role, complexity of network, information systems etc.

Organizations are realizing that "you can't manage what you can't measure." For budgeting and ROI evaluation there is an increasing focus on measuring security effectiveness. Driving the trend is the fact that security budgets have been rising by 20 % annually over the past couple of years.

Despite increased awareness and the recommendations for improvement by Governments in advanced nations, key areas of security management especially for small enterprises continue to receive precious little attention. The lack of formalized security metrics for SMEs impairs the ability of security stakeholders in such organizations to effectively measure and manage security.

This paper looks at Risk Assessment from the perspective of security managers in small and medium enterprises. It highlights the limitations and challenges faced by SMEs in measuring and consequently managing information security risks. It goes on to propose a methodology for relative risk benchmarking through application of statistics. Besides risk assessment this would help in resource prioritization.

2. RISK ASSESSMENT TODAY

Information security risk management is the process by which an organization's information assets are valued, vulnerabilities and threats are identified and the implementation and monitoring of the measures put in place to protect these assets (Whitman & Mattord, 2005). The information security risk assessment process is a staged approach within information security risk management that aims to identify and prioritize information assets, the specific threats that an organization faces the chance of these threats occurring and the impacts on the business.

A number of risk analysis and management methods have been proposed. Currently there exists security management "framework / guidelines" for large organizations however the development of specific risk analysis / management methodology to help small and medium enterprises has not received much attention. A few existing guidelines (to be applied manually) or interactive software packages are listed below:

- The Software Engineering Institute (SEI), a federally funded research and development center sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University has introduced the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), a framework for identifying and managing information security risks.

- CRAMM is based on the UK Government's preferred risk assessment methodology. CRAMM by Siemens provides an approach to both technical (e.g. IT hardware and software) and non-technical (e.g. physical and human) aspects of security. CRAMM includes a comprehensive range of risk assessment tools that are fully compliant with BS7799.

- NIST has provided a free software program called ASSET to document and manage the risk assessment process.

- Risk Management Guide for Information Technology Systems (SP 800-30) issued by US National Institute of Standards and Technology in July 2002 provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems.

- In July 2003 NIST published the NIST Special Publication 800-55 Security Metrics Guide for Information Technology Systems that highlights that the requirement to measure IT security performance is driven by regulatory, financial, and organizational reasons.

- Australia and New Zealand have come up with a joint standard AS/NZS 4360:2004**:** Risk management. The standard provides a generic guide for managing risk. It may be applied to a wide range of activities or operations of any public, private or community enterprise, or group.

- Information Security Management Standards
  - COBIT
  - ISO 27001

- "The Common Sense Guide to Cyber Security for Small Businesses, Recommended Actions for Information Security", 1st Edition – March 2004 from Internet Security Alliance lays down their recommended "Best Practices – A Twelve Step Program to Cyber Security". It argues that one likely reason that smaller enterprises are being hurt by such a dramatically higher percentage than larger firms is that many larger companies, with greater economies of scale, are making systematic attempts to manage the risk to their information systems. For this they use large information technology departments that small businesses cannot afford.

- "Homeland Security: Tools for Small Business" workbook that was compiled by Risk Management Small Business Development Center, USA in September 2004 argues that there are still far too many small businesses that have unprotected computer systems. It stresses that security for (your) business should be built in layers, it should be appropriate for the location and type of business and it should be in the form of a written plan. Small businesses will have many variables that are unique to SMEs that the security assessment needs to cover.

3. NEED FOR RELATIVE RISK MEASUREMENT

Risk assessment is the first logical step in an organization's quest to manage risk. Organizations are driven to measure and manage information risks due to regulatory, financial, and organizational reasons.

Small and Medium enterprises are faced with the problem of managing their security without the benefit of having dedicated security managers in house or budgets to outsource the same to external experts. Today a SME cannot just turn to some defined standards, guidelines or processes and in a self facilitating manner measure their levels of security and implement requisite measures to mitigate risks associated with it. The guidelines or standards, where they exist, typically tend to address large enterprises or Government agencies with a suitable organizational framework that enables and supports the security management framework around which the guidelines are based. Such security management framework may be virtually a single person in a SME!

The million dollar question in front of SME is "How do I prioritize my resource (budget and people) allocation to mitigate the different risks my organization is faced with?" The constraints / challenges faced by SMEs are enumerated below:

3.1 UNIQUE SECURITY REQUIREMENTS

Assessment mechanism for SMEs needs to address specific security requirements of SMEs rather than generic security requirements oriented towards large enterprises. The risk assessment methodology needs to be custom built for the SMEs from the scratch rather than mere adoption of assessment methodology that was developed for large enterprises; simple and less resource intensive for an SME to handle; and they must cover all elements of security.

3.2 RESOURCE LIMITATIONS

Often, organizations do not have the funding and personnel resources necessary to mitigate every risk identified in the Risk Assessment. Moreover, not all weaknesses identified in risk assessments carry the same risk levels. By having a mechanism for relative risk benchmarking organizations can ensure that high impact weaknesses receive immediate funding and personnel resources to mitigate risks. Organizations can ensure that they factor in interdependence between impacts of risks under different security attributes. E.g. issues that impact physical security could have cascading effects on information protection. With the reality of resource limitations, it is essential that high "overall" (including individual and related impact) impact weaknesses receive adequate attention.

3.3 DIVERSITY AND NUMBER OF RISKS

There are numerous types of risks, affecting various business functions. Due to constraints it becomes difficult for the organization to identify and understand risks and thereafter prioritize resources based on relative importance or severity of risks. A key element in prioritization of resources towards security controls and mitigation plans is firstly, understanding the individual impact of each element of risk. For example as a security manager of the SME, to begin with I would need to evaluate risks faced by the networks, the physical infrastructure, and operational framework individually.

Secondly, interdependence of different elements of risks (today risks faced by an enterprise are diverse and too many) needs to be understood before any mitigation plan can be worked out. Since risks and their impacts are interrelated and the result one gets out of managing each of these risks is not independent of each other. As per the report "Convergent Security Risks in Physical Security Systems and IT Infrastructures" commissioned by The Alliance for Enterprise Security Risk Management (AESRM), a coalition formed in February 2005 by ASIS International (ASIS), Information Systems Security Association (ISSA) and ISACA, special systems and devices are increasingly being deployed in a manner that exposes them to external access from the Internet. Perpetrators who gain unauthorized access to these systems and devices may be able to use them to launch attacks on other resources within the network, some of which may be business-critical.

Lastly, the degree of impact of each element on the overall risk profile (or security posture) must be understood before a security manager can allocate resources for risk mitigation. E.g. as a security manager I need to know the severity of impact (what could be the extent of my losses) of lack of Access Control Device on my overall security posture before I take a decision on whether I will spend $4000 on it.

For establishing information security of any organization/enterprise/institution, it is crucial to identify the impact of different elements of information security on the overall information security posture of an enterprise. This can play an important role not only in resource allocation but also for budget allocation.

Relative Risk Benchmarking (RRB) could help in determining these interrelations between different risk elements, understanding relative importance of impacts that each risk element could have on the overall security posture (e.g. determine how the Network Security impacts the overall security posture) and thus provide guidance on which risks need what kind of attention and resources.

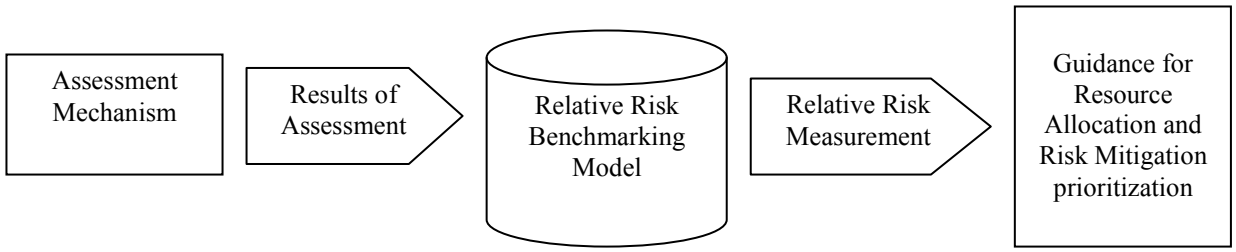

Figure 1: RRB model

4. MODEL FOR RELATIVE RISK BENCHMARKING

It is imperative that the assessment mechanism (which maybe in the form of a questionnaire, checklist or such other evaluation method) for risk assessment be based on a comprehensive and complete knowledgebase, which caters for SMEs specific security requirements. The security elements could include but not be limited to Network Security, Physical Security, Administrative Security and Telecommunication Security. The outputs of the assessment mechanism for each separate risk element are used as the input for further derivation of the Relative Risk Benchmark.

The information security status (s1, s2, s3) of the organization in terms of each element of information security using statistical measures and methods is linked relative to each other and to the overall security posture of the organization. For example, we can consider s1 as physical security, s2 as network security and s3 as operational security. "S" represents the overall information security status of the organization.

Measures of associations between overall information security status of the enterprise and the different elements are calculated and linked statistically. Drawing from the much established field of financial risk management the methodology based on a mathematical function, models the relationship between the elements of security vis-à-vis the overall security posture of the enterprise, thus making the RA process more quantitative than previously possible.

Such a security measurement framework that caters for the specific requirements of the SMEs and is based on relative risk benchmarking would give enterprises a basis for quantifiable security measurement and assessment that would in turn enable them to make business decisions about resource allocation and prioritization (for managing security risks). Security managers can better manage budgets based on the relative importance of different elements of Information Security to the business which can lead to a sort of cost / benefit analysis regarding various controls & measures. In other words relative risk benchmark could help lay down the basis of a sound framework for an Information Security Management System (ISMS) particularly for SMEs.

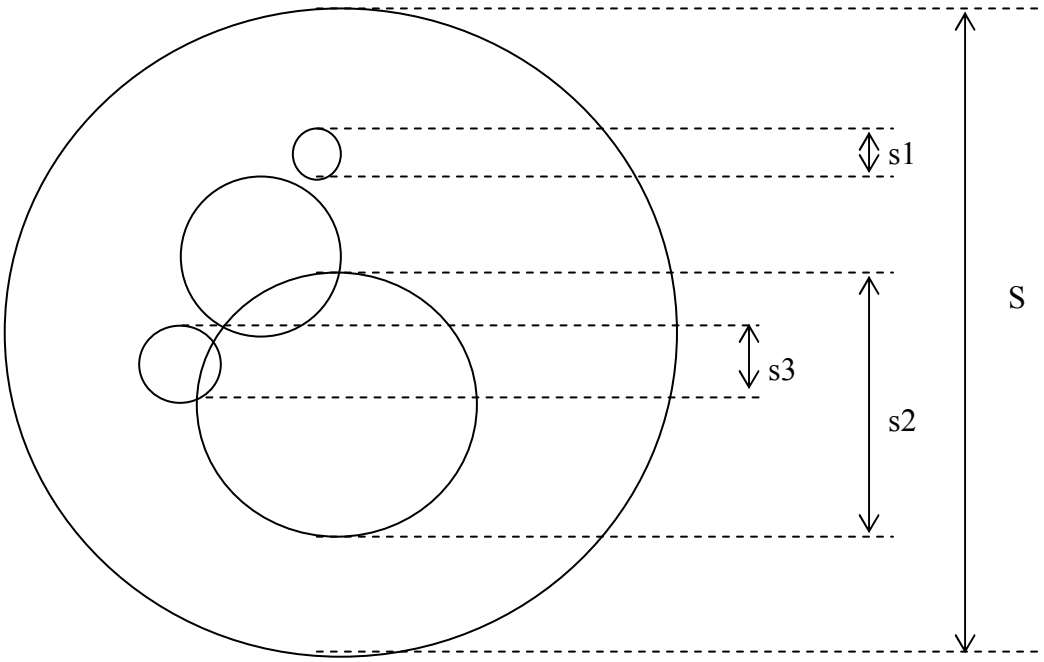

Figure 2: Relative Risk Benchmark – Diagrammatic representation of risks relative to other elements and to the overall risk of the organization.

5. CONCLUSION

The paper focuses on information risk management for small and medium enterprises. In the past, efforts at information risk management have traditionally sought to create guidelines, principles or frameworks for risk management. The "subject" organisation for these macro level efforts has typically been a large enough enterprise or Government agency with a set of critical elements and performance goals suitable to such larger organisations. While larger organizations could have security experts at their disposal, SMEs are often left

wondering how they can provide or increase the security of their IT systems.

REFERENCES

[1] Homeland Security Tools for Small Businesses, Risk Management Small Business Development Center (© 2004 Risk Management Small Business Development Center, 1402 Corinth Street, Suite #1537, Dallas, TX 75215, (214) 860-5821).

[2] Quoted from "Security administrators are under growing Information Security News: IT Managers See Need for Risk Metrics" From: InfoSec News (isn_at_c4i.org) Date: Jun 09 2003.

[3] Risk Management Guide for IT Systems NIST Special Publication 800-30 Jul 2002 Gary Stoneburner, Alice Goguen, and Alexis Feringa.

[4] Risk Metrics Needed for IT Security, Vol. 6, April 1, 2003, By Will Ozier, President, OPA Inc quoted on IT Audit journal of The Institute of Internal Auditors.

[5] Security Metrics Guide for Information Technology Systems, NIST Special Publication 800-55, and July 2003, authored by Marianne Swanson, Nadya Bartol, John Sabato, Joan Hash, and Laurie Graffo.

[6] Corporate Information Security Working Group (CISWG) - The group's objective is to recommend alternative approaches to improving information security for public and private sectors. http://www.theiia.org/?doc_id=4644

[7] The Common Sense Guide to Cyber Security for Small Businesses, Recommended Actions for Information Security, 1st Edition – March 2004 - Internet Security Alliance "Best Practices – A Twelve Step Program to Cyber Security".

[8] "Homeland Security: Tools for Small Business" by Risk Mgt Small Business Development Center, USA Sep 2004 (© 2004 Risk Mgt Small Business Dev Center, 1402 Corinth Street, Suite #1537, Dallas, TX. http://www.asbdc-us.org/.

[9] "Convergent Security Risks in Physical Security Systems and IT Infrastructures" commissioned by The Alliance for Enterprise Security Risk Management (AESRM), a coalition formed in February 2005 by ASIS International (ASIS), Information Systems Security Association (ISSA) and ISACA.