Using protection profiles to simplify risk management

Vassilis Dimopoulos, Steven Furnell, Ian Barlow and Benn Lines

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

Risk assessment is widely recognised as a necessary procedure in order to properly assess organisational network security. However, even though a number of relevant tools are available, surveys indicate that small and medium enterprises (SMEs) frequently fail to undertake risk assessment (NCC 2000). By not assessing the risks to which they are exposed, these enterprises leave important assets vulnerable to malicious exploitation, as well as to accidental loss or damage. This may, in turn, endanger a company's assets, reputation and credibility. This represents a clear problem from the company perspective, and necessitates an understanding of the underlying reasons. The answer resides in the drawbacks related to current risk analysis tools, which prohibit SMEs from using them, and instead restrict their risk assessment options to the use of checklists, guidelines and managed security services. In order to improve SME risk management, there is a need for the development of a novel risk assessment methodology that will improve the ease of application, as well as a simplifying the interpretation of the results. Although some requirements can be met by the aforementioned checklist and guideline approaches, the problem here is that they propose a solution that is too generic, and therefore those organizations without in-house security expertise to guide them may not recognize how certain elements apply to their environment. A potential alternative is to partition the generic approach in some way, and a means of doing this is based upon the concept of pre-determined protection profiles, which offer a means to simplify risk assessment, and make it accessible to SMEs from all industry sectors. A Protection Profile is "an implementation independent statement of security requirements that is shown to address threats that exist in a specified environment" [Commoncriteria 2003]. Rather than providing a single set of guidelines that aim for applicability across all organizations and environments, the protection profiles would take a more focused approach, and can be considered to provide baseline guidelines for different types of domain, different types of platform, etc - which organizations would then combine to suit their individual situation. In order to facilitate such a mix-and-match approach, protection profiles need to be structured into suitable top-level categories according to the type of protection they provide (e.g. technical, data, personnel, physical etc), which in tern would be divided into appropriate sub-categories and provide further recommendations on the security needs according to the business function and the importance of the data within. An organization would be expected to consider each of the top-level categories, and then select any of the underlying sub-categories and profiles, as appropriate to their environment. At the final level, each profile would include a general statement of relevant threats and common vulnerabilities, along with suggestions for consequent countermeasures (including an indication of the level of protection that they would provide. However, the specific content and structuring of the profiles could be approached in different ways. This presentation will, therefore, consider some of these alternatives, and the related advantages and disadvantages in each case.

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

NCC (2000) *The Business Information Security Survey 2000.* National Computing Centre URL http://www.ncc.co.uk/ncc/, Accessed 23 September 2003

Using Protection Profiles to Simplify Risk Management

Vassilis Dimopoulos

Network Research Group
University of Plymouth

Overview

- The importance of assessing risks
- SMEs and risk management
- Drawbacks of current risk analysis methods
- A suggested methodology to eliminate these drawbacks

Threats towards Organisations

- Information must be accessible in order to be useful, and it is this accessibility that puts it at risk (Hunter 2000)
- All companies have data and physical assets that are critical to their operation
- These assets are open to internal, external deliberate and accidental threats

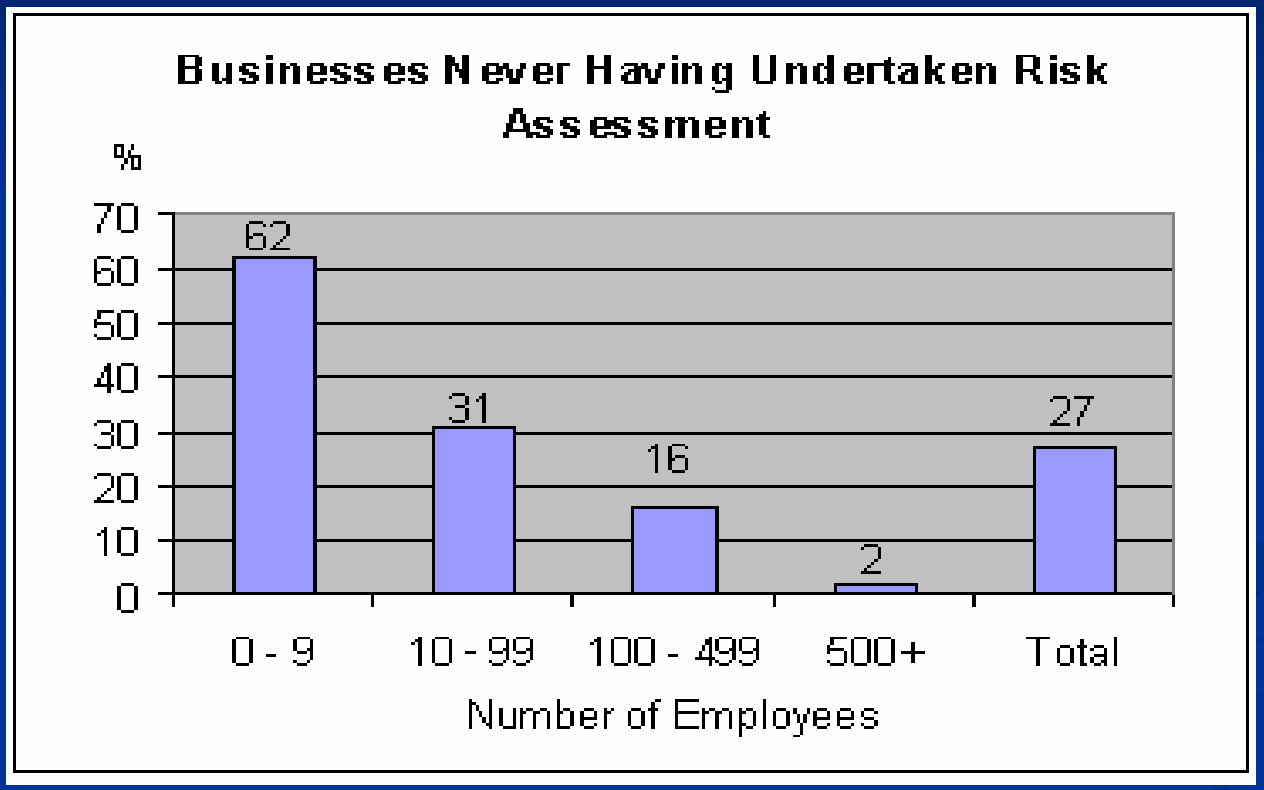
Importance of Risk Analysis

- Without having properly assessed the risks to which its assets are exposed, questions can be raised over the suitability of any security countermeasures that have been introduced
- Risk Assessment, a process which involves **analysing** and subsequently **managing** the risks is widely recognised as necessary procedure in order to assess organisational security properly

Risk Analysis in the Industry

- In 2000, only 37% of organisations in the UK had carried out a risk assessment (DTI 2000)
- In 2002, 65% of organisations had carried out a risk assessment (DTI 2002)
  - However the vast majority of those (85%) were large organisations

Risk Analysis in the Industry



(Source : NCC 2000)

- The lack of risks assessment mainly focuses upon the SME sector of the industry

Reasons why SMEs have not adopted Risk Analysis

- **Small budgets:**
  - small, medium and large enterprises have a significant difference in their budget
  - has knock-on consequences for what they will spend on security
- **Lack of expertise:**
  - 49% of small and 51% of medium organisations do not employ any employees with IT security training (ISM 2002)

Reasons why SMEs have not adopted Risk Analysis

- **Lack of awareness:**
  - creates a false sense of security
  - SME administrators and managers do not appreciate the importance of performing a comprehensive risk assessment
- **Other reasons:**
  - performing a risk analysis can disrupt management and employee activities
  - no well-understood economic model for evaluating the benefits of reducing the risks versus the investment in security technology

Other solutions available to SMEs

- Security checklists and Baseline guidelines
  - too generic and not particularly popular amongst SMEs
- 3rd party managed security services
  - still involves the cost of hiring outside expertise

Requirements for a New Approach

To tackle the problem, methodology needs to:

- Be generic enough to allow use by various types of organisations
- Be easy to implement
- Produce results that are comprehensive to the management
- Indicate the return on investment offered by security solutions

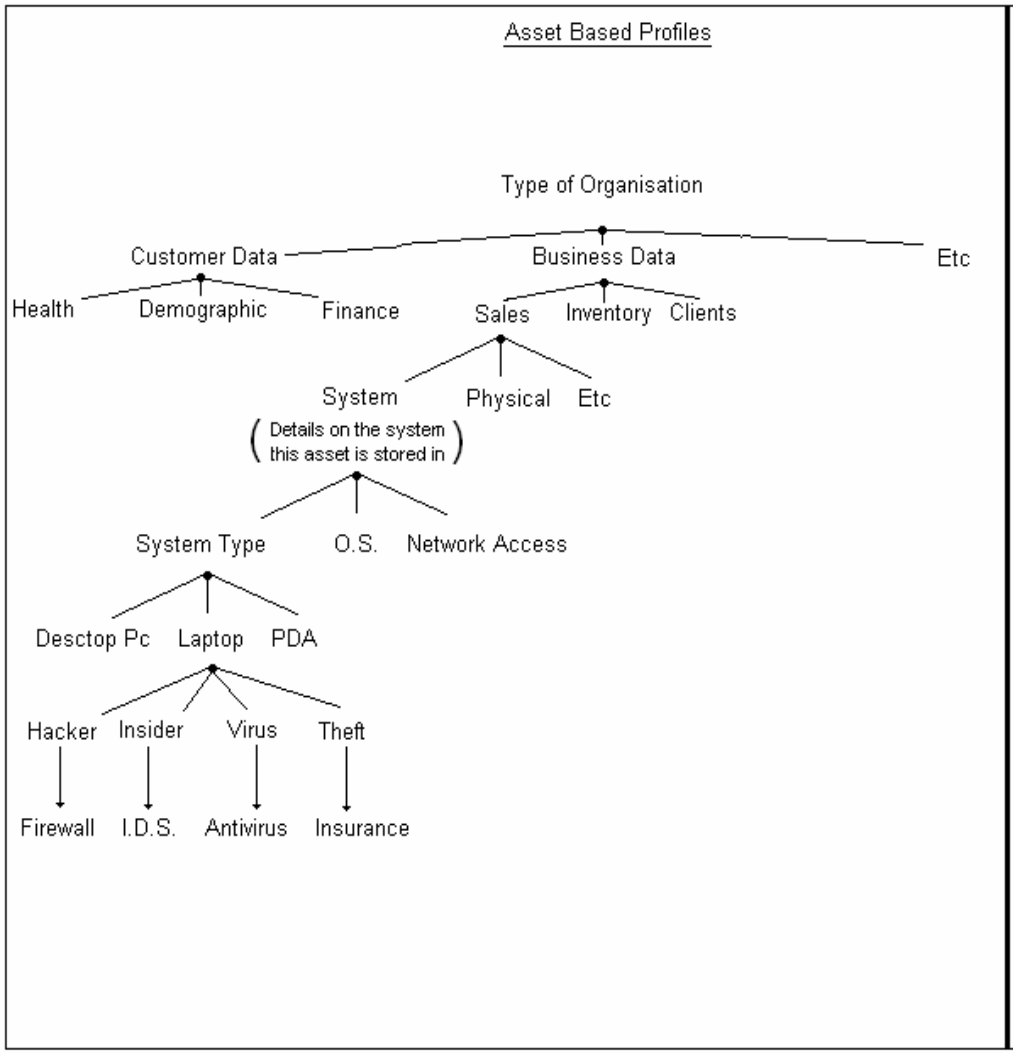
Pre-determined Protection Profiles

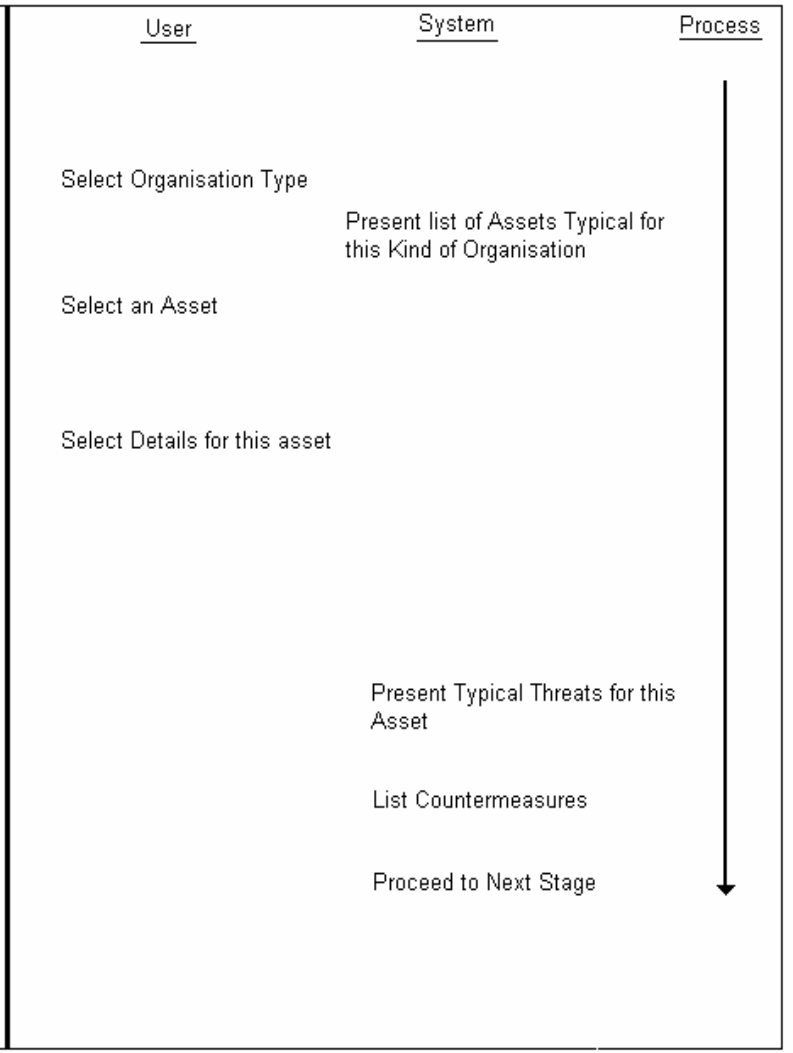
- *"An implementation independent statement of security requirements that is shown to address threats that exist in a specified environment"* (Commoncriteria 2003)
- Represent a progression of baseline security
- Can be considered to provide baseline guidelines for different types of domain, different types of platform, etc

Protection Profiles Approach

- First indicate the **type of organisation** (e.g. healthcare, manufacturing, retail etc) to identify the threats that are unique to each
- **Asset-based** PP's will assess the security of an organisation's assets
- **Personnel-based** PP's will assess personnel in terms of job function, level of access etc
- **Solution-based** PP's will assess configuration issues of the solutions to be implemented according to an organisations needs

Example: Asset-based PP's





Example Structure of a Threat Profile

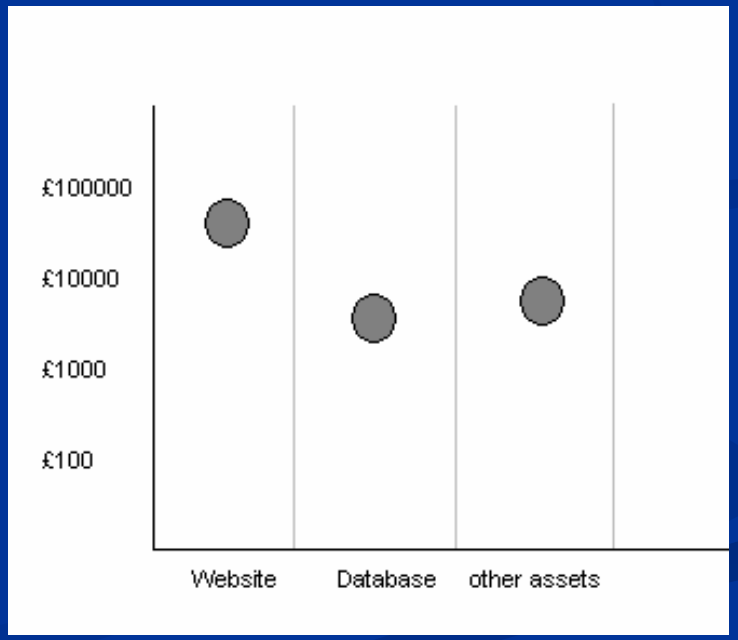
Threat Profile				
Threat name :	Malicious Code			
Definition:	Software or firmware capable of performing an unauthorised function on an information system [INFOSEC 99]			
Example:	Virus	Trojan Horse	Worm	Spyware
Likelihood level:	High			
Damage Level:	High			
Countermeasure:	O.S. Patches	Antivirus Software	Firewall	Awareness Initiatives
Importance Rating:	5/5	5/5	5/5	4/5
Implementation Order:	1	2	3	4

- Increase managerial awareness on the various threats
- Assist with the selection of countermeasures
- Suggest the order in which these need to be implemented

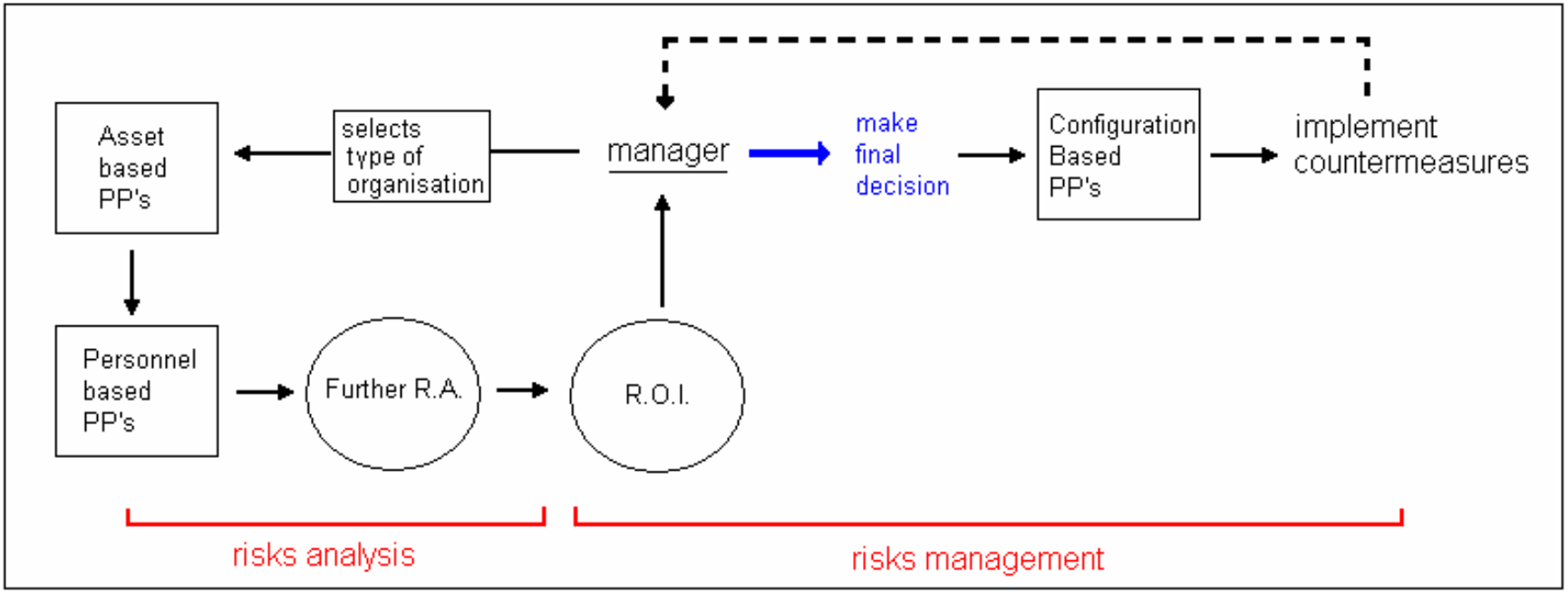
Other Necessary Elements

- Provide an indication of the Return on Investment (ROI) of the selected countermeasures

  - System would provide an estimate of a certain asset
  - Manager would then decide if this estimate is realistic



The Resulting Methodology



Conclusions

- Risk assessment is required in order to secure assets critical to an organisations operation
- SMEs do not generally adopt such practices due to lack of expertise, lack of awareness, lack of funds etc
- To be more widely adopted by SMEs a risk analysis methodology needs to be:
  - simple to implement
  - easy to interpret and
  - provide an estimation of the ROI of security solutions